

Testimony of
Michael Moodie
President
Chemical and Biological Arms Control Institute
To the
Subcommittee on International Security,
Proliferation and Federal Services
Committee on Governmental Affairs

7 November 2001

Mr. Chairman, Members of the Committee,

I appreciate the opportunity to appear before the Subcommittee as it addresses “Current and Future Weapons of Mass Destruction (WMD) Proliferation Threats” and considers the effectiveness of export controls in meeting the threat. My remarks are drawn from work conducted over the last six years by the Chemical and Biological Arms Control Institute (CBACI) on issues related to chemical and biological weapons and CBRN terrorism. My remarks today will focus on chