8. Is the Intelligence Community Changing Appropriately to Meet the Challenges of the New Security Environment?

Grant Wardlaw

The changed intelligence environment

Pity the intelligence policymakers or officials attempting to design the ideal organisation to meet the changed strategic and operational environment that now faces them. The world has changed so much since the end of the Cold War that it is in many respects almost unrecognisable.

Many see a clear divide between the 'old' and 'new' threat environments. Treverton (2009), for example, sees the 'old', characteristic of the Cold War era, as concentrated on large, slow-moving targets (for example, Soviet political–military establishment, strategic missile systems) and a shared frame of reference between agencies that facilitated communication with policymakers and made it easy to slot in new information. The focus was on intelligence puzzles—questions for which there were answers if only the veil of secrecy could be penetrated. By way of contrast, 'new' issues are the transnational threats, such as terrorism, weapons of mass destruction, and transnational organised crime, which are small and constantly changing targets with no permanent addresses. They are constantly and rapidly evolving, they exploit our societal vulnerabilities, and they are intelligence mysteries—questions whose answers are inherently unknowable in detail (often because even the targets do not know precisely what they are going to do until they do it).

The implications of this change of targets are substantial. The threats are increasingly diffuse, transnational in nature and cannot be dealt with by single states. The information required to produce intelligence analyses comes from many different sources—often not secret—which need to be shared with a growing number of partners, many of whom are outside government. In an era of terrorism and transnational organised crime, the focus of much intelligence is prevention of individual or small group acts, rather than the intentions and behaviour of states. The nature of the targets means that more emphasis is being placed on human sources (such as spies, informants, interrogation of suspects) than on the technical approach (such as satellite surveillance, communications interception) that came to dominate the Cold War. New technologies of surveillance that are applicable to the new targets raise serious questions about civil liberties and this may limit their use. The nature of the new targets means that the boundaries between domestic and foreign intelligence and between national security intelligence and law enforcement intelligence are increasingly being blurred, if not becoming irrelevant. The danger of intelligence gaps arising has increased because, when compared with the attack preparations of states, those of targets such as terrorists may be more difficult to discern and thus offer less strategic warning (Maddrell 2009).

Analysts coming from a Cold War background were used to vertically integrated intelligence systems focused on a monolithic target (primarily the Soviet Union). The target itself evolved slowly and the analysts had years to develop a good understanding of it (AFCEA 2005). But the current environment for analysts is quite different. The threats are many and diverse in nature. Information has exploded in amount and ubiquity, and sorting for relevance has become one of the most critical jobs of the intelligence analyst. Timelines are very compressed and the requirements of the intelligence clients are more numerous, diverse and immediate. Interaction between analysts and clients is now the norm, while it used to be strongly discouraged. The operational tempo places great strain on intelligence systems and makes it difficult to schedule time for thinking, mentoring and self-development. Analysis needs to be networked, rather than the relatively solitary business it has traditionally been.

It is likely, then, that the nature of intelligence systems and practice requires both fundamental change and a capacity for continuous adaptation if these are to keep pace with the changing environment. This chapter attempts to assess the extent to which the intelligence community has been up to this challenge. It outlines some of the debates about what change is necessary, describes some changes that have taken place and asks how significant (and fit for purpose) the changes that have occurred have been.

Managing change in an intelligence context

The intelligence community faces all of the challenges of managing change according to accepted change management principles (see, e.g. Jones et al. 2004 for a brief outline of these principles). There are, however, some important context issues that affect the ability of intelligence to change meaningfully. The first is the obvious observation that using the word 'community' to describe the organisation and operations of intelligence disguises the fact that the community is really a collective term for a number of individual agencies and units. These operate often quite separately, have specific mandates that sometimes put them at odds with each other, and individual agency cultures that do so even more. So change in the community can and does occur at different times and speeds, in different manners and with more or less success in different agencies.

Policymakers have realised that this makes it very difficult to achieve more directed and comprehensive change across the community and have moved to address the issue from a strategic perspective. For example, one of the prime objectives of recent policy in Australia, especially following the release of the first National Security Statement in December 2008 and the National Security Strategy of March 2013, has been to consciously create a national security community, of which the national intelligence community is a subset. The strategy has included new coordinating mechanisms, strategic documents guiding planning, priority setting and budget management, and the creation of the position of National Security Adviser to provide leadership to the national security community. The lack of an adequate evaluation strategy, however, makes it difficult to judge accurately how far this approach has both harmonised approaches to change and been successful in changing intelligence appropriately to meet the threat environment.

A second issue is that the pressure on intelligence to change its way of operating most often comes from alleged intelligence 'failures', accusations of politicisation of intelligence, and scandals (usually involving alleged intelligence abuses). Bad publicity, poor performance, and failure are all quite common drivers of change in other settings (e.g. business) too. But in these settings it is rare that the pressure falls on a whole community or industry. In the case of an intelligence failure, it is the whole intelligence community that feels the pressure for change. This is typically driven by media hype, and suggested reforms are often simply imposed by government fiat.

Resistance to change is common in all settings, and the intelligence community is no exception. The community often disagrees with the diagnosis of the issue (for example, many would argue that intelligence failures are more often policy failures—see, e.g. Marrin 2011), the solutions are often imposed without serious consideration of expert intelligence opinion (which is often accused of merely protecting agency interests or established, comfortable ways of doing things) and some parts of the community feel that they are immune from criticism even if it may rightly apply to other parts. As Barger (2004, 23) notes:

> Intelligence professionals often have a visceral reaction to calls for new reforms, largely because the connotation of reform suggests an approach to remedy a perceived failure, implies no willingness on the part of the Intelligence Community to change, and is regarded as punitive.

