CHEMICAL AND BIOLOGICAL WEAPONS TERRORISM: FORGING A RESPONSE [1]

The 11 September 2001 terrorist attacks in the United States changed fundamentally threat perceptions regarding the use of weapons of mass destruction by terrorists. The ability to use such weapons is all the more credible because sophisticated delivery systems are not required to conduct a terrorist attack. As a consequence, governments have reviewed longstanding plans to respond to terrorist incidents and have sought to identify weaknesses and address these where possible.

Effectiveness of the response may increase through international cooperation and coordination in a number of areas. Priorities should include sharing intelligence; improving cooperation among likeminded states; sharing information about national activities and programs, etc. Forging a coordinated response will require governments and counter-terrorist practitioners to produce relevant threat assessments, including chemical and biological (CB)-related threat in the context of all terrorist-related risks; to improve public information and relations strategies; to strengthen existing international arms control regimes; to improve fundamental public health care; to consider how regional approaches may best be developed; to ensure that plans to deal with an incident are tested through regular exercises, etc.

National Responses

National responses to the CB terrorism threat will inevitably be affected by countries' past experience with terrorism, the nature of their political system and existing national counter-terrorism plans and capabilities. Sharing information on the challenges faced by different countries and on their responses will enable those dealing with the problem to benefit from lessons learned.

***The US case*.** The US 120 Cities Program is designed to prepare 'first responders' (police, fire and medical staff) to respond to chemical, biological, radiological and nuclear (CBRN) terrorism. The program drew on existing Department of Defense (DoD) capabilities and experience and it was coordinated by the US Secretary of the Army. Training was given to local 'responders' in the use of detection equipment;

monitoring and prevention; protection of 'first responders' and the public; and decontamination. Key prerequisites for a successful response which were identified through conducting the program include: ensuring coordination at a very senior political level (e.g. the Secretary of Defense in the US); understanding that the improvement of 'national' (rather than local) capabilities is essential if a country is to be able to respond effectively; maximizing the convergence of all agencies and actors involved.

It is generally recognized, that in order to combat terrorism effectively, cooperation between agencies is essential both during and outside crises. This said, cooperation need not mean 'agreement' and it involves debate and strong differences of opinion. The need for debate must be balanced against the need for decisions to be taken. US counter-terrorism activity involves many agencies and programs: national security; biological weapons and related control regimes; US Homeland Defense issues. For example, Homeland Defense and biological weapons-related issues involve the Department of Defense, US allies, the Department of Transport, medical R&D agencies; various intelligence agencies, etc. Lead agencies for combating terrorism are the State Department (Overseas); the FBI (on US soil); FEMA (consequence management). The National Security Council plays a coordinating role on occasion, although its role post-11 September has yet fully to be clarified (as indeed is the case for other agencies).

Cooperation in this context prompts three difficult questions: who is in charge, who is to pay, whose interests are threatened by possible cooperation? Departmental competition for appropriations prompts strenuous efforts to defend related programs and expenditure and this may limit agencies' willingness to cooperate.

Additionally, the US response system has been enhanced by the newly-developed US Bio Defense Initiative that will also require high-level coordination and a lead agency to draw all related agencies and communities into the program. The newly-created Office of Homeland Security could be charged with this role, although it currently lacks the funding and command and control capabilities needed. However, the size of the US bureaucracy and interdependent responsibilities demand interagency cooperation to optimize results of national security programs in general, and counter-terrorism efforts in particular. A comprehensive national strategy is necessary to facilitate this cooperation while an effective program and budget oversight authority is required to ensure that this occurs.

The UK Experience. The United Kingdom Government has given overall authority for the coordination of counter-terrorism to the Home Office, which works in cooperation with the Foreign and Commonwealth Office, intelligence agencies, and other relevant departments. Implementation of legislation deriving from the Chemical

Weapons and Biological Weapons Arms Control Regimes rests with the Department of Trade and Industry (DTI).

Post-11 September, a review of UK policies has been undertaken. Themes of particular interest include: transport security, CBRN terrorism, suicide attacks, macro-casualty attacks, spectacular/concurrent attacks, crisis/incident management, consequence management, legal frameworks, policy/decision structures, public information structure, terrorist use/abuse of IT, threat perception. Dealing with the last issue pointed to a number of key requirements and problems as well as the need to:

- have multi-agency, trained, equipped and well-exercised 'first response' personnel;
- include risk assessment expertise;
- have effective command and control;
- establish a public 'help-line';
- have sufficient laboratory analysis capability to permit speedy identification of substances;
- divide 'initial' from 'first responders';
- train police, fire, and ambulance personnel to respond in a cooperative manner;
- provide coordinated accurate public information quickly; a media emergency forum is being established in the UK to bring crisis management personnel together with media 'leaders' to consider how best to deal with crisis situations in the future;
- develop and deploy equipment 'at street level' to detect BW as well as CW effectively in differing conditions and situations, etc.

