The failure to discover proscribed weapons systems and programmes in Iraq after the US-led invasion in 2003 has shaped many commentators’ understanding of counter-proliferation intelligence. This is not surprising; the invasion was a defining political and international event. Yet, if we look at counter-proliferation intelligence collection and assessment only through the prism of that experience, we risk the heat of political controversy obscuring important lessons for the intelligence profession. Instances where Western intelligence outcomes have been more successful are equally instructive. The negotiated end to the Libyan nuclear-weapons programme, the take-down of the A.Q. Khan nuclear-proliferation network, and the exposure in 2009 of the Iranian secret enrichment site under construction near Qom all help delineate specific features of counter-proliferation as a sub-genre of intelligence activity. The speed with which many more countries are now launching civil nuclear programmes, and the degree to which enabling technology and know-how for chemical-, biological- and nuclear-weapons programmes are becoming freely available among proliferating countries or in the marketplace, are making counter-proliferation, and accurate, actionable intelligence to support it, ever more urgent.

Today’s high demand for intelligence across a range of fields involving national security contrasts with the questioning by some Western observers
at the end of the Cold War as to whether governments still needed secret intelligence. The more perceptive could see that the monolithic existential challenge presented by the Soviet Union had given way to a range of diverse, less structured threats that would be harder for Western governments to locate and counter. In this new environment, a concerted drive by Western intelligence and security agencies to demonstrate value combined with changes in the character and spread of threats to place a new premium on effective exploitation of intelligence. The defining quality of high-value secret intelligence for a government became whether it could enable action in an area of key state interest. This stress on effective outcomes from intelligence has been particularly intense in three fields: counter-terrorism, counter-proliferation and support for deployed military forces. Even in areas that lend themselves less readily to a presumption in favour of action (such as international politics or defence), agencies and governments have sought, for cost and efficiency reasons, to ensure that intelligence gathering did not become an expensive form of professional stamp-collecting, without practical dividend beyond improving the understanding of a few specialists.

A government’s action based on high-value intelligence may be publicly visible; it may take the form of policy or contingency planning; or comprise operations pursued in secret. Even public acknowledgement of action by the government may not involve official admission that it has been driven by secret intelligence, although in some cases, like raising a state of alert, that inference is obvious and inevitably leads to speculation about the nature and scale of the threat. We witnessed in October 2010 just such media attention given to reports, first leaked out of Washington, of an al-Qaeda-inspired plot to launch fedayeen-style attacks in Europe. Everyone understands how important it is for governments not to prejudice security, police investigations or subsequent prosecutions by premature revelation of counter-terrorism intelligence, which could alert the targets of those investigations to the security authorities’ capabilities or coverage of them. But, despite the risks and potential consequences of disclosure and the need to safeguard sources, the presumption with both counter-terrorist and counter-proliferation intelligence must be that, sooner or later, the government will seek to eliminate or reduce the threat and disrupt those posing it.
Traditionally, the trick has been for the government to act without risk to sources when the threat is sufficiently advanced for the shape of it, and those involved, to be identifiable, and for effective disruption still to be feasible, yet not to delay so long that the threat becomes magnified and take-down politically or operationally complicated, or even impossible.

This pressured exercise in risk management requires delicate professional and political judgements in an unforgiving environment, where the Western media and publics, which have limited grasp of the point or principles of risk management, have no compunction about applying 20/20 hindsight. On occasion, serendipity will enable the break-out of exploitable knowledge, without risk of damage to coverage or sources. Two examples in the counter-proliferation field are the US–UK-instigated detention at Taranto in October 2003 of the vessel BBC China (a lynchpin in both the US–UK take-down of the A.Q. Khan network and negotiations with the Libyans on their nuclear programme), and the release into the public domain of details of the Iranian nuclear enrichment facility at Natanz and the heavy water production plant at Arak by the oppositionist National Council of Resistance of Iran (NCRI) in August 2002.

**A difficult business**

The drive to exploit intelligence has to be balanced against the essential fragility that characterises all, and especially the highest-quality, intelligence coverage. It has also to be set against the intrinsic limitations of intelligence, including its incompleteness, piecemeal nature and irregular availability. Recognising this, the Robb–Silberman Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, set up in 2004, noted in a tone of apparent surprise: ‘it is easy to forget just how difficult a business intelligence is’. It is one that requires professional leadership with an instinct grounded in field experience, strong organisational discipline, the creative meshing of diverse skills and capabilities, and readiness to adopt new and innovative approaches to long-standing operational problems, drawing on the lessons of earlier failures and successes. These qualities have become even more important since the invasion of Iraq brought unprecedented levels of scrutiny and public criticism for UK and US
intelligence agencies. Controversies in the late 1970s and 1980s had already caused the United States to adopt intrusive oversight by the legislature, but the Iraq experience helped generate new political and legal concerns about intelligence activity. It raised important questions about the relationship between intelligence analysis and policy that have not been resolved, and perhaps cannot be. It also had the valuable effect of educating opinion-formers, to some degree, in the complexities of intelligence and the dilemmas that can confront policymakers when given pre-emptive intelligence about a potential threat on which they may feel they have little choice but to act.