> Most insiders would argue that intelligence reform efforts have resulted in more regulation and bureaucracy and little, if any, improvement in intelligence performance.

The result, again, is uneven approaches to change across the agencies that comprise the intelligence community. Consequently, some experts argue that reorganisation in response to change should be resisted more often than it is 'because the costs of reorganisation are always substantial, because it is disruptive and creates negative side effects, while the benefits often prove dubious' (Betts 2008, 6). Betts recommends that we should focus on changes that do not require major reorganisation—advice that seems to resonate with Australian approaches over the last three decades.

Ironically, in the post-9/11 era an almost universal response by governments to intelligence failures has been to increase the resources going to the community, so that it has grown substantially over the past decade. This has introduced another layer of complexity to the manner in which agencies respond to change. Not only are they grappling with a rapidly changing threat environment and constantly shifting government requirements, but they are facing all of the problems of managing rapid growth—a major change issue in its own right. While there are positives here, particularly with the recruitment of younger, more technically savvy people who might be more attuned to the contemporary threats and information technology, there are also major problems with integrating large numbers of inexperienced officers. There is often a clash of workplace expectations between old hands and new recruits and there are limitations in developing and introducing new methods and structures when a largely untrained workforce is deployed in a high-tempo operational environment.

More recently, the situation has been further complicated by the international financial situation which has seen a cutting of intelligence budgets in some countries and at least stabilisation of resources in an environment which sees continued growth in intelligence taskings. In essence, the agencies are being asked to do more with fewer resources. So the challenge facing some intelligence agencies is managing downsizing at the same time as managing an apparently insatiable appetite for intelligence. Managing changes to culture, operating procedures and analytical methodologies will be especially challenging where the fiscal realities of the present rub up against change fatigue in the agencies and security fatigue in the community (in the latter case, especially in the absence of any actual serious national security incidents).

How is intelligence changing?

It is useful to distinguish two ways in which the intelligence community adapts to changes in its environment (Nicander 2011). The most obvious (and most publicised) form of change is reactive. The community changes because of external demands, most often made as a result of a perceived intelligence failure (e.g. the 9/11 terrorist attacks) or an obvious major change in the operating environment (e.g. the end of the Cold War). The community (or some elements of it) may also adapt proactively, by changing practices or organisation as a result of either observing or anticipating changes in the environment (e.g. the emergence of new threats or wider issues such as the introduction or spread of technologies). Such changes will usually be internally driven rather than externally imposed and would be largely characterised as being innovation.

An important change that intelligence agencies have to deal with is the context for oversight of their activities. Traditionally, intelligence has been shrouded in secrecy, with intelligence activities protected from public gaze by both convention and draconian laws forbidding disclosure of sources and methods, information and even the existence of the agencies themselves. In Australia, for example, the existence of the Australian Secret Intelligence Service (ASIS) was not acknowledged by government until 1977, although it was established in 1952. It was not put on a legislative footing until 2001. However, the exposure of illegal activities by intelligence agencies in a number of countries, the occurrence of intelligence 'failures', and the changing nature of the targets—which have drawn an ever-widening number of organisations into the system of providing information or assessments—have all combined to bring intelligence much more into the public arena. The nature of the new information environment of ubiquitous information technology, social media and 24-hour news cycles has made it impossible for the governments to monopolise information in ways they used to, and media coverage and official inquiries are revealing more and more, at least on a general level (and sometimes quite specifically), about the agencies, their missions and capabilities and their activities.

Two other developments have also contributed to the increasing transparency. One is the increasing willingness (indeed, some would say enthusiasm) for politicians to release intelligence publicly to support political decisions. This was essentially the argument that was at the heart of much of the angst over the Iraqi weapons of mass destruction issue. The second is that, now that the targets are often terrorists and criminals whom states want to bring to justice, it is necessary if they are to be tried in ordinary courts that the use of intelligence in apprehending the offenders is revealed and tested in court. This means that it may sometimes be difficult to protect intelligence sources and methods.

On the whole, intelligence has responded very conservatively to this problem, challenging the right to access the intelligence which is also the evidence that a judge or jury would need to weigh up. Responses have mostly been to restrict access to intelligence either by legislative provisions or by proposing (and, in some jurisdictions, establishing) special courts that are not open to the public, have security-cleared judges and lawyers, and have different rules of evidence from ordinary courts. So far the arguments on these issues have largely been in a counterterrorism context, but they are now beginning to arise in ordinary criminal cases where transnational crime is said to be involved. Although there is an increasing trend to view high-end crime (transnational organised crime, cybercrime, significant financial crime) as a national security threat, it is going to be more difficult to argue that there should be severe restrictions on the rules of evidence and the law governing criminal investigations, just because intelligence has been the genesis of the evidence against an accused person.

