16

Intelligence in arms control and disarmament

Tim McCarthy

The complexity of the post-Cold War arms control and disarmament environment imposes exceedingly difficult demands on international verification bodies.[1] These demands arise from a fundamental requirement to assess quantitatively and qualitatively information provided to the verifier—a task complicated in recent years by increased pressures on resources and a highly dynamic political milieu. Despite these obstacles, international organisations have generally proven adept at appraising the correctness of data. More pronounced difficulties arise, however, in the attempt to assess the completeness of information—cases where governments may be acting in bad faith and where declarations are incomplete or deceptive.

Since international organisations act under a number of legal and political constraints, their ability to solve this (well-recognised) problem is ultimately limited. In the breach, verifiers can, and have, exploited the information gathering and analytical techniques available only to sovereign governments, or, more specifically, to their national intelligence agencies.

Finding the appropriate type and degree of contact between national intelligence and multilateral arms control and disarmament organisations is a continuing and controversial issue.[2] Debate over the efficacy of this relationship centres on the profound 'credibility' dilemma that any international body faces when it accepts, refuses or does not act on intelligence. On the one hand, the use of national information strengthens the organisation's capabilities, allowing it to pursue its mandate more rigorously. On the other hand, the extent to which an international organisation accepts or relies on 'subjective' state intelligence may decrease its legitimacy as an objective agent of verification and may call into question its credibility and standing as a truly international body.[3]

The state providing intelligence faces its own predicaments. As a rule, intelligence organisations are reluctant to release information to bodies outside their national authority. Oft-repeated fears of disclosing 'source and methods' are one of a series of potential risks in providing classified data. But the information may only be actionable, or even provable, through the agency of an international verification body, most typically via an on-site inspection. In this regard cost–benefit calculations on the release of intelligence are just as daunting for the provider as they are for the receiver in deciding whether to accept or to use it.

This chapter explores the inherent dilemmas raised between national intelligence bodies and international organisations involved in arms control and disarmament, and analyses the role intelligence plays in international verification. The first section provides brief case histories of three organisations—the UN Special Commission (UNSCOM) on Iraq, the International Atomic Energy Agency (IAEA) and the Organization for the Prohibition of Chemical Weapons (OPCW)—in order to understand their experiences with intelligence agencies and information. This section also examines efforts within these bodies to analyse substantial amounts of internally and externally generated data that, in effect, create their own organic 'intelligence' capability. The second section surveys the approaches and guidelines that underlie the provision of intelligence by the US, the most important actor in terms of this issue. The results will serve as a model for future comparisons of other intelligence providers' policies. The last section reviews several, perhaps less publicised, areas, where the use of intelligence can most benefit an international verification body, and looks to the future of the complex relationship between international organisations and intelligence providers.

The UN Special Commission

In its 1991 resolution creating UNSCOM, the Security Council implicitly recognised that the new inspectorate would require classified intelligence and information from member states to fulfil its mandate. Resolution 687 gave UNSCOM the authority to designate sites for inspection beyond those declared by Iraq.[4] Information as to the location of those undeclared sites—particularly at the outset when the Commission had no corporate expertise—could only come from national governments and their respective intelligence agencies. From this rather humble beginning, UNSCOM's acquisition and consumption of intelligence grew to levels unmatched by any previous international organisation. Iraqi recalcitrance and the relative lack

of bureaucratic or legal obstacles helped to drive the unusual degree of contact between inspectors and intelligence agencies.

To a large degree, operational goals determined UNSCOM's interaction with secret services and its use of intelligence information on a specific issue.[5] For example, intelligence data did not fuel the majority of inspections to verify Iraqi declarations, a more traditional arms control and disarmament exercise. Of course UNSCOM did receive 'tips' in this regard, and member states did provide routine reconnaissance briefings. But internal analysis and planning produced most of these verification leads. National information, however, did play heavily in the search for hidden weapon sites and undeclared information, as well as in the investigation of Iraq's 'concealment mechanism'—its systematic effort to hide weapons, documents and equipment from inspectors. Indeed intelligence was an integral, even inseparable, part of this latter pursuit.[6]