The bias towards taking action on intelligence, and the degree to which terrorism and proliferation of prohibited weapons programmes and systems go to the core security interests of the state, ensure special significance for both the quality and the timeliness of intelligence on such threats. By the same token, more than in other fields of intelligence collection (save, potentially, in conflict zones), that quality and timeliness are likely to be subject to retrospective review. With counter-proliferation intelligence in Britain and the United States, government-launched or congressional inquiries have performed the review function in public, in camera or in a blend of the two. Confirming the accuracy of intelligence on state nuclear, chemical, biological or missile programmes overseas is inevitably harder than, for example, reviewing intelligence previously collected on terrorist threats at home. Exceptionally, because on-the-ground access became available, a review of the accuracy of counter-proliferation intelligence was feasible in the cases of Iraq and Libya in 2003–04. That exercise was conducted in Iraq by the US-led Iraq Survey Group (ISG) and in Libya by UK and US intelligence teams operating in cooperation with the Libyan government, with overt follow-up by an official delegation from the International Atomic Energy Agency (IAEA). The Butler Review of Intelligence on Weapons of Mass Destruction (WMD), which reported in July 2004, took as case studies Iran, North Korea and the Khan network, in addition to Iraq and Libya, even though the prior intelligence on the Iran and North Korea stories was not susceptible to on-the-ground review and some aspects of the A.Q. Khan story remained unverified. The review’s broad terms of reference required it ‘to make recommendations ... for the future on the gathering, evaluation
and use of intelligence on WMD, in the light of the difficulties of operating in countries of concern’. This remit was designed to give a wider counter-proliferation context to its investigation of the Iraq proliferation intelligence issue. Robb–Silberman took a similarly sweeping look and considered broadly the same comparative case studies as Butler.

**Counter-proliferation, counter-terrorism and non-state actors**

To illuminate specific pitfalls in collecting and evaluating counter-proliferation intelligence, it is worth looking at the similarities and differences with counter-terrorism intelligence. Both require global reach and targeting of intelligence effort, and are concerned with transnational networks and connections. They are often bracketed together by intelligence professionals, but there are major differences. As a general rule, counter-terrorism intelligence is tactical, though there are exceptions and the impact of a devastating terrorist attack can be strategic – as illustrated by the way 9/11 has transformed the international landscape and precipitated a war in Afghanistan, which continues without resolution to this day. The threat represented by long-lasting state nuclear, chemical or biological programmes, supported by government or private supply networks, is longer term and less immediate. It offers fewer obvious opportunities for external operational intervention beyond occasional interdiction or disruption of a prohibited shipment, or moves against a supplier. Unless a denouement is accelerated by an imposed political timetable for intervention, it also allows more leeway for the review and validation of intelligence sources and assessments. Each item of intelligence has to be integrated into a patchwork of evidence derived from a range of sources, both publicly available and clandestine. This enables a process of assessment of technical progress, capability and intention that requires regular updating and challenge. This slow accumulation of often disjointed and fragmentary data, like working on a jigsaw without a picture to work from, can make counter-proliferation appear less urgent and vital than counter-terrorism. Terrorism threatens the here-and-now, whereas proscribed state weapons programmes and associated acquisition and supply networks involve investments and effort that may take decades to show how dangerous and destabilising they are.
This contrast in timescales and apparent levels of urgency, and domestic pressures to protect the public in the course of their everyday lives, make it natural and inevitable for Western governments or agencies to divert precious intelligence resources from counter-proliferation to counter-terrorism when forced to establish priorities. This is especially true when the terrorist threat appears to surge alarmingly in scale and ‘unknown unknowns’ make its magnitude and imminence temporarily unassessable, such as immediately after 9/11 or the London bombings of 7 and 21 July 2005. Similarly, security officials and policymakers are always likely to give the interests of counter-terrorism precedence over those of counter-proliferation when the two collide, as they can in relation to a country like Pakistan. At a time of heightened terrorist threat, counter-terrorism cooperation (often of an investigative nature) will appear of more immediate and greater value than impeding or choking off incremental progress in a long-standing state programme, however destabilising that programme might ultimately become.

In many respects the proliferation threat presents a greater strategic policy challenge to policymakers than terrorism does. It is hard to identify a more taxing foreign-policy problem in the past 30 years than the Iranian nuclear-weapons programme. It is indeed arguable that the spread of nuclear-weapons technology and capability across volatile regions has a greater capacity to change the world for the worse than any conventional terrorist outrage, however well directed and successful. As Iraq has shown, confrontation with a state over suspected nuclear, chemical, biological or missile programmes can be vastly more controversial, and have potentially more far-reaching domestic and international consequences, than any action pursued directly against terrorists, even if taken on the territory of another state by lethal military means (such as drone attacks). The potential seriousness of a late-stage confrontation over a state programme is indeed an argument for tackling and warning a culprit government early, provided such warning is not based on an aggressive judgement grounded in slender intelligence.
The complication here, as across the whole field of international non-proliferation and counter-proliferation, is the absence of an international consensus on nuclear weapons, with the diversity of views also reflected in some countries’ domestic public opinion. Some governments perceive the international regimes as an attempt by the declared nuclear-weapon states in the UN Security Council (the P5) to prevent other states acquiring the technology they themselves possess. This sense of P5 hypocrisy is compounded by resentment at their apparent tolerance of Israel’s undeclared nuclear-weapon capability. There is much greater consensus, international and domestic, behind counter-terrorist measures, partly as a result of a widespread, shared appreciation of the damage terrorism can wreak. This contrasts with weak public recognition of the risks of nuclear-, chemical- or biological-weapons proliferation, a post-Cold War phenomenon compounded by the failure to discover evidence of such weapons or programmes, other than prohibited missiles, in Iraq after the invasion.

Proscribed state weapons programmes increase the risk, through seepage of know-how or materiel, of terrorists acquiring what has traditionally been labelled CBRN (chemical, biological, radiological and nuclear weapons) capability. It is here that the terrorism and proliferation threats come together, combining the obvious urgency of the former with the potentially catastrophic impact of the latter. Terrorist groups will seek to pursue their efforts to acquire such capabilities in environments where they are comfortable and have some freedom to pursue R&D, without institutionalising it in the form of a programme that could be subject to sustained intelligence attack over time. It is therefore greatly to President Obama’s credit that he launched a campaign to reduce the risks of terrorists acquiring some form of nuclear or ‘dirty bomb’ capability by calling a summit of 46 nations to commit to a programme of cooperation in April 2010. He appreciates that, by definition, any CBRN acquisition by terrorists, once identified and however unsophisticated it may be, is bound to generate operational proposals for immediate pre-emptive action, especially since the imminence of the threat may be impossible to assess and no doctrine of conventional deterrence can be effective against groups with nihilist tendencies. Such operational proposals would be hard for a US president to resist, even if the consequences
of pre-emptive action would themselves be badly destabilising. The take-over by extremists of a state’s nuclear armoury, uniting undoubted ambition to acquire and use a nuclear device with a demonstrated capability, would inevitably trigger the same response. Recent WikiLeaks releases reveal enduring US and UK concerns about the security of Pakistan’s extensive and sophisticated nuclear weapons capability in this regard.

**Worst-case estimates**

Since 9/11 there has been minimal political and public tolerance in the United States and some other Western countries for failures of pre-emptive intelligence affecting homeland security. This has created a strong political and intelligence-community bias in favour of worst-case scenarios. In the case of Iraq, there was also an unfortunate history of proliferation analysis, which led the generation of analysts in 2002–03 to overcompensate for previous underestimates. Congress had criticised the US intelligence community sharply after 1990 for failing to appreciate how advanced Saddam Hussein’s nuclear-weapons programme was and for failing to identify all the chemical-weapon storage sites. This message about past analytical complacency was reinforced when the temporary defection of Saddam’s sons-in-law to Jordan in 1995 and Iraqi declarations revealed how far Western agencies had underestimated the Iraqis’ pre-1990 biological-weapons programme. In 1998 the Commission to Assess the Ballistic Missile Threat to the United States, formed by the US Congress and chaired by Donald Rumsfeld, concluded that ‘the threat to the U.S. posed by these emerging capabilities [from North Korea, Iran and Iraq] is broader, more mature and evolving more rapidly than has been reported in estimates and reports by the Intelligence Community’.

The anxiety of the UN Monitoring, Verification and Inspection Commission (UNMOVIC) not to repeat this underestimating of Iraq’s prohibited weapons capabilities, and determination to resolve unreconciled issues inherited from its predecessor UN Special Commission (UNSCOM), helped generate its exaggerated picture of those capabilities in 2002–03. Clear evidence of a previous presence in Iraq of intellectual property and know-how helped to justify assumptions about what the Iraqi regime was seeking to acquire and develop that on past form seemed eminently reasonable.
A traditional trap with intelligence assessments is that analysts will inherit assumptions, and not challenge them. Here prior assumptions had been shown as too conservative and unimaginative. Those analysts, who had no desire to be caught out a third time, were predisposed to assume the worst, unless the intelligence became available to disprove it. In effect, they shifted the burden of proof, oblivious to the wider consequences, though conscious in Washington of the post-9/11 political environment and the unforgiving mindset of administration policy principals. Perhaps more worryingly, other analysts may have been unaware of this shift and of their own inherent bias. More broadly, a worst-case mindset fitted neatly into a widely recognised tendency among intelligence officers to take a bleak view of future prospects, a pessimism that is often described, and acknowledged by the officers themselves, as a déformation professionelle. Finally, as war approached, intelligence agencies were asked by governments to advise on precautions and defensive measures in confronting Iraqi forces while they were still trying to assess the existence and nature of concealed programmes. Inevitably, assessments defaulted to worst-casing to guard against the potentially devastating consequences for Coalition armed forces of underestimating deployed capabilities.

After the 2002–03 experience, and due to the lack of an international (and sometimes domestic) consensus on nuclear weapons, a US administration or other Western government would struggle today to convince a sceptical public of the need and justification for pre-emptive military action to neutralise a potential threat identified by counter-proliferation intelligence. It might succeed if an international body lent its authority unequivocally in support, but even that endorsement might not be enough. Western public cynicism generated by the Iraq proliferation experience has been reinforced by a wariness born of the war in Afghanistan, where the argument for the continuing Western military intervention on the ground, based this time on counter-terrorism, is ceasing to carry conviction with wearying NATO publics.

Israel has offered a different model of action. Whatever its merits in international law, its successful destruction by air strike of the secret
Syrian nuclear reactor on 6 September 2007, to which the Syrians did not respond and which aroused remarkably little international controversy, is an example of accurate intelligence collection and assessment and neatly executed military action. But the Israeli government operates in a unique domestic political context, in which it claims the right to take whatever unilateral action it considers necessary to disable threats that might become existential, regardless of wider consequences. We should also recall that the raid offset earlier Israeli intelligence failures to identify the Libyan nuclear-weapons programme and to appreciate the extent of the Hizbullah missile threat from South Lebanon in 2006. As it was, the episode served to heighten still further the awareness of target states such as Iran of their vulnerability to intelligence and military attack. The difficulty of envisaging how a Western government might justify to its citizens extensive pre-emptive military action based on secret intelligence about a target state’s nuclear, chemical, biological or missile programmes is thus matched by the intensifying professional challenge, within a tightening counter-intelligence environment, of acquiring that intelligence in the first place.