But it is in this area of the intersection between traditional national intelligence and criminal intelligence that many of the responses of intelligence to change are thrown into sharp relief. Law enforcement agencies have significantly increased their intelligence capabilities in the last decade, both in size and sophistication. Originally the need to support the new counterterrorism responsibilities assumed by police drove the need to interact more comprehensively with the national intelligence community. Law enforcement agencies rapidly expanded their collection and dissemination of intelligence on terrorism to share with the national agencies, and the latter were required to share terrorism-related intelligence with law enforcement. The interaction also led to the increasing incorporation into law enforcement intelligence of national intelligence methodologies, so that the two communities are converging in terms of intelligence doctrine and processes. This convergence is something that some police intelligence officials have resisted, believing that the incorporation of military intelligence methods (in particular) into policing reflects either a takeover of police approaches or a lack of understanding of how intelligence applied to crime problems differs from its application in security settings.

This provides an interesting case study of how two parts of the larger intelligence community using the same intelligence terminology can differ so much in their approaches to the business of intelligence and in how to manage the intersections between their two domains. It is also a case study in how there can be demonstrable change (e.g. significant reorganisation) but still disagreement about the significance or impact of the change on the critical problems identified. In this case, while the language is the same, there are substantial differences in areas such as intelligence collection tasking and management and in analysis, which actually make communication and collaboration between the two communities difficult at times and certainly hamper the effectiveness of the overall system. This fact is often obscured by the official rhetoric about how far-reaching the changes have been and how well the agencies get on with one another. This is not to deny the changes that have taken place. In many ways the degree of interaction between law enforcement and national intelligence agencies would have been unimaginable 15 years ago. But observers looking at the fundamentals of intelligence in the same time span, or looking back to the post-World War II intelligence era, might find little that has essentially changed in the craft of intelligence. Since the world has certainly changed, is it realistic to expect that the basic concepts and operating methods of intelligence can have changed so little and still have a system that delivers quality advice to its clients?

One other issue is important in the attempts of intelligence to manage change in the relationship between law enforcement and national (especially foreign) intelligence—that is, the increasingly blurred lines between intelligence collection for police and for security use. The debate arose initially in the context of counterterrorism work, but is now especially relevant domestically with the designation of transnational crime as a national security issue. There has been pressure to allow foreign intelligence collectors to use their resources to spy on Australian citizens and, in some cases, to do so within Australian borders. The arguments are based on the alleged seriousness of the threat and the argument that some of the old boundaries are artificial and outdated. Similar calls have been made in other countries.

The arguments are complex, but it is easy to see why law enforcement agencies would be frustrated with some of the current restrictions. They argue that they are not being allowed to keep pace with technologies that criminals exploit and that the resulting criminality poses serious threats to national wellbeing that could be avoided if traditional intelligence collection and sharing restrictions were to be changed. The reality is that there is an inherent tension between what law enforcement perceives to be its intelligence collection needs and the collection technologies that they believe they should be able to employ, and citizen concerns about civil liberties. As Betts (2008, 11) notes: 'At some point, optimising intelligence collection and maximising civil liberties come into conflict, and which takes precedence is likely to depend on how alarmed or relaxed the public is about national security.' Managing change in this area is likely to be one of the most difficult for the intelligence community. The intelligence community must understand how both it and its adversaries can exploit evolving technological capabilities, and integrate this knowledge into its business practices. New technological capabilities also raise questions of balance between a state's rights to intrude on its citizens' privacy and the citizens' right to privacy. It involves judgments about the seriousness of the threats and how they are communicated to the public and government in a manner that is not merely self-serving.

On past indications it would not be unreasonable to conclude that police and intelligence agencies have focused almost exclusively on perceived obstacles to operational effectiveness and have little time for arguments about either the consequences of further erosions of privacy or questioning of whether or not the intrusions are proportionate to the threats. This will probably not be a sustainable position as the technologies of surveillance and data integration become even more powerful and the debate about civil liberties becomes more of a mainstream issue. If this happens, intelligence will have to be much more adept at providing a convincing case for increased capabilities and powers and will almost certainly need to manage increased oversight of its activities if additional powers are to be granted. The situation is made more complex by the public reaction to intelligence abuses. Writing about US intelligence, Treverton (2009) argues that the intelligence community faces the challenge of both reforming itself and restoring the social contract with the public, after scandals such as the treatment of insurgents and terrorist suspects in places such as Abu Ghraib and Guantanamo Bay. As a consequence, he claims: 'Intelligence agencies labour under the weight of having been deemed not just incompetent [in terms of failures such as 9/11] but malignant' (Treverton 2009, 64) and will not be given the powers and capabilities they need to respond effectively to the changing world. This is not just a problem for US agencies. Intelligence is now seen as an international community. Issues affecting one country's activities and policies tend to flow over to other jurisdictions, especially where there is a close relationship between them.

National differences

A number of observers have claimed that there are national differences in which ways of handling change predominate. As one might expect, it is widely agreed that change is externally imposed in the case of perceived failure. Studies in the US, UK and Australia have all shown that organisational change, either at the agency or the system level, is the preferred solution to failure. But each country seems different in the degree of enthusiasm for organisational solutions. Significant organisational change is the norm in the US after a perceived failure of intelligence. In the most recent example, after the terrorist attacks of 9/11 and the furore over the role of intelligence in the claims of Saddam Hussein's possession of weapons of mass destruction, the US government substantially reorganised its intelligence community. It did so following the critical findings of various commissions of inquiry (e.g. National Commission on Terrorist Attacks upon the

United States 2004, Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction 2005). The changes involved the creation of the position of Director of National Intelligence, new organisations (such as the National Counterterrorism Center) and significantly changed roles and functions for some agencies. Similar findings from inquiries in the UK (e.g. Lord Butler 2004) did not result in such significant organisational changes. The equivalent inquiry in Australia (the Flood Review; Australian Government 2004) produced even less organisational upheaval and the most recent inquiry (the Cornall Review; Australian Government 2011) also concluded that fundamental change, particularly in structure, was not required. Interestingly, this review claimed that a transformation had already taken place in the Australian intelligence community in response to the changing environment. But the evidence for this was that budgets had substantially increased, and that agencies were working more closely together than previously and were working in some new areas (such as people smuggling). This is hardly transformational and there was no discussion of fundamental changes in the way the community goes about its business.