The Commission pursued the acquisition of intelligence and national information through a variety of means; the type of data received reflected this multifaceted approach. Member states provided inspectors with the reconnaissance briefings and *ad hoc* tips on, for example, illegal procurement activities, such as Iraq's covert purchase of Russian inertial instruments and test equipment. Lower-grade tactical intelligence—on security conditions in Baghdad, for instance—was available once the team assembled for its mission. The bulk of intelligence, though, arrived following a specific request from the Special Commission. Supporting governments produced, *inter alia,* estimates of remaining weapon capabilities, technical evaluations of equipment, site assessments, or decryption services. In an interesting twist to the international organisation–nation state relationship, UNSCOM often provided member governments with detailed information on illegal procurement endeavours that had occurred within their borders. In supplying the data, UNSCOM sought an investigation into the activities, and, in turn, expected to be briefed on the results.[7]

Despite its reliance on intelligence for certain undertakings, UNSCOM never became a captive instrument of the providers of information for two key reasons. First, the Special Commission pursued a deliberate policy of seeking information from many countries that, according to former Chairman Rolf Ekéus, did not necessarily talk to one another or were willing to have their contributions known.[8] Second, and most important, UNSCOM's expertise on Iraq's weapon programmes, along with the information gathered through its missions in Iraq, eventually outpaced the expertise and data held by any one country. The Information Assess-

ment Unit—the Commission's analytical and operational arm—effectively organised inspection and other data and focused assessment efforts. As a result, UNSCOM analysts knew more about the Iraqis than anyone else did. These developments led to a subtle shift in the terms of trade regarding the provision of intelligence: UNSCOM not only had to rely relatively less on a particular country's intelligence to mount an operation, but inspectors were also able to obtain more raw data to evaluate on their own terms.

Ultimately the often tightly coupled relationship between UNSCOM and several intelligence bodies led to severe criticism of the organisation and contributed, in no small part, to its demise. But the inspectorate's extraordinary pursuit and use of intelligence can only be understood within the context of Iraq's long-running efforts to thwart UNSCOM's mandate, and the inability of the Security Council to deliver a consistent, meaningful message to Iraq in response to its intransigence. Faced with incomplete declarations and lack of international political will, inspectors pushed hard on concealment and other investigations to uncover both remaining proscribed items and to force Iraq either to accept inspection of sensitive sites or explicitly to refuse access. Clear denial of access, it was hoped, would politically damage Baghdad and awaken the Security Council to on-the-ground realities in the country. Given the sophistication of Iraq's deception techniques, data to support effectively these investigations had to come from intelligence organisations.

The International Atomic Energy Agency

Before the passage of resolution 687 in 1991, the IAEA in Vienna had little meaningful access to intelligence from its member states, nor an organisational capability to receive and assess such information.[9] However, the Agency's new nuclear disarmament mandate in Iraq brought with it an obvious requirement to exploit national intelligence data. Meanwhile, revelations about the Agency's supposed failures in Iraq, and its subsequent pursuit of a more robust safeguards regime, resulted in member states providing expanded intelligence on countries other than Iraq, and the creation of new analytical approaches within the Agency for examining a number of data sources.

The IAEA created an Action Team, a new body under the Director-General, to conduct inspections in Iraq. It drew some of its experts from the Department of Safeguards, but it was never a formal part of the Department. Intelligence agencies were apparently wary of providing information directly to Vienna at the onset of

inspections. The language of resolution 687, which gave UNSCOM authority to designate undeclared nuclear sites for inspection (and implicitly to receive intelligence towards that end), in part reflected this unease. In the event, supporting governments initially sent information to the Special Commission, which, in turn, provided targets for the first UNSCOM–IAEA teams sent to undeclared nuclear sites. Indeed the Action Team did not have full access to defector information that triggered early nuclear inspections. But it appears that, after several inspections were completed, some intelligence was flowing directly to the Action Team without the UNSCOM filter. By the end of 1993, the Agency began receiving U-2 reconnaissance briefings in a manner similar to those provided to UNSCOM, although not on a systematic basis. Thereafter it appears that member states continued to provide information to the nuclear inspectors, based on specific requests from the Action Team and on an *ad hoc* basis.