**At the heart of the secret state**

Accurate intelligence on prohibited weapons programmes has always been awkward to extract because these programmes lie, by definition, at the heart of the secret state. With both state programmes and non-state CBRN capabilities in mind, Senators Robb and Silberman commented in their covering letter to the president that ‘there is no more important intelligence mission than understanding the worst weapons that our enemies possess, and how they intend to use them against us. These are their deepest secrets, and unlocking them must be our highest priority.’ Governments hosting prohibited weapons programmes that represent intelligence targets have a reciprocal priority to ensure this does not happen. As soon as a programme becomes known to hostile or potentially hostile intelligence services, perhaps through exposure of procurement activities, and subjected to intelligence attack, the secret state will ensure that programme officials, scientists, engineers and researchers are encircled by the strongest layers of protective security. They will be submitted to rigorous, perhaps regular, vetting; for-
bidden to travel, save for defined beneficial purposes; not allowed to publish scientific or research papers; required to observe highly restrictive operating procedures; and subjected to monitoring of their communications. An effective regime may enforce compartmentalization of knowledge and application of need-to-know restrictions, so few individuals will have a complete overview of the programme.

In these circumstances, direct human intelligence (‘humint’) on a programme becomes hard to obtain, unless a target with the right kind of access volunteers his services in a way that does not highlight his actions immediately to his security authorities and so compromise him from the outset. Even then his access is likely to throw only a narrow shaft of light onto the programme that will not illuminate the connections between its various components. The risk is that humint agencies will default to dependence on indirect access, in other words on sources who do not have direct bureaucratic or technical access themselves, but get their information from someone who has, or claims to have, that access. Even the simplest such chain or network introduces fresh hazards for security, understanding and reliability. A plethora of secondary casework then risks overwhelming available resources, for a poor intelligence return. It becomes easy to misjudge the size, shape and direction of a programme when reliable insights into its workings are disconnected and occasional, and when there are insufficient avenues of direct access to gain fixed bearings on the structure of the programme and to enable new data to be cross-checked. This is where the closest cooperation between collectors of intelligence of all kinds, both human and technical, can pay the greatest dividends in supplying vital corroboration and building a frame for collective understanding.

**The fog of myth**

National nuclear, chemical, biological or missile programmes lie not just at the heart of the secret state, but at the centre of the state’s vision of itself and its actual or potential position in the international order. These programmes help shape the government’s image and both domestic and regional presentation of itself. As disarmament expert Rebecca Johnson recently expressed it:
The pressure imposed on those who seek (or persistently try) to acquire nuclear weapons may be considerable, but the possession – that is to say, the successful acquisition – of such weapons has become associated with national pride, independence, technological prowess and the ‘masculine’ ability to punch above one’s weight.  

Not only will accurate, up-to-date intelligence be tough to extract in these circumstances, any intelligence targeting of a programme has to focus on those with direct and accurate knowledge of it, so that no confusion develops between myth and reality. Myths can exist at all levels in a programme. They can be ‘strategic’ in the sense of going to its very existence and be put about by politicians for domestic and regional political reasons. This appears to have been the case with some senior Iraqis before the 2003 invasion, who considered a government in Baghdad that did not have nuclear, chemical or missile weaponry ostensibly at its disposal to be at the mercy of Iran or ethnic minorities, and vulnerable to popular overthrow. Unable to question or probe without risk to their own lives, some undoubtedly believed the regime’s own bluff. Persuaded by Saddam Hussein’s obstructionism towards UNMOVIC weapon inspectors, most Western capitals also swallowed the line, encouraged by Iraqi exiles who worked their own political agenda in talking up Saddam’s prohibited weapons capabilities. Here, as elsewhere, analysts were perhaps guilty of mirror-imaging, presuming that if a member of the Iraqi leadership was reported reliably to believe that Iraq had such a capability or capabilities, then he would be in a position to know, on the grounds that a comparable figure in a Western government would be so informed, directly or indirectly. This was misplaced. It may also have reflected a naive view of how much some senior Western political figures understand of their own countries’ nuclear, chemical or missile capabilities.

Myths may operate below the strategic level and exert tactical effect, for example in relation to a programme’s technical progress. Some of Iranian President Mahmoud Ahmadinejad’s boasts about Iran’s uranium-enrichment centrifuge programme have at times appeared deliberately fanciful, designed to taunt the international community and reassure his domestic
audience that its sacrifices are worthwhile. More usually, practices of active
deception and denial, which have been a regular feature of prohibited
state programmes that have attracted international attention, are designed
to disguise progress and mislead observers, reducing external pressure
and giving the government greater space for diplomatic manoeuvre. Such
techniques and approaches are often an integral part of basic programme
planning from the outset, even down to the design of buildings. Centrifuge
halls may be housed in regular-style industrial warehouses with false roofs
and located in normal suburban industrial areas, to prevent overhead identification. A characteris-
tic feature of the A.Q. Khan blueprint, in its later stages, was that installations involved in a covert
nuclear programme should be geographically dispersed and disguised, and that work should
be broken down between various institutions, to reduce vulnerability to intelligence or military attack. Such techniques have
tended to disable traditionally productive intelligence capabilities such as imagery.8

On the other hand, misrepresentations by senior government figures
may be unintentional rather than the product of deliberate policy. They
can reflect the passage up the programme management chain of inaccurate
reporting about attainment of technical targets. Such false reporting may
reflect dislike within an authoritarian system of elevating bad news, or it
may reflect inefficiency at programme manager level or further down within
individual projects. Another driver is corruption. This is always likely to
infect a clandestine programme that is diversified and not subjected to strong
financial controls, rigorous record keeping or accountability. There will be
no parliamentary or legislative oversight of such a programme; funding will
be distributed to disguise its size and aims; much of the procurement will
be managed covertly with little supervision and few records; and technical
ignorance will prevent the leadership exercising a strong grip on expendi-
ture. Policy principals may indeed have little idea of the total financial
or industrial cost of the programme, and certainly would not want their
international or domestic opponents or the populace to know the price tag

---

Misrepresentations may be unintentional.
attached to the government’s nuclear-, chemical- or missile-weapon ambitions. A leadership’s inability or refusal to quantify the financial burden it imposes on an already strained economy complicates the task of the international community in trying to force a regime to recognise that the overall costs, financial and non-financial, of a nuclear-weapons programme outweigh its potential benefits.

Against such a background of false reporting and corruption, there is a risk that a body of petty myths about the progress achieved by the target programme will accumulate over time. These may derive from anecdotal accounts or from bureaucratic records or updates for programme managers who do not check developments on the ground through personal field visits. If such misleading accounts reach the outside, they will encourage hostile intelligence agencies, already prone to ‘worst-casing’, to exaggerate the effectiveness or speed of a programme. Comparable unintended bias at the heart of the programme towards under-reporting progress is intrinsically less likely, although, as we have seen, a leadership may seek to conceal or downplay progress, as a matter of deliberate policy and practice, by engaging in active deception.

**Leadership and management**

The extent to which political leaders understand their own nuclear, chemical or missile programmes from a technical and managerial standpoint is a critical issue. The answer will vary from country to country, but the scientific and technical aspects of a programme represent a major barrier to top-level government understanding. It is improbable that Supreme Leader Ayatollah Khamenei, whom we may assume to have the last word on the future of the Iranian programme, has a strong grasp of the complexities of a nuclear-weapons programme or the different routes to achieving weapons capability. It is inevitable that leadership will delegate direction and oversight of a programme it understands only loosely to senior figures who are managerially qualified to sponsor and drive it forward, even if not themselves scientists or engineers. These programme sponsors will have their own institutional or personal interests in shaping the programme. In the case of a nuclear or missile programme, it will represent both a major indus-
trial effort drawing on resources across government and the economy, and a serious drain on government finances. This creates the probability that, unless tightly regulated at the centre, it will become distorted by corruption, weakened by diversion of funding or capability, and undermined by rivalries between competing programme or resource managers.

Any intelligence service investigating such a programme will have to recognise the impact of these elements on its coherence and effectiveness and take account of them in analysing incoming intelligence reporting or data. The example of Pakistan and A.Q. Khan, who turned from clandestine procurement for the Pakistani nuclear-weapons programme he launched to clandestine start-up and supply of other states’ programmes on his own account, demonstrates that such factors do not rule out ultimate delivery of a highly effective and diversified nuclear-weapons capability. Indeed, while multiplying the cost of a programme and extending its timelines, they can spur that diversification, create greater resilience through duplication or competition, and generate confusion and ‘noise’ that is misleading and distracting for foreign intelligence analysts. It is a mistake to assume that an ill-functioning or erratic political or bureaucratic system cannot host a highly effective weapons programme. The incredulity in some Western capitals at the nature of the Libyan nuclear-weapons programme, once disclosed, reflected just this kind of underestimation.

The problems top-level leadership will have in grasping the science and engineering involved in a nuclear, chemical, biological or missile programme raises the interesting, but under-studied, question of how programme management exercises influence on the policy of the leadership, and what mechanisms exist for resolving the conflicting demands of the programme and of foreign policy. Insight into how the intersection of science and policy (and politics) plays out within a particular government system is vital for understanding the motivation for the programme, and its strategic concept and direction. In the case of a nuclear-weapons programme, such as Syria’s, what has been the strategic rationale? Understanding this would help us
to assess the chance of its clandestine revival, perhaps again with North
Korean support. In respect of Iran, was the original concept of Tehran’s pro-
gramme to have a break-out capability or a deployed capability, or have its
plans encompassed both? Has the objective changed over the course of the
programme? What are the present priorities and requirements of the pro-
gramme? These questions, which represent key intelligence requirements for
Western intelligence services, have also been vital ones for the government
of the host state. Those controlling high-level government policy, or their
representatives, will have reviewed them in forums where they can be briefed by those in charge of the
programmes on technical progress, obstacles, resource
requirements and so on, and work out with them how
best to proceed before issuing instructions. The impor-
tance of such forums and of this kind of exchange of
views will be all the greater when negotiations are
under way in which the international community seeks suspension of a
programme, or aspects of it. The Iranians have on occasion agreed to short
suspensions, presumably at times when the programme managers could
assure the policy principals they would not damage immediate pursuit of
the programme or its longer-term advance.