In examining Australian responses to the challenges of responding to change, Wesley (2006) noted that such reform as has occurred has been a reaction to controversies and reviews but has always been informed by three organising principles. These are:

- functional specialisation in intelligence (i.e. different types of intelligence collection are the responsibility of separate specialised agencies)
- separation of intelligence collection from intelligence assessment
- separation of domestic and foreign collection and assessment.

If these principles are used as yardsticks against which to measure the extent of change in the community, I can only agree with Wesley's conclusion that recent reforms in Australia 'have reinforced, rather than challenged, the basic organising principles according to which [the Australian intelligence community] has always operated'. This conclusion is further reinforced by the Cornall Review which argued that 'there is no need to consider any significant restructure of the existing agencies at present although the agencies will have to consider carefully how they will adapt in response to the future challenges they face within those existing structures and cooperation arrangements' (Australian Government 2011).

The reasons for resistance to change are somewhat different in the US. Nicander (2011), for example, argues that generally the US intelligence community moves slowly in response to change, partly because of the strength of organisational cultures and the ability of the US to 'throw money at the problem', thus building new capacity or capability, often in new agencies or structures, with a corresponding unwillingness to fundamentally assess the way business is done at a systemic level. Thus, the US can have substantial change, but possibly without really adapting to the changes in the environment in anything other than a superficial or partial manner.

This brief comparison points to one difficulty in reaching general conclusions about how intelligence deals with change. The manner in which change occurs will likely vary, often substantially, depending on which country is being examined. A number of authors have pointed to the different ideas about intelligence that guide national approaches to practice. Davies (2010), for example, claimed that British intelligence culture tends to be integrative in nature while the US culture tends to be disintegrative. As Duyvesteyn (2011, 527) observes: 'These distinctive cultures are prone to specific weak points; integrative cultures are highly sensitive to groupthink and disintegrative cultures to turf wars.' In an earlier discussion of intelligence culture, Davies (2002, 62) had also pointed to the significant divergences in the concept of intelligence between the US and the UK. He notes wryly that in the mid-1990s, official committees in both the US and the UK examined intelligence methods in the other's intelligence community but in their final reports '[n]either side found anything to incorporate from the other's methods, and yet neither seemed to detect that they were talking—and hence thinking—about entirely different things when they were talking about intelligence'. Probably more importantly, however, the same observation could be made even *within* national intelligence communities. This is certainly true of the foreign intelligence and criminal intelligence communities. These differences make the task of harmonising effective change in the broader intelligence community that much more difficult and underpin a number of implementation problems.

How much change in intelligence is required to manage the changed threat environment?

According to Lahneman (2007), experts on intelligence community change fall into one of three categories based on the degree of change that they believe is required to deal with the changing environment. The first group believes that significant reform is not necessary. They claim that views that intelligence is not sufficiently attuned to change are too influenced by so-called intelligence failures. (The argument here is that failure to predict a specific threat or event is evidence that intelligence is not able to keep up with the changing threat environment.) But the non-reformers argue that since we cannot eliminate surprise altogether, the occurrence of occasional surprises does not necessarily indicate anything about the adequacy of the system. In this group, even those who recognise that some changes are necessary believe that there are greater dangers in wholesale change motivated by specific failures.

A second group of experts believes that the intelligence community is so poor at keeping up with change that it requires significant change to the way it does business and that this change needs to be transformational if it is to make a real difference. Finally, a third group falls somewhere between the other options, believing that intelligence faces such a changed (and continually changing) environment that significant reform is necessary—*but* that the change should be evolutionary rather than revolutionary.

Strangely, although there is a large literature on the changing strategic, political and social environment which is driving changes in intelligence community targets, there is a relative dearth of attention paid to how intelligence is changing conceptually to deal with these changes. Most attention is paid to intelligence community reorganisation, but not much to thinking about whether or not intelligence theory and practice should change also. As one commentator has noted: 'Very little has been written about how intelligence community agencies—traditionally rigid organisations in the core of the state apparatus—evolve and adapt to new circumstances when no market or other competitive mechanisms are present' (Nicander 2011, 535). That may be about to change, however, since one of the new trends evident in the intelligence environment is that there are now competitors to traditional agencies, ranging from clients who see themselves as analysts to commercial practitioners who claim to offer better, faster or newer services than some government organisations.

So is intelligence adapting adequately to the changed environment?

Responding adequately to changes in the new, complex and fast-moving security environment requires that intelligence has the capacity to analyse threats in a systemic manner—to see them as being interconnected and interdependent, with changes in one having impacts on others. But in reality most analysis is still stove-piped (that is, held and worked on in relative isolation from other analytical areas), generally on an issue or geographical basis. This makes it very difficult to see the connections between the threats.