UK experiences in dealing with suspect maritime cargoes (possibly including CW or BW) offer the pointers for future action such as: strengthening and correctly locating C2 facilities; giving further consideration to how best to locate and dispose of CBW; considering how best to involve 'new' partners in addition to the 'expected' agencies, e.g. maritime agencies and organizations, and related industries as source of potentially useful advice and support. Other lessons drawn from the UK experience include dealing with CBW as part of an overall and broader counter-terrorism effort; managing complacency, and maximizing interagency cooperation to protect the public and pursue terrorists. Additional key areas of concern include improving border controls; considering possible changes in the involvement of military forces in dealing with the problem; balancing the protection of society from physical danger

with the maintenance of human and civil rights of individuals; the maintenance or introduction of suitable oversight mechanisms.

EU and Europol Responses. The adopted response mechanisms have been designed not only for EU member states but also for candidate countries and other European neighbors. Cooperation efforts had to overcome differing political interests of member states vis-à-vis 'rogue' nations; lack of a common definition of terrorism and disagreements which organizations are 'terrorist'; lack of a common strategy (states seek to retain oversight of their essentially national reactions); different legal systems in different countries; lack of conformity of national approaches to crime fighting and counter-terrorism (e.g. police cooperation with the intelligence services is close in the UK but virtually forbidden in Germany); language problems and resulting associated bureaucracy.

Despite this, a common response to organized crime and terrorism has been developed. Measures agreed include: setting new tasks for Europol; developing closer police-security service cooperation between member states; increased harmonization of national laws; agreement on an EU Warrant of Arrest.

Efforts are underway to agree on a common approach to counter-terrorism. An operational crisis center has been established to work on a 24-hour-a-day basis to gather and research all available information and intelligence about terrorist attacks and related investigations in Europe. The Center facilitates operational analysis of data collected and the dissemination of key developments to expert contact points in member states. A counter-terrorist task force has been established. It includes experts from the law enforcement agencies of all EU member states and specialists from security services. An inventory list of anti-terrorism security measures has been provided by EU member states in the EU with the aim of helping them to compare their security measures, their assessments of the CBRN threat and to share best practices. A key goal has been to produce a threat assessment to help member states to calculate terrorist risks, including the risks associated with CBRN weapons.

The risk assessment reached the following conclusions:

- it is highly unlikely that terrorists could manufacture and detonate a nuclear device without assistance from a rogue state;
- a crude radiological dispersal device (dirty bomb) seems to be within the current capabilities of terrorist organizations and poses a realistic threat;
- BW and CW are unlikely to be already available to terrorist networks. If such weapons were available, the problems concerning transport and dispersion remain.

Problems to be addressed in the future include: providing adequate financial resources for Europol to undertake its new tasks effectively; recruiting more personnel; improving arrangements for information-sharing both within the EU and with the US; building on existing cooperative links with the UN, Organization for the Prohibition of Chemical Weapons (OPCW), EURATOM, and interested states; improving expertise on CB weapons to facilitate better contacts with other interested expert communities.

Israel's Way. The Israel-Palestinian conflict provokes a particularly intense interest in the issue of CB terrorism in Israel. As suicide bombers constitute the 'end point' of an organized activity, they need not be schooled in CBW-related knowledge which can be provided by planners and organizers elsewhere in the system. Israel's first priority remains to address the threat of war through deterrence, early warning, prevention, and active and passive defenses. This strategy has been adjusted to meet the threat of terrorism and the two are perceived to be closely linked not least because some WMD-capable states in the Middle East actively support terrorist groups.

The Israeli response is governed by three major principles: international cooperation (because the threat is global); prevention; mobilization of all national resources to meet the threat. International cooperation involves political-diplomatic activity; military security and technical cooperation; economic activities, legal issues, public education. It is intended to directly combat terrorists, undermine the infrastructure which supports them (whether states or international non-state actors as well as local organizations, labs, etc), change the culture which is supportive of terrorist activity.

Prevention is stressed because it preserves life, effectively marshals resources and prevents panic. It requires good intelligence, international cooperative action, effective combat capability, acting within the law, a 'layered' effort from borders to the High Street, understanding the terrorist mindset and anticipating unusual or novel methods of attack, monitoring what is going on in laboratories and universities and the activities of their personnel. Centralized responsibility for consequence management rests with the Ministry of Defense and its Home Front Command. Its mission is to support the civilian population during wartime and to prepare civilians for war during the peace. It coordinates activities of civilian organizations in wartime and prepares and trains them for this eventuality.

Maintaining a high degree of readiness is a central Israeli concern. C2 and coordination exercises are held regularly to ensure that those involved have a common approach to dealing with a crisis situation. Particular efforts have been made to prepare the medical system to deal with a CB event, which may come without warning and therefore require early detection if widespread casualties and/or infection are to be avoided. Much work has been done on public information and how

this affects public behavior in a crisis. A lack of information and instruction tends to generate panic. Therefore, sufficient, correct, reliable and authoritative information must be available in 'good time' to ensure effective control of a situation.