The effectiveness of such forums and the extent to which they are institu-
tionalised will be key to the efficacy of a programme in achieving a
regime’s strategic objective, especially once it is beyond the earliest stages
after launch. The forum need not be large in terms of leadership representa-
tion. Indeed, it may comprise just a few individuals, one of whom may be
the lynchpin. For the Syrian nuclear programme, that figure was General
Muhammad Sulayman, who was killed by a sniper on the sea front near
Tartous in early August 2008, less than a year after the Israeli attack on
the al-Kibar reactor. A programme may have weak political direction and
control after launch, with the drive coming from scientists and engineers
after the initial fiat from the leadership, but it cannot remain free-standing
for long. Resource constraints and disguise requirements usually guarantee
a regular link with senior regime policymakers. After a certain point, there
will also be connections to other programmes, especially in relation to plans
eventually to marry up a warhead with a delivery system. The quality of the gearing between leadership and programme management becomes increasingly crucial to success as the programmes progresses. Any state programme will have to rely heavily at some stage on the clandestine procurement of equipment abroad, though this dependence is likely to diminish as the programme becomes more mature. A state’s prohibited weapons programme represents a broad effort across key arms of government. Intelligence and security agencies, in particular, are likely to have prominent roles, ensuring protective security and driving covert acquisition abroad. There may also be state-to-state transfers or exchanges, linking parallel nuclear or missile programmes and governments that have no obvious common identity or interest other than pariah status (such as North Korea and Iran). Such links, which are a feature of proliferation today in contrast to the original state nuclear-weapons programmes, enable programmes to short-circuit and accelerate processes, reducing their detectable footprint. The provision by Pyongyang of uranium hexafluoride (UF₆), for example, obviates the need for a tell-tale uranium conversion facility (UCF). Such transfers have helped breed private networks that deal in plans, blueprints and components, and are an increasingly globalised phenomenon. These linkages between states or between private suppliers and states can supply leads and insights that would not be available if programmes were free-standing without reliance on external support, yet they also extend the range and complexity of the analytical task.

The analytic challenge
Policy, military or intelligence actors engaged in directing and safeguarding a programme are all susceptible to conventional intelligence attack, but intelligence targeting and assessment of the programmes themselves require technical and scientific expertise in the fields of nuclear, chemical or biological weapons or missiles. This is in short supply among Western analysts, and those who have it are increasingly likely to lack previous personal involvement in such state programmes. As Butler pointed out, this means that the views of specific individuals may carry disproportionate weight. They may also be the champions of inherited assumptions that could domi-
nate thinking without challenge, unless subjected to deliberate, systematic questioning and red-teaming.

Relative lack of expertise and practical experience makes it the more likely that analysts will adopt a linear framework for assessment based on the pioneering experience of early programmes, such as the established uranium-enrichment route familiar to the UK and European partners in Urenco, or the path trodden more recently by equivalent non-P5 powers pushing for missile or other capability. Such a linear approach, with its emphasis on continuity, has the virtue of providing an analytic framework. It also generates potentially valuable benchmarks of progress, and assumptions about procurement, sequencing, bottlenecks, rate of progress, testing and so on. Traditional timelines need, however, to be reckoned against the availability today of computer numerically controlled (CNC) machines. These have greatly accelerated the performance of previously difficult engineering tasks, while demanding markedly less skill on the part of engineering staff. These and other technical advances have shortened timelines and allowed programmes to overcome or sidestep important hurdles.

The linear approach retains its value, but it also increases the chances of analysts not putting themselves in the shoes of those they are studying. They will be liable to take it as read that they understand the direction of a specific programme. However, subject to pressures appreciated only in theatre, whether shortfalls in expertise, raw materials or engineering capacity, programme scientists and engineers may be prepared, or forced, to experiment with alternative and untried routes to their objectives. Distant analysts, operating within a different tradition, may not take these seriously or underestimate them. They may not appreciate that less stringent safety requirements or demands for accuracy or reliability can open other avenues of development. A classic example of this was the dismissal by US analysts of the ‘super-gun’ effort pursued by Saddam’s regime before 1990. In a comment that applies to all forms of prohibited weapons programmes, the Rumsfeld Commission warned in 1998 of emerging ballistic-missile powers: ‘their ballistic missile programs often do not follow a single, known pattern
or model, and they use unexpected development patterns. These are not models of development the U.S. follows or that intelligence analysts expect to see.\textsuperscript{11} Challenge to prevailing assessments, based on red-teaming or other approaches, is vital to ensure analysts take into account all potential routes to a programme’s intended or presumed outcome.

Intelligence collection and assessment in the area of nuclear-, chemical- or biological-weapons systems or missiles or related programmes should in principle be easier than in, say, the field of politics, because the science introduces an ostensibly objective benchmark against which elements of the reporting can be judged. Politics being an art rather than a science, there is much that is anecdotal or subjective about political intelligence reporting. A sensitive political event will appear variously to different protagonists, depending on personal interests and agenda, access and understanding of the background. Intelligence reporting will reflect those variables and consequent uncertainties. There is ready scope for a source to invent, distort or embellish, whereas technical reporting on prohibited weapons systems or programmes can be tested, in theory at least, against the science. This may show straight away that a source does not have the access or qualifications he claims and that the reporting is therefore a fabrication. A source on a VX chemical-agent programme who claims technical expertise and access cannot fudge or invent convincingly, although today’s ready access to open-source data through the Internet may lend initial technical plausibility. One either does or does not know about the production of VX. The scientific benchmark injects an element of genuine objectivity into the assessment process and greatly assists validation of both reporting and source. Yet that objectivity is far from absolute and the scientific element enormously complicates both collection and assessment.

With regard to collection, there is a fundamental problem of handling, when a humint source offers intelligence on technical counter-proliferation issues. A normal operational case officer will not have the technical background and understanding needed to question, probe and assess a source’s technical access, qualifications and assertions. He can be easily misled or confused by technical explanations and data, and will be unlikely to trust his normal instincts about a source since he is conscious of not personally comprehend-
ing the scientific or technical dimension. On the other hand, technical analysts or experts, who are not trained for fieldwork and may be in heavy demand for operational deployment as well as analysis, will tend to focus exclusively on the technical dimension with sources and to neglect the human element. They lack the skills, experience and instincts of a specialist in humint, and can even be affected by direct personal contact with sources into giving them more credence than they deserve. Such analysts are much less likely to spot the nature of a source’s motivation, the extent of his truthfulness, and whether he had the relevant technical access throughout the period he claims, or has used knowledge of the direction and projected timescales of a programme to pretend he was involved for longer than he was (a particular problem in this area). The solution is to bring the two areas of expertise, humint and technical, to bear simultaneously. Unfortunately, practical operational circumstances and the personal nature of case management and debriefing can make this awkward and sometimes ineffective. Moreover, unless senior intelligence officers take particular care, contrasting professional backgrounds and thought patterns can lead humint and technical specialists to communicate poorly, using terminology or projecting a mindset their counterparts do not comprehend.