The information sharing relationship between UNSCOM and the Action Team did not always reflect the relatively well ordered Action Team–intelligence relationship. While the two bodies continued to work together throughout the inspection process, the Team felt that the Commission never granted Vienna full access to the considerable intelligence data in its possession. This was especially true for valuable data regarding Iraq's concealment activities in the nuclear area. From UNSCOM's perspective, the sensitive nature of the information demanded strict compartmentalisation, even if it meant keeping relevant data from nuclear inspectors.

By the end of 1991, IAEA Director-General Hans Blix began to seek broader access to intelligence to enhance the safeguards regime. At first he wanted to create an office in the Agency to receive and assess this type of information. The Board of Governors did not support this approach, so, instead, Blix informally named a senior aide in his own office to whom intelligence should be given and with whom responsibility rested for making initial evaluations.[10] These officials have included Pierre Villaros, a French national, and, later, David Sinden, a Canadian. A small group of senior IAEA officials assisted Villaros and Sinden in the evaluation process.

As this informal structure took shape, governments (especially the US) began to provide the Agency with intelligence on countries other than Iraq. For example, it appears that the US provided intelligence briefings and/or information derived from national technical means (NTM) related to:

- Iran in early 1992, late 1993 and, perhaps, in early 1996 and 1997;[11]
- South Africa in mid-1992; and

- the Democratic People's Republic of Korea (DPRK) in early 1992, early 1993, late 1994 and late 1998.[12]

It also appears that Blix, along with senior aides, received some of these briefings at the US Embassy in Vienna. Intelligence provision concerning the DPRK resulted in an extraordinary Board of Governors meeting on 22 February 1993, where the US displayed satellite photos of North Korea's undeclared waste processing sites and a decoy facility.[13] Agency officials say they did not provide any formal feedback to, or engage in data exchanges with, the US intelligence agencies.

To enhance significantly the effectiveness of safeguards—pertaining, in particular, to the completeness of data—the Agency is pursuing a variety of measures that extend well beyond access to intelligence, including environmental sampling, expanded state declarations and increased physical access to declared and undeclared sites.[14] Evaluating data collected through these efforts is an integral element of the effectiveness of enhanced safeguards, and the IAEA has created new management structures and processes to improve analysis of information. State Evaluation Reports, produced by country officers in the Operations Division of the Safeguards Department, are at the heart of the now three-year-old system. Assessments are derived from several sources:

- state declared information (such as design information and operating records);
- safeguards verification information (for example, inspection data and analysis, sampling, and inspector observations); and
- other IAEA and 'open source' information (such as internal IAEA databases, technical co-operation reports and public media).

The Safeguards Department integrates these data, checking for consistencies across a spectrum of evaluation points.

The new Information Review Committee, comprising Division Directors and a Co-ordinator from the Office of the Deputy Director-General for Safeguards, assesses these evaluations and develops consensus recommendations for follow-up activities. For example, the assessment might point to a declaration inconsistency that could require discussions with a member state or additional inspections. The Committee reports these recommendations to the Deputy Director-General for Safeguards, with the results ultimately contributing to conclusions in the Agency's annual Safeguards Implementation Report. This process allows the IAEA to judge better the correctness and completeness of state declarations.[15] Future iterations of

the evaluation system will incorporate commercial satellite imagery, visualisation software, and geographical information systems.

Organization for the Prohibition of Chemical Weapons

The Chemical Weapons Convention (CWC), which was opened for signature in January 1993, and the implementation guidelines approved by the Conference of States Parties (CSP) define in detail how information—state declarations and inspection and other data—will be handled, processed, used and released by the OPCW. The Convention and the CSP have similarly elaborated criteria for determining timing and frequency of inspections of treaty relevant sites, which, in turn, provide the basis for the OPCW's internal analyses. In sharp contrast to UNSCOM, and to a lesser extent the IAEA, the Technical Secretariat and the Director-General are more constrained in their potential dealings with intelligence bodies and in the development of analytical methodologies.