Dupont (2013), commenting on the new National Security Strategy in Australia, claims,

> The Australian national security community does not yet have the analytical tools or rigorous methodologies for assessing and prioritising complex risks and anticipating system-threatening tipping points. The need for new analytical tools and methodologies was clearly identified … [in the 2008 National Security Statement] but there is no evidence they have been developed or applied.

This view is echoed by Zegart (2005) who, commenting on the US scene, claimed that the intelligence community failed to adapt to the rise of terrorism after the Cold War. She acknowledges that there has been substantial change, but notes that organisations are always changing. But she argues that change is not as relevant as adaptation—the question is, do the changes matter and does the rate of change keep pace with the rate of change in the environment? Zegart lists a number of impediments to adaptive reform and argues that important amongst these is the fact that government agencies are built to be reliable, consistent and predictable—not adaptive. Unfortunately, 'the very characteristics that give an organisation reliability and fairness reduce the probability of change' (Zegart 2005, 96).

But adaptability is exactly the characteristic that intelligence needs, to keep up with the changing environment. A senior analyst with the Central Intelligence Agency (CIA) has nicely summarised some of the characteristics of the changed environment for intelligence (Andrus 2005). Foremost among these is the fact that intelligence, especially in some of its new support to military operations and crisis roles, increasingly works in a 'real-time, worldwide decision and implementation environment' where the 'total "intelligence–decision–implementation" cycle time can be as short as 15 minutes' (Andrus 2005, 63). This is a huge change from the way intelligence has operated in the past. Tactical and strategic superiority now requires a very different way of organising intelligence and different ways of assigning responsibilities to its staff. Andrus makes the point that these compressed cycles are just the way the environment generally is organised these days, but that makes changes and individual events very hard to predict. It follows (Andrus 2005, 63) that the intelligence community

> is faced with the question of how to operate in a security environment that, by its nature, is changing rapidly in ways we cannot predict … [So] the Intelligence Community, by its nature, must change rapidly in ways we cannot predict.

But Andrus is wary of reorganisation as the basis of the solution. By its nature, reorganisation is both predictable and slow. 'By the time any particular reorganisation has taken effect, the causes that spawned it will have been replaced by new and different causes' (Andrus 2005, 63–4). Importantly, though, this judgment itself is at the core of the debate over the differing views on the correct manner in which the intelligence community should manage change. Is change as fast and as continuous and as fundamental as Andrus and like-minded experts believe? This is a critical question to resolve before deciding on the right approach to take.

However, while the preponderance of expert opinion (clearly contrasting with the opinion of politicians) is that reorganisation is not *the* answer to managing change in the intelligence world, it is almost certainly *part* of the solution. As previously noted, one of the biggest changes affecting intelligence has been the move from a focus essentially on one huge national security problem (the USSR) to an environment of many targets of a vastly different nature (for example terrorism, organised crime, weapons proliferation), requiring many more locations, smaller footprints, very mobile targets and different collection and assessment methodologies. As Hammond (2010) points out, it is unlikely that the 'best structure' for addressing the USSR intelligence target will be the same as for the much different and more diffuse threats of today. While there have been many experiments with different structures since the Cold War, none could be described as truly revolutionary. This is partly explained by institutional inertia and cultural resistance, but a more fundamental reason is that there is simply no agreement across the board as to the nature of the intelligence enterprise. This comes as something of a surprise to community outsiders but, as Hammond (2010, 687) rightly observes,

> What allows these debates to continue after so many decades is the fact that most of the key issues remain unresolved, both theoretically and empirically … Indeed, knowing how to think about this design problem in any theoretically fundamental manner is problematical, and what some observers think they know (e.g. about the virtues of centralised control and management, or about the virtues of decentralised competition) has not been subjected to rigorous theoretical or empirical evaluation.

The need to change is not just about new methods or structures. A crucial question is that of whether or not changes in the intelligence environment will change or are changing the intelligence process itself (i.e. how intelligence is developed and used). For example, there is a growing literature detailing dissatisfaction with the traditional intelligence cycle—the model which is supposed to describe and guide the conduct of intelligence through from tasking to dissemination to users (see e.g. Davies 2012, Hulnick 2006 and 2013, Richards 2012). Some experts have claimed that while much is different, there has been little real change. Lahneman (2010, 206), for example, claims that the (US) intelligence community 'still looks and operates substantially as it did at the end of the Cold War'. A seasoned CIA officer, after noting the huge changes that have occurred in the environment in which intelligence operates, goes on to say: 'Yet the DI's [Directorate of Intelligence's] approach to analysis has hardly changed over the years. A DI analyst from decades ago would recognise most of what a typical analyst does today' (Medina 2002, 23). Although that judgment was made over a decade ago, many commentators believe the same is substantially the case today. So a recent analysis (Agrell 2012) found that, while the intelligence environment and the conduct of intelligence in terms of technology, collection ability and focus have all changed significantly since the end of the Cold War, there has been no corresponding change in the underlying theory of intelligence or the industrialised knowledge production system. He believes that intelligence is significantly under-theorised and that the knowledge production system must evolve to meet new information processing and sense-making realities.

With such disagreements on fundamentals and the corresponding lack of data, it is not surprising that views on how well intelligence manages change often sound more like personal opinion than solid analysis. Nevertheless, many writers agree with Bruce (undated) that the intelligence practices required by the current environment require far greater adaptability than they are designed for, especially if they are to keep up with the changes in the environment.