**Strategic context**

One characteristic that working-level technical analysts and operational case officers tend to share is a discreteness of mind that is a reflection of both temperament and their practical approach to professional challenges. They are inclined to focus on individual pieces of the jigsaw and use inductive reasoning. As the picture of the target programme expands in scope and complexity, they will need to work closely with those who possess wider expertise, a broader strategic overview, and the geopolitical background to achieve a comprehensive and accurate understanding of what is happening within the programme. This is not straightforward; just as humint experts and technical specialists find it difficult to develop effective teamwork, a chasm in understanding can exist between technical and geopolitical analysts. The latter do not have the technical expertise needed to probe and question the technical specialists, while the former find it hard to comprehend the strategic context. Yet, collectively, they should aim for a seamless
understanding of a programme that extends from the top scientists at the core, its institutes and research or engineering offshoots, to its commercial companies, supply routes and international partnerships. This requires that those with the strategic overlay develop a good grounding in the technical aspects of nuclear, chemical, biological and missile programmes, and spend time considering with those who command the available detail what are the strategic objectives of the programme under study. Those who lead analytical or operational effort also have a responsibility to ensure that they seek expert opinion from outside the narrow intelligence community and give it adequate weight, whatever institutional interests may be at stake. Shared analytic techniques will be key to effective exchanges.

Strategic understanding of a target state programme should be an integral part of discussion and review from the point at which that programme starts to take shape from the emerging data, instead of being introduced at a later stage when ill-justified assumptions about its rationale, nature and direction may already have become rooted in analytical thinking. This understanding, based on analytical interpretation uninfluenced by government policy or domestic politics, should then form the framework within which senior intelligence officers or top analysts present intelligence on difficult technical issues to policymakers. This should be in easily digestible and assimilable form, while avoiding over-simplification or distortion. Like those leaders who launch state weapons programmes with little grasp of the scientific and technical fundamentals, policymakers pursuing counter-proliferation goals often have limited background or frames of reference for evaluating the intelligence that comes before them. The role of the senior intelligence officer or top analyst is to ensure accurate transmission of the intelligence, subject to all the appropriate caveats attached to sourcing and analytic interpretation, and to help policymakers, who carry great responsibility, understand the significance of the intelligence, without themselves seeking to influence the policy outcome.

A confusion of specialists

If the difficulty of combining technical expertise with effective agent handling is a problem that hampers effective and productive management of a
source to which an intelligence agency has direct access, it is compounded where the technical access belongs to a sub-source, and reporting is mediated through a source without relevant technical expertise. Unless the sub-source’s reporting is in documentary or electronic form, there is small chance of it offering genuine value, even if the source is reporting reliably and accurately (which was not the case in some instances reviewed by Butler12). A similar issue can arise in relation to sources in the hands of a third service. That service may simply pass on reporting without giving background on the source, making validation impossible, or it may provide the background, including identification of the source and a description of his access, but without making the source directly available for debriefing. The Iraq reviews offer an excellent example of the hazards that can arise in the latter case.

Curveball was a former Iraqi technician in Baghdad’s biological-weapons programme, who reported to the Germans on the alleged status of that programme (and in particular on mobile production facilities) at the point he left Iraq in 1998. His reporting was subject to considerable scrutiny and treated with some scepticism from the outset, but the process of validation was made immeasurably more difficult for the US and UK agencies by lack of direct access to him and the fact that his account was mediated through a third service with inevitable language and professional impediments. The US and UK agencies were unable to make their own direct assessments of man and data and to separate fact from speculation until too late in proceedings. This detachment and lack of control gave space for technical and humint disagreements over the case to become part of wider institutional disputes in Washington about the handling of Iraq’s prohibited programmes.

The Curveball saga is instructive in highlighting the extent to which scientific experts can disagree about the same intelligence reporting. His account became increasingly controversial following the Coalition’s failure to find evidence of prohibited weapons programmes or systems (other than missiles) in Iraq immediately after the invasion. He was finally discounted in
2004 as unreliable and insufficiently corroborated. Yet scientific opinion throughout this period was divided about whether he had had the access he claimed and at what point he lost it. Experts could also argue that, even if some or all of his reporting was generally assessed to be unreliable and should be withdrawn, it nonetheless offered useful insight into the nature of the programme and those participating in it (a view that could apply also to fabrication or exaggeration in fields beyond technical intelligence). However, the phenomenon of scientists’ disagreeing was also evident in Iraq in mid-2003 in connection with claimed physical evidence of a biological- and chemical-weapons programme, where there was no direct intelligence dimension to add complication. The two trailers discovered by the Coalition in Iraq in April 2003 generated a major controversy among scientists. Some believed these were mobile biological-warfare laboratories built to a Russian design, which they resembled. Others considered their purpose entirely conventional, specifically for hydrogen production. The weight of scientific opinion in the end favoured the second view, but it remained contested long after autumn 2003, when the wider political argument about Iraq’s prohibited weapons programmes and systems was settled.