While neither the CWC nor its implementation documents explicitly refer to 'intelligence', it is clear that the OPCW may receive intelligence in pursuit of its mandate. Indeed there appear to be several plausible scenarios under which states might provide intelligence data to the Organization:

- by initiating a challenge inspection;
- by providing a designated observer with more detailed data during a challenge inspection;[16]
- by supporting investigations of alleged use of chemical weapons (CW);[17]
- by initiating and supporting investigation of an OPCW employee for breach of confidentiality;[18] and
- by requesting assistance and protection against use or the threat of use of CW.[19]

In addition, it appears that, in conversations with Director-General José Bustani or, prior to that, with the Executive Secretary of the Preparatory Commission, Ian Kenyon, member delegations informally provided 'information' on the CW activities of other countries. Pakistan, for instance, expressed specific concern regarding India's programme in meetings with Kenyon. The degree of detail of the information is unclear. Regardless of how or where states transmit information, the OPCW will benefit from having a large number of staff who either have intelligence backgrounds or who are familiar with intelligence issues, and who meet frequently with state party delegations comprised of foreign and defence officials.[20]

A CWC challenge inspection will surely generate political controversy. It is useful to examine in detail, therefore, how challenge inspections might involve intelligence sharing and the factors that will determine the scope and detail of information a state party provides. Surprisingly, the former US Arms Control and Disarmament Agency concluded that information defined by the CWC as being necessary for initiating a challenge inspection does not require intelligence data.[21] But the Conference of States Parties approved an illustrative list of data that would fulfil a state's obligation to supply 'appropriate information on the basis of which a concern has arisen' over non-compliance. For example, the list suggests provision of detailed information on the nature of suspected non-compliance, the period of such activities and the specific chemical signatures emanating from a facility.[22] It is difficult to imagine that this could come from anywhere other than an intelligence source.

Clearly it is in the interest of the party requesting a challenge inspection both to provide enough information so that the chances of discovering non-compliance are high and to increase the political burden on an inspected state party if, and when, it refuses to allow a thorough inspection.[23] These powerful motivations might force a state to convey more detailed, all-source data, as it takes the calculated risk of a challenge inspection proposal. Certain OPCW policies might also inspire confidence among intelligence agencies that their data will be (relatively) secure, leading to the provision of more detailed information. For instance the OPCW's elaborate Policy on Confidentiality incorporates stringent penalties for unauthorised disclosure of sensitive information,[24] and the organisation has consistently focused on developing a 'security culture', even during the PrepCom process.[25] Finally, in addition to the formal requirements for information provision leading to a challenge, the requesting state may engage 'in further exchanges of information' with the Director-General on the matter.[26] This provision may allow the state to gauge the level of information the Director-General views as appropriate or to convince him further of the validity of the information provided.

Of course, a number of factors might also dissuade a state party from intelligence sharing. First, the CWC text calls for due regard to be paid to selecting team members for challenge missions 'on as wide a geographical basis as possible'.[27] If a state does not trust a national on a team, it will be more reluctant to provide data (or more detailed data once the team is in the field) for fear of misuse. Second, a potential information supplier may be reluctant to do so given a possible (although politically unlikely) determination by the Executive Council that a state has abused the right

to request a challenge inspection—a finding that carries financial and organisational penalties. The CSP proposed several indicators of an abusive request, including negative determinations on the authenticity or reliability of information provided.[28] Clearly the practice of intelligence makes ensuring reliability of information a difficult proposition, and, based on the UNSCOM experience, on-site inspections often reveal that intelligence data was 'false'. Third, the inspected state party can demand copies of team notebooks, increasing the risk of an unintentional disclosure of sensitive information. Finally, the inspected state can reject a designated observer, potentially robbing the team, therefore, of its ability to communicate with the information source in the field and undermining inspection effectiveness.

In the absence of state-provided intelligence or a challenge inspection request, the OPCW generates its inspection planning through an internal analytical process. The CWC, its verification annexes, and a number of conference decisions establish guidelines for this process. These guidelines are far too complex to discuss in detail in this chapter, but, in general, the Convention provides, *inter alia,* a legal obligation for the timing of most initial inspections, development of facility agreements for some sites, and a limit to the number of inspections at declared facilities. Decisions taken by the CSP elaborate and refine these legal requirements. Thereafter, in most cases, the Technical Secretariat determines the number and intensity of inspections based on facility 'risk assessments', the criteria for which are, again, often detailed in the Convention or in CSP decisions. For example, the Convention notes that inspectors shall assess the facility's 'risk to the object and purpose of the convention' posed by the chemicals produced at a so-called Schedule 2 site, and the characteristics and activities of the site.[29]

The Chemical Demilitarisation and Industrial branches in the OPCW's Verification Division are jointly responsible for performing risk assessments of the relevant facilities, and, therefore, comprise the chief analytical arm for OPCW operations. Once site declarations are processed, the two branches use this data for inspection planning, which began in earnest one year after the Convention's entry into force in April 1997. The OPCW also uses software tools and its information management system for inspection planning.[30] It is not clear if intelligence provided by a member state will be fed into this information management system, thereby allowing inspectors to use the data as part of its standard assessment process. Alternatively the OPCW might opt to follow a more informal structure for intelligence assessment similar to the IAEA.

The US approach

In the decade following the 1991 Gulf War, the US has gone from having, at best, an inconsistent intelligence relationship with international organisations to being the most important provider of such information to international verification bodies and regimes. A brief history of these events indicates that the growth in information sharing has not taken place smoothly, as the intelligence community and even Congress have shown greater reluctance to release data than policymakers. Sharp disagreement over control of, and access to, information has also characterised the relationship between American providers and international receivers of intelligence. Other countries seem likely to mirror these dynamics. This review also offers, via the debate over CWC ratification and the resolution forwarding the Senate's consent, a unique public insight into how the intelligence sharing process works.

Early UNSCOM inspections established a precedent for the US to provide intelligence. The administration of President George Bush, intelligence officials, and congressional committees worked to establish the ground rules and to fund the effort, which extended beyond data transfers to include the establishment of a liaison centre in Bahrain. These arrangements—facilitated by the presence of US nationals on UNSCOM inspection teams and in senior UNSCOM positions—proved to be extremely effective. The information flow was timely enough to lead to several highly successful inspections (particularly, although not exclusively, in the nuclear area) which demonstrated Iraqi non-compliance with its disarmament obligations. At the same time, US intelligence agencies surely benefited from discussions with inspectors regarding UN requirements to identify additional sites. Release of information to non-US team members, control of certain collection efforts, and access to raw data were a few of the continuing problems between US intelligence and UNSCOM, although the overall relationship was surprisingly smooth. These problems, however, came into sharper focus as UNSCOM employed more intrusive inspection techniques and the stakes for American military involvement in Iraq rose.[31]

This precedent paved the way for the US to expand intelligence sharing beyond UNSCOM. As noted earlier, US intelligence flowed to the IAEA Action Team, just as Washington supplied other information to the IAEA in pursuit of its broader safeguards mandate. In the case of intelligence related to North Korea, the scope and detail of information grew rather slowly. In part this was because US analysts wanted access to IAEA data (operating records for DPRK reactors and test results from foreign laboratories) in exchange for American information. Although the

IAEA did not oblige, Washington ultimately concluded that it was important to provide its knowledge without reciprocity. When lower level CIA analysts balked at providing satellite photos to the Board of Governors, they were overruled first by then CIA Director Robert Gates and later by the Clinton administration.[32]

This trend toward increased information provision hit a critical snag in February 1995, when US officials discovered several boxes of classified US documents left in a vacant UN office in Somalia.[33] The discovery and subsequent controversy reinforced congressional efforts to limit data exchanges with international organisations, culminating in an unsuccessful Senate attempt to restrict intelligence sharing with the UN, through a variety of measures.[34] The backlash from the Somalia episode affected even UNSCOM, as weapon inspectors experienced a temporary interruption in the receipt of intelligence until the case was resolved.