Bruce proposes that we need to analyse adaptations across four different domains. The first is functional—what is it that intelligence organisations do? What are their principal functions and missions? Second is the cultural domain—what are the attitudes, values and beliefs that define the profession? Third is the question of change mechanisms—what processes are (or are not) built in to ensure adaptation? And, finally, there is the structural dimension—what are the organisational forms that characterise the agencies and the community? Bruce believes that a detailed analysis of these domains can produce a useful classification into 'old' and 'new' approaches to intelligence that could help design a truly adaptive intelligence community. We are a long way from that point at present. But Bruce (2006) also sounds a note of caution about adaptation that often seems to be overlooked—adaptation is a two-way street. As intelligence gets better at finding and understanding its targets, the smarter targets also adapt to evade intelligence. The effectiveness of intelligence will decline if its adaptive cycle falters at any point.

Some have argued that intelligence changes most when an event (usually characterised as an intelligence failure) acts as a wake-up call which focuses attention on a new threat or issue and stimulates new thinking and approaches or a redirection of effort. Broader studies of organisational change (see, for example, Clarke 2006) have found that organisations seldom take significant action to improve security or safety without the impetus of a disaster affecting them or their interests. Disasters or failures thus act as focusing events that stimulate change. Kingdon (1995) asserts that studies of focusing events show that policy change is more likely if the events highlight widespread problems (often indicating the issues are already on someone's agenda) and potential solutions have already been proposed. Exposure of novel problems is less likely to drive policy change. Further, the impact of focusing events is not necessarily long-lasting.

These findings have important implications for intelligence change. As Dahl (2010) points out, incidents such as the 9/11 terrorist attacks are often described as focusing events for the intelligence community. Certainly the attacks provoked a flurry of inquiries, recommendations, budget increases, legislative changes and intelligence reorganisations, not only in the US but around the world. But there is a wide range of opinions about the extent to which they were focusing events that had long-term effects or meant deep change to the way intelligence goes about its business. For example, Zegart (2007) believes they were not focusing events, arguing that change leading to significant performance improvements has been stymied by organisational and bureaucratic limitations. On the other hand, Dahl (2010 797) believes,

> The history of unsuccessful terrorist plots within the US in recent years does, in fact, suggest that the 9/11 attacks acted as a wake-up call that jolted the intelligence community and policy makers into a new understanding of the danger from home-grown as well as international terrorism.

It seems to me that this is a premature judgment. It may reflect little more than a willingness to change priorities—and so to change targeting and analysis—in this one field of intelligence, but might not indicate changes in the field of intelligence itself. Of course, this begs the question of how much fundamental change is really necessary and also underscores both the conceptual difficulty in designing an evaluation strategy for intelligence and in collecting and accessing relevant data. Dahl's work has, however, made an important initial contribution to analysing the influence of focusing events and wake-up calls on intelligence success and failure, and is particularly relevant in pointing out the role that decision-maker receptivity to new directions in threats or intelligence itself plays in successful implementation of meaningful change.

While Zegart (2007) claims that the intelligence system as a whole is not designed to cope well with change, others have examined the possibility that particular parts of the system have, in effect, been designed *not* to adapt. Peterson (2009), for example, discusses the central role given to intelligence requirements (the specification of the information that is needed to fill gaps in knowledge) to drive collection and analysis, and concludes that the strength of this approach—efficient allocation of scarce resources and a focus on meeting client needs—is also its Achilles heel because it ensures that most effort is put into filling gaps in existing knowledge rather than challenging assumptions and creating new insights. As Peterson (2009, 27) sees it:

> We mobilise the intelligence system to seek greater and greater clarity based on old insights and fail to develop new insights that reflect changing circumstances. We begin to seek information that helps us execute our chosen courses of action while ignoring information that suggests flaws in our original assumptions.

In other words, the requirements system itself limits the ability of the community to detect change and to make sense of it.

Especially in an era when so much emphasis is put on meeting client demands (as in the wider, non-intelligence, world) we may actually be cutting off the raising of new issues for analysis or policy consideration. Client demands for certainty—especially in an environment in which decision-makers want to (unrealistically) reduce risk to zero—can mean that the system fails to develop novel insights that may be critical for future challenges. This is true both at the operational and strategic levels. This does not mean the abandonment of the current system—which does have virtues—but it indicates that the system needs modification to ensure some capacity to collect on areas not of current concern. As Peterson (2009 33) concludes:

> If our decision makers accept that intelligence cannot provide certainty and our intelligence community gives priority to equipping them with insights necessary to support decision making under uncertainty, then we will be much more capable of anticipating events, avoiding surprise, and maintaining the strategic initiative in an ever changing world.

Treverton and Gabbard's (2008) report on the tradecraft of intelligence analysis reflects similar concerns. Following an extensive review of the way analysts work in the US intelligence community, they concluded that the traditional approaches are not optimised either to take advantage of changing technology and methodologies or to keep pace with the threat environment. They found (Treverton and Gabbard 2008, 33–4),

> Analysts still mostly work alone or in small groups. Their use of formal analytic methods, let alone computer-aided search engines or data-mining, is limited. Their basis for analysis is their own experience, and their tendency is to look for information that will validate their expectations or previous conclusions.