Such differences in technical views confuse and delay the evaluation and validation of a source and his reporting. They also illustrate the point that in the biological- and chemical-weapons field reporting or evidence may be compatible with quite different processes, leaving those without scientific or technical backgrounds helpless in the effort to arrive at an agreed technical interpretation. This is a subset of the wider problem of equipment that can be used for two or more purposes, only one of which is linked to a prohibited programme (‘dual use’). An industrial dryer can be used for producing anthrax or dehydrated mashed potato. The uncertainty this introduces with regard to both purpose and process mainly but not exclusively affects the biological- and chemical-weapons field; it can apply to equipment such as aluminium tubes, which may be rocket-motor casings or used in centrifuges. It greatly complicates international monitoring and domestic export-licensing regimes (against the background of a weak chemical-weapons convention and no international biological-weapons convention at all), and demands that intelligence used to justify or trigger
interdiction or another form of intervention be extremely precise. In addition, a biological-weapons capability can be developed in a small laboratory without any obvious signature, and the product of that programme held in a small lock-up or bunker. In this field, the know-how and intellectual capital is more important than the hardware, with much of the practical challenge lying in weaponisation or delivery of the agent.

The intrinsic difficulty of the intelligence challenge in these circumstances, and the consequences of underestimating the threat, encourage worst-casing as soon as new intelligence appears that points worryingly to a new dimension of that threat. If a senior official involved in a nuclear-weapons programme is confirmed to be breeding pathogen-free chickens, analysts will posit the existence of a biological-weapons programme rather than an innocuous explanation. A terrorist’s use of coded language will likewise be subject to worst-case interpretation. It is no accident that the greatest counter-proliferation successes over the last few years have been in targeting and tackling nuclear and missile programmes, and the greatest failure has related to chemical weapons in Iraq. The US cruise-missile attack on the al-Shifa pharmaceutical factory in Khartoum in 1998 in the apparent belief that it produced VX was warning enough of the hazards of relying on partial, contradictory, vague or indicative intelligence as the basis for military action. However, even a chemical-weapons programme is easier to identify accurately than its biological-weapons equivalent. The Robb–Silberman Commission despaired that ‘the threat is deeply troubling today; it will be more so tomorrow, when genetic modification techniques will allow the creation of even worse biological weapons. Most of the traditional Intelligence Community collection tools are of little or no use in tackling biological weapons.’

* * *

Whatever the eventual outcomes in Iraq and Afghanistan, at some point governments will again have to face the question of how to tackle a serious threat in the proliferation field identified through intelligence, and how to secure public support for the pre-emptive action they propose. Nuclear
Exploring the Maze: Counter-proliferation Intelligence

proliferation threatens to become more widespread, thanks to the Iranian example and increasing reliance in emerging countries on civil nuclear power for clean energy and to meet rapidly increasing demand. Confronted by a growing range of potential intelligence targets, Western policymakers and intelligence agencies will meanwhile be constrained by increasingly tight resources in the present fiscal climate. The priority will still be tackling the al-Qaeda-led terrorist challenge which, despite having been suppressed in recent years, continues to demand heavy intelligence and security coverage. The development of offensive and defensive cyber capabilities is also likely to absorb growing levels of resources, since cyber attacks have the potential to wreak havoc, even destruction, on technologically advanced countries.

Budget and resource pressures imply that Western governments will have to opt for earlier political intervention once they become aware of a fresh proliferation risk when dealing with nascent state non-conventional-weapons programmes. Such action will mean greater consequential security risks for sources and even greater dependence on reliable validation. In these circumstances, the security of the source, however professionally sacred to intelligence practitioners, can no longer be such a key determinant for policy. In the future, intelligence agencies will have to accept, and from the outset prepare for, the risks and costs of exfiltration and resettlement for sources that have been burnt through diplomatic action, just as policymakers will have to recognise the loss of access and insight that might ensue from such action.

Western governments and agencies do not yet appear to have confronted this issue of earlier intervention. The risk in today’s environment is that sustained focus by Western intelligence agencies on just a few targets over a long period will result in them being shocked by break-out from a state programme they are not covering, or are even aware of. This was already a concern for Robb–Silberman in 2005: ‘Across the board, the Intelligence Community knows disturbingly little about the nuclear programs of many of the world’s most dangerous actors. In some cases, it knows less now than it did five or ten years ago.’ With such a high proportion of intelligence and security effort devoted to counter-terrorism since then, and with an
expanding range of countries developing access to nuclear technology, the situation is surely worse today. If there is one new encouraging element, it is the development in recent years of new forms of measurement and signature intelligence (‘masint’) based on remote sensing and other techniques, which can supply first alerts of emerging threats and valuable corroboration for human and other forms of intelligence.

There will be little chance of securing a new strategic international regime as a successor to the Nuclear Non-Proliferation Treaty if governments intending to breach the regime are not warned off nuclear-weapons programmes before they have invested heavily. If Western agencies are to embark on effective burden-sharing, they will have to take their relationships with one other to a new level of trust and agree methodologies for validation. At a time of tightening resources, this is the only realistic means of covering the widening range of countries that deserve close intelligence attention in the nuclear and missile fields, and of enabling early diplomatic intervention. If they are to replicate the successes, not the mistakes, of the past, and avoid being blind-sided, Western agencies will have to identify, and act on, agreed lessons from earlier experience with counter-proliferation intelligence.

Notes

4 Robb–Silberman, p. 9.


8 Robb–Silberman, p. 16.


10 Butler Review, p. 16.


12 Butler Review, pp. 100–01.

13 Robb–Silberman, p. 34.

14 Ibid., p. 4.