During debate and analysis over CWC ratification, the question of intelligence provision and the relationship between international inspection regimes and US intelligence efforts were once again brought into sharp relief. Both the Clinton administration and the intelligence community noted that the CWC would be a net plus in unilateral US attempts to detect potential chemical threats. National Intelligence Estimates and other analyses concluded that, overall, state declarations and the inspection regime would: improve the ability of intelligence to obtain data regarding CW programmes; give access to useful information otherwise unobtainable; and add another tool to the intelligence collection kit.[35] The intelligence community made this argument in spite of the recognition that state parties would largely be prevented from access to raw inspection data, and that employee secrecy provisions forbade the US government from seeking special information from American nationals employed at the OPCW.[36]

While the Senate noted and concurred with these judgements, it sought to enact stringent rules and safeguards related to potential US provision of classified data to the OPCW. In approving the ratification of the CWC, the Senate attached 28 conditions to its resolution, one of which dealt specifically with the required process for intelligence sharing. The spirit of the condition, and its language, was derived from earlier Senate attempts to restrict intelligence following the Somalia case. The process enumerated in the resolution reflects the approach that US intelligence now apparently takes with all international organisations, including the IAEA and UNSCOM's successor, the UN Monitoring, Verification and Inspection Commission (UNMOVIC). In brief, the Senate declared that the US may not provide

information to the OPCW until the President establishes that: mechanisms for its protection (within the OPCW) are in place; OPCW staff can protect it and security procedures will be enforced; unauthorised disclosure will result in only minimal damage to American national security; and no matter how thoroughly sanitised, the information and its provision must have inter-agency US intelligence community approval. However, the Director of Central Intelligence can find that it is in 'the vital national security interests of the United States' to release the information. If he does so, the above conditions may be waived, although such waivers must be reported in detail to the appropriate congressional committees.[37] Thus far, and despite strenuous efforts by government personnel, agreement has not been reached with the OPCW on handling US classified data and, as a result, no information has been provided.

Conclusion

The foregoing analysis highlights a number of areas where international disarmament bodies have used intelligence to expand their verification capabilities. It indicates that the provision of intelligence to international disarmament organisations is a now a well established practice, although it remains politically sensitive.

In terms of future developments, it is useful to identify relatively unexploited opportunities.[38] One possibility is the use of intelligence in identifying denial and deception (D&D) operations. States seeking to hide weapon capabilities will employ D&D techniques, but international organisations are generally ill-prepared to uncover and understand them. National intelligence has a unique role to play in this respect.[39] Moreover, a cover-up (D&D in practice) often yields more signatures than the hidden or proscribed activity itself. Thus, the unmasking of a cover-up may be the first step towards revealing non-compliant behaviour; the ability to do so will be an important tool for international organisations.

Another option involves the training of international inspectors by intelligence agencies. This relatively value-neutral mission would prepare and educate inspectors and international analysts, allowing them to pursue more effectively their tasks. Training courses might include interview techniques, observation skills or recognition of denial and deception signatures. A third possibility is a systematic request by international organisations to intelligence agencies to provide broader analyses on subjects of concern. Analyses would extend beyond the 'smoking gun' tip to include, for example, proliferation scenarios for a particular country, 'lessons learned'

studies of prior proliferation cases, economic assessments, or broader country overviews. These reports do not have to be based on highly sensitive information; they would simply provide international analysts (such as the IAEA's country officers) with additional sources of data that they might reject or accept.

International arms control and disarmament bodies are likely to continue efforts to promote intelligence provision, but this will not extend to 'co-operation' or systematic exchanges of data with member states. These and future organisations also seem likely to adopt strict confidentiality policies—like those of the OPCW—which would be designed to increase intelligence providers' trust in the organisation. Compartmentalisation of data will be more acceptable, as the realities of handling sensitive information become more engrained in the international disarmament culture. Internal analytical capabilities will also be enhanced—especially through the exploitation of open and grey source data—as organisations adapt to, and integrate, developments in the information revolution.[40] Indeed, access to high-resolution commercial satellite imagery will likely have a profound impact not only on how organisations make assessments, but also on their relationships with intelligence agencies.[41] No longer will the IAEA, for instance, have to rely on governments for quality imagery of a particular site (although it might still lack interpretative expertise). Finally, international organisations will promote cross-fertilisation to compare systematically their experiences with intelligence and data analysis. It seems doubtful, however, that this cross-fertilisation will involve information sharing, at least in the short term.