This approach is the opposite of what many regard as the appropriate set of behaviours in a world of many, small, rapidly emerging and changing targets, of information overload and of the availability of sophisticated analytical methods and technologies. Such a world requires an analytical community that is collaborative, often virtual and linked by robust tools and datasets. The new targets also require collaboration with a host of partners outside the formal intelligence community. The information and knowledge required for many contemporary intelligence issues lie in industry, non-government organisations and the academic community. Intelligence contact with these partners has increased substantially out of necessity but is still often hampered by old-fashioned notions of secrecy and by an intelligence agency attitude that treats partners just as sources. This latter attitude is unsustainable. Notions of secrecy will have to evolve if the collaboration is to be truly successful.

My own experience with police intelligence would lead to similar conclusions in that environment. Advanced analytical techniques are seldom employed and collaborative technologies not exploited. The confining effects of organisational culture are also very apparent. Clients focus on immediate operational outcomes in matters that they already know about, and have little appetite for additional or novel areas for exploration. Resource management almost always drives collection priorities to immediate operational support. Perhaps more surprisingly, there is little interest amongst analysts to explore new approaches. Those who do so tend to be alone in their excitement about new methods and get little support or time allocated for experimentation with them. Overall, there is little indication that intelligence is changing fundamentally in order to keep up with the changing environment. This is particularly obvious in the lack of support for strategic intelligence that is aimed at looking widely at the operating environment for signs of new developments. Such work, while seen by some as potentially interesting, is seen by most as operationally irrelevant. The tyranny of the present stifles the long view and the opportunity to be prospectively adaptive.

The limitations on the ability of analytical areas to change mean that effective intelligence in the new environment is threatened by 'a convergence of societal and governmental trends that make it extremely difficult to hire the right people, train them or allow them to collaborate effectively' (Hart and Simon 2006, 35). Although there is widespread recognition of the human resources challenges that the changed environment has brought to intelligence (see e.g. O'Brien 2008), very few of the current reforms to the community attempt to comprehensively address the recruitment, retention, workplace environment, cultural and organisational issues that arise.

Conclusion: How significant are the changes?

How significant and appropriate to the challenges of the new environment are the changes that have taken place? There does seem to be a general appreciation of the extent of the changes that have occurred in the intelligence operating environment. Most official reviews and intelligence scholars and commentators agree that the shift from an almost single-minded focus on the Cold War to the new agenda of transnational and 'new security' threats necessitates substantial changes to the intelligence community. The rapidly evolving information technology revolution is also noted as driving new challenges and opportunities for intelligence. All agree that this means new targets to be pursued, new technologies to be embraced and new partners to be engaged. There is considerable disagreement, though, about whether or not this necessitates fundamental change to the very nature of the intelligence enterprise—an 'intelligence transformation' or a 'revolution in intelligence affairs' (Lahneman 2007, 2011) to parallel the much-discussed 'revolution in military affairs' (Gray 2004).

In asking whether or not a revolution in intelligence affairs is occurring, Lahneman (2007) suggests that the answers to four questions will help determine the extent to which real change is taking place. Adapting questions originally asked about the revolution in military affairs in a seminal article by Eliot Cohen (Cohen 1996), he asks: Will developments in intelligence change how it is developed and used (process changes)? Will they change the structure of the intelligence community (organisational changes)? Will they create new elites in the intelligence community (skill set changes)? And will failure to embrace the changes affect the national security of countries that do not move with the environment (changes in effect)?

Lahneman judges that the answer to all four questions is yes, and that a revolution in intelligence affairs is already under way. Others are not so sure. An American intelligence community working group tasked to examine intelligence analysis concluded that 'for all the experimentation with technology and intelligence production over the years, intelligence products have remained remarkably unchanged: they are primarily static, branded and stove-piped' (Anon 2012). Treverton (2009, 55) believes that 'the carousel of reorganisation has produced more shuffle than substance'. However, the intelligence literature is littered with reports of either attempts to change the system (or parts of it) or suggestions of how the community should respond to the changes it faces. Whatever the merits of individual change proposals and attempted implementation, it will be useful for the intelligence community to take note of the lessons of other transformation efforts in large organisations. Barger (2004) argues that looking at these experiences teaches that three things seem to characterise successful transformations: a deliberate and focused attempt to think strategically about the business of the organisation *before* any attempt to change it; a core group who develop a new idea and stay long enough to see changes through; and a method of critically analysing change proposals to evaluate how well they would serve all (or the most important) of the organisation's strategic objectives.

My own view of where we are at present is that there is plenty of activity, some of it cosmetic and designed to meet political objectives. Some is potentially substantial change which is muted in implementation by organisational resistance and the difficulties inherent in culture change, and some is significant but too limited in scope to affect the intelligence enterprise overall. So there are questions about how real many of the changes are, how widespread they are at a fundamental level within the intelligence community, and whether or not many of the changes are actually adaptive. Given the importance to security and safety of getting intelligence right, and in view of the vast amounts of money expended on intelligence internationally, assessing the ability of the community to successfully adapt to change is a subject worthy of much more study and debate.

References

Agrell, W (2012) The next 100 years? Reflections on the future of intelligence. *Intelligence and National Security* 27(1): 118–32.

Andrus, D (2005) The wiki and the blog: toward a complex adaptive intelligence community. *Studies in Intelligence* 49(3): 63–70.

Anon (2012) Products or outputs? Probing the implications of changing the outputs of intelligence. *Studies in Intelligence* 56(1): 1–11.

Armed Forces Communications and Electronics (AFCEA) (2005) *Making analysis relevant: it's more than connecting the dots*. A White Paper prepared by the AFCEA Intelligence Committee, Fairfax VA.

Australian Government (2004) *Report of the inquiry into Australian intelligence agencies*. Canberra.