The Impact of New Technologies

Developing technologies are of particular use in threat assessment, e.g. surveillance and tracking of individuals and material, iris and palm scanning technologies to control entry to sites; risk assessment, e.g. assessing the likely impact of release of BW through mathematical modeling which will assist planning and decision-making; increasing general levels of security and the security of particular assets, e.g. aircraft, chemical loads in transport to be tracked by satellite, designing the structures of potential targets – for example CB plants – to maximize physical protection.

Technologies also have much to contribute if a CB event actually occurs. Chemical detectors are already available and deployed with police forces in a number of countries. Street-level detection of BW remains a 'holy grail'; the science already exists which permits the screening of a wide range of organisms and systems are already available commercially. Single-molecule detection is also technically possible. However, the challenge is to produce equipment which is easy to use, reliable, has no false alarms, and is usable in varied environments.

Technology can also facilitate clinical diagnosis and the protection of those affected. The design of vaccines 'to order' is now possible which will improve their effectiveness. Genetic screening will permit to identify individuals at risk and best able to respond.

'Cleaning up' after an event remains problematical as well, not least because the clean-up agents are themselves dangerous and toxic. Furthermore, a wide range of environments could be involved, each requiring differing attention and treatment.

Improving criminal detection methods is also a priority. DNA profiling is already a very powerful tool. It will have a vital role to play in dealing with BW release and the identification of strains and sources of material involved. The barriers to use technology in counter-terrorism include the high costs involved (requiring a 'weighing' of risk and perceived risk against cost); concerns about human rights and implications for individual freedoms; the need to ensure that they are working 'as advertised,' reliably, and with few or no false alarms; medical safety regulations and the need for testing.

The protection of advanced technologies is an important issue, for they may be used against society. However, cooperation will be difficult if technology is too protected, and some systems will need to be multilateral. Efforts to develop cooperation will

also be affected by concerns about fair trade and the maintenance of security of information collected on individuals.

It is possible for individuals to provide related information to terrorist groups. Apparently, there is lack of concern in industry about this and related issues. Therefore, it will be essential to establish effective control over organism design to ensure that the focus of work is on destruction of organisms rather than making them more toxic, etc., and make systems broadly focused to permit them to be updated and changed as needed. How to keep sensitive information secure will inevitably be problematical in the face of any drive for more scientific openness.

Technology will not offer a panacea for the counter-terrorist community. If properly handled, it will have much to contribute. It is important that developments be both technology- and user-driven; a dialogue between the two concerned communities is essential and must be regular and ongoing to ensure that the right sort of equipment is developed and deployed.

Intelligence Sharing

The interstate exchange of CBRN terrorism-related intelligence is problematic but encouraged by the nature of the threat, the size of the (possible or imagined) consequences, the focus on prevention, the need for technical know-how and shared inexperience. In turn, intelligence-sharing is required inside states between key organizations engaged in combating.

The difficulties of engaging in intelligence exchange include: the requirement to protect sources of information; diverging perceptions of the problem and agency interests; fears of a breach of confidentiality on the part of those to whom information is given; legal commitments; constraints and incompatibilities; the competence of those outside the intelligence agencies to handle the information provided, etc.

Facilitating cooperation within the country should take due account of the differing responsibilities and world views of the agencies involved. Intelligence agencies are policy-oriented and forward-looking and information has to be ‘good enough’ to feed into the policy-making process. In contrast, law enforcement agencies make considerable use of intelligence after an event has occurred, given their interest in securing convictions. Material has to be of sufficient quality to withstand the legal process and achieve convictions in a trial. In addition, it is likely that the ‘war on terrorism’ will not be an exclusively governmental enterprise; it will be necessary to involve the public, local police and industry to achieve success and how information is to be shared with these communities requires further consideration.

There is also the concern that the structures of national governments are ill-suited to deal with the new threat of international terrorism and the role of national militaries is outward-looking and less focused on internal defense roles and efforts which may need to be reexamined. Furthermore, the validation of information (ensuring its authenticity) as well as effective oversight of what is being shared, and with whom needs to be assured.

US domestic arrangements also point to future key requirements: dealing with the fact that many of the agencies and organizations which need to be mobilized lack any security clearance and fail to receive intelligence as a consequence; the need to improve the collection and analysis of domestic intelligence and to develop an overall strategy which is adaptable and flexible.

For a successful information exchange it is essential that information from whatever source is presented to others in a form which they can utilize effectively. Actually, some difficulties will not be solved and will remain part of the environment within which intelligence is shared and the war on terrorism is conducted in the decades ahead.

Information & Security

Notes:

[1] This is an excerpt of Wilton Park Conference (WP671, 22-24 March 2002) report, prepared by Dr. Richard Latter. The full text is available at http://www.wiltonpark.org.uk/web/conferences/reportprintwrapper.asp?confref=WP671.