While intelligence provision may be an accepted practice, several issues—which will determine the future relationship between intelligence agencies and verification bodies and the political acceptance of the relationship—remain unresolved. In the final analysis, the critical issue is to determine the most appropriate and effective use of intelligence, which, at the same time, ensures that international bodies continue to be, and continue to be perceived as, objective, independent actors. The answer to that question will reflect the notion that, while dilemmas in the relationship are inherent and potentially troubling, they are manageable.

Tim McCarthy is a Senior Analyst and Program Director at the Center for Non-proliferation Studies, Monterey Institute of International Studies, US. He served as Deputy Chief Inspector for the UNSCOM Missile Team, undertaking 15 inspection missions in Iraq.

Endnotes

[1] Unless stated otherwise, information for this study is derived from interviews and correspondence with former and current officials who serve(d) in international agencies, governments, or in both. These sources wish to remain anonymous.

[2] This paper defines 'intelligence' and its linguistic derivatives, such as 'national information', as the secret collection and analysis of confidential data by a state. Although this definition conveys a process, the paper focuses on the output of that process: the secret information or analysis itself.

[3] For an example of this view, see Brahma Chellaney, 'Arms Control: The Role of the IAEA and UNSCOM', in Muthiah Alagappa and Takashi Inoguchi (eds.), *International Security Management and the United Nations*, United Nations University Press, Tokyo, 1999, pp. 375–393.

[4] United Nations Security Council, S/RES/687 (1991), 8 April 1991, Section C, paragraph 9(b)(i). Of note, the resolution also gave this 'designation authority' to UNSCOM for nuclear sites, with inspections to be carried out jointly by the IAEA and UNSCOM.

[5] The type and character of the personal relationships between particular inspectors and intelligence providers also facilitated (or hindered) information flows. The greater the degree of trust, the more willing an intelligence agency was to release information to inspectors.

[6] See Barton Gellman's two-part series, 'Shell Games: The Hunt for Iraq's Forbidden Weapons', *Washington Post*, 11–12 October 1998. Available at www.washingtonpost.com.

[7] These efforts achieved uneven results. Several governments did, in fact, provide information and went as far as inviting UN experts to their countries for more detailed discussions. Others simply refused to respond.

[8] Gellman.

[9] According to the former head of the IAEA Action Team, Maurizio Zifferero, the Agency had no access to intelligence before resolution 687. See Maurizio Zifferero, 'Iraq and the UN Security Council Resolution 687: A New Approach to Verification', in James Brown (ed.), *New Horizons and Challenges in Arms Control and Verification*, VU University Press, Amsterdam, 1994, p. 222. Other sources dispute this account. Author interview.

[10] In February 1992, the Board formally approved Blix's efforts to make intelligence available to the Agency.

[11] Pierre Villaros participated in the Agency's February 1992 and November 1993 'visits' to several undeclared sites in Iran. He also took part in the Blix mission to North Korea in May 1992. Before these trips, US intelligence apparently briefed Villaros on American information related to these countries.

[12] Undoubtedly, the US provided additional briefings/data not included above. Moreover, other member states, such as France and the UK, also supplied intelligence data.

[13] See R. Jeffrey Smith, 'North Korea and the Bomb: High-Tech Hide and Seek', *Washington Post*, 27 April 1993, at www.washingtonpost.com. This article indicates that the US provided degraded satellite photos, although other very reliable sources note that the photos were not degraded. Author interview.

[14] Generally grouped under the Strengthened Safeguards System. See chapter by David Fischer in this volume.

[15] 'Strengthening the Effectiveness and Improving the Efficiency of the Safeguards System', IAEA General Conference, GC(42)/12, 16 September 1998, paragraph 3, at www.iaea.org. 'Report of the Director General to the Conference', IAEA General Conference, GC(42)/22, 17 September 1998, paragraph 19(a), at www.iaea.org.

[16] Chemical Weapons Convention, Verification Annex, part X, paragraph 54.

[17] Initiated under Article IX or X of the CWC.

[18] 'OPCW Policy on Confidentiality', OPCW Conference of the States Parties, First Session, C-I/Dec. 13, 16 May 1997, part IX, paragraph 3.1(b) and 3.3, at www.opcw.org.