Australian Government (2011) *2011 Independent review of the intelligence community report*. Canberra.

Barger, D (2004) It is time to transform, not reform, U.S. intelligence. *SAIS Review* 24(1): 23–31.

Betts, R (2008) *21st century intelligence: progress and limits*. Address to the Canadian Association of Security and Intelligence Studies, Ottawa, 30 October.

Bruce, J (2006) Denial and deception in the 21st century: adaptation implications for Western intelligence. *Defense Intelligence Journal* 15(2): 13–27.

Bruce, J (undated) *Dynamic adaptation: a twenty-first century intelligence paradigm*. Unpublished PowerPoint slides from the author.

Clarke, L (2006) *Worst cases: terror and catastrophe in the popular imagination*. University of Chicago Press, Chicago.

Cohen, E (1996) A revolution in warfare. *Foreign Affairs* 75(2): 37–54.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (2005) *Report to the President of the United States, 31 March 2005*.

Dahl, E (2010) Missing the wake-up call: why intelligence failures rarely inspire improved performance. *Intelligence and National Security* 25(6): 778–99.

Davies, P (2002) Ideas of intelligence: divergent national concepts and institutions. *Harvard International Review* 24(3): 62–6.

Davies, P (2010) Intelligence culture and intelligence failure in Britain and the United States. *Cambridge Review of International Affairs* 17(3): 495–520.

Davies, P (2012) *The intelligence cycle is dead, long live the intelligence cycle: rethinking an intelligence fundamental for a new intelligence doctrine*. Paper prepared for the Annual Convention of the International Studies Association, San Diego, 1 April.

Dupont, A (2013) National security dilemma: new threats, old responses. *Australian Financial Review* 15 March: 1.

Duyvesteyn, I (2011) Intelligence and strategic culture: some observations. *Intelligence and National Security* 26(4): 521–30.

Gray, C (2004) *Strategy for chaos: revolutions in military affairs and the evidence of history*. Frank Cass, London.

Hammond, T (2010) Intelligence organizations and the organization of intelligence. *International Journal of Intelligence and CounterIntelligence* 23(4): 680–724.

Hart, D and Simon, S (2006) Thinking straight and talking straight: problems of intelligence analysis. *Survival* 48(1): 35–60.

Hulnick, A (2006) What's wrong with the intelligence cycle? *Intelligence and National Security* 21(6): 959–79.

Hulnick, A (2013) *Intelligence legoland: seeking better models of the intelligence process*. Paper prepared for the Annual Convention of the International Studies Association, San Francisco, 3–6 April.

Jones, J, Aguirre, DeA and Calderone, M (2004) 10 principles of change management, *Strategy+Business,* Booz and Co, 15 April, available at www.strategybusiness.com/media/file/resilience-04-15-04.pdf.

Kingdon, J (1995) *Agendas, alternatives and public policies*, 2nd ed. HarperCollins, New York.

Lahneman, WJ (2007) Is a revolution in intelligence affairs occurring? *International Journal of Intelligence and CounterIntelligence* 20(1): 1–17.

Lahneman, WJ (2010) The need for a new intelligence paradigm. *International Journal of Intelligence and CounterIntelligence* 23(2): 201–25.

Lahneman, WJ (2011) *Keeping US intelligence effective: the need for a revolution in intelligence affairs*. Scarecrow Press, Lanham MD.

Lord Butler (Chair) (2004) *Review of Intelligence on Weapons of mass destruction: report of a committee of privy counsellors,* HC 898. Stationery Office, London.

Maddrell, P (2009) Failing intelligence: U.S. intelligence in the era of transnational threats. *International Journal of Intelligence and CounterIntelligence* 22(2): 195–220.

Marrin, S (2011) The 9/11 terrorist attacks: a failure of policy not strategic intelligence. *Intelligence and National Security* 26(2): 182–202.

Medina, C (2002) The coming revolution in intelligence analysis: what to do when traditional models fail. *Studies in Intelligence* 46(3): 23-29.

National Commission on Terrorist Attacks upon the United States (2004) *The 9/11 commission report*. WW Norton and Co, New York.

Nicander, L (2011) Understanding intelligence community involvement in the post-9/11 world. *International Journal of Intelligence and CounterIntelligence* 24(3): 534–68.

O'Brien, K (2008) *The changing security and intelligence landscape in the 21st century*. International Centre for the Study of Radicalisation and Political Violence, London.

Peterson, S (2009) *US intelligence support to decision making*. Research Paper. Weatherhead Center for International Affairs, Harvard University, Cambridge MA.

Richards, J (2012) *Peddling hard: further questions about the intelligence cycle in the contemporary era*. Paper prepared for the Annual Convention of the International Studies Association, San Diego, 1 April.

Treverton, G (2009) Intelligence test. *Democracy Journal* 11 (Winter): 54–65.

Treverton, G and Gabbard, C (2008) *Assessing the tradecraft of intelligence analysis*. Rand Corporation, Santa Monica CA.

Wesley, M (2006) *Between probity and proficiency: challenge and change within the Australian intelligence community*. Commentary no. 88. Canadian Security Intelligence Service, Ottawa.

Zegart, A (2005) September 11 and the adaptation failure of U.S. intelligence agencies. *International Security* 29(4): 78–111.

Zegart, A (2007) *Spying blind: the CIA, the FBI, and the origins of 9/11*. Princeton University Press, Princeton NJ.