[19] Article X, paragraph 9 of the CWC.

[20] It is not clear if any member state has provided information of an intelligence nature to the new disarmament body; nor is it clear if any state has established formal or informal mechanisms for the transfer of such data. This is certainly the case for the US government.

[21] US Arms Control and Disarmament Agency, 'Answers to Questions [related to the CWC]', in *US Capability to Monitor Compliance with the Chemical Weapons Convention*, US Senate, Select Committee on Intelligence, 103rd Congress, Report 103–90, US Government Printing Office, Washington, DC, 30 September 1994, Appendix B, p. 109.

[22] 'Notification Formats in Challenge Inspection . . .', OPCW Conference of the States Parties, First Session, C-I/Dec. 44, 16 May 1997, p. 15, at www.opcw.org.
[23] Douglas J. MacEachin, 'Routine and Challenge: Two Pillars of Verification', *CBW Conventions Bulletin*, issue no. 39, March 1998, p. 2.
[24] The policy is enumerated in 'Guidelines for Release of Classified Information . . .', OPCW Conference of the States Parties, First Session, C-I/Dec. 13, 16 May 1997, at www.opcw.org. Admittedly, the policy appears aimed at the unauthorised release of commercially sensitive or state declared information, although the same rules and procedures would certainly apply for intelligence data.
[25] See, for example, Preparatory Commission for the OPCW, *Report of the Executive Secretary*, PC-XII/II, 7 December 1995, paragraphs I.II–I.I3, at www.opcw.org.
[26] OPCW, 'Notification Formats in Challenge Inspection', paragraph I(f)(III).
[27] Verification Annex, part X, paragraph A(I), of the CWC.
[28] 'Illustrative List of Objective Indicators . . .', OPCW Conference of the States Parties, First Session, C-I, Dec. 45, 16 May 1995, pp. I–2, at www.opcw.org.
[29] CWC, Verification Annex, part VII, paragraph 18. The Conference further elaborated on these criteria in the OPCW, 'Assessment of the Risk Posed By a Schedule 2 Facility', Conference of the States Parties, First Session, C-I/Dec. 32, 16 May 1997, at www.opcw.org.
[30] In its decision to adopt the architecture for the information management system, the Preparatory Commission noted that the system must support the OPCW's verification activities by providing the means to store, access and analyse data provided through declarations or gathered through inspection '*or by other means*'. Preparatory Commission for the OPCW, *Report of the Preparatory Commission*, PC-3/II, 2 July 1993, paragraph I.2. (emphasis added)
[31] For a review of the high stakes disagreement involving US intelligence and UNSCOM, see Seymour M. Hersh, 'Saddam's Best Friend,' *New Yorker*, 5 April 1999, pp. 32–4I.
[32] See Smith.
[33] R. Jeffrey Smith and Julia Preston, 'US Probes Security for Somalia Files', *Washington Post,* 12 March 1995, at www.washingtonpost.com.
[34] See *Report on the Foreign Relations Revitalization Act of 1995*, US Senate, Committee on Foreign Relations, 104th Congress, Report 104–95, US Government Printing Office, Washington, DC, p. 75 and pp. 223–225.
[35] *US Capability to Monitor Compliance with the Chemical Weapons Convention*, p. 37 and p. 81.
[36] *US Capability to Monitor Compliance with the Chemical Weapons Convention*, p. 59.
[37] The condition's full text is in *To Advise and Consent to the Ratification of the Chemical Weapons Convention, Subject to Certain Conditions, S. Res. 75*, US Senate, 105th Congress, First Session, 24 April 1997, pp. 7–14, at www.thomas.loc.gov.
[38] Some efforts have been undertaken in all of the following areas, but they should be expanded.
[39] Timothy V. McCarthy, *UN Verification and Strategic Denial and Deception: Iraq and Beyond*, Colloquium on Strategic Denial and Deception, Georgetown University, Washington, DC, 10 July 1999.
[40] See chapter by Andrew Rathmell in this volume.
[41] See chapter by Bhupendra Jasani in this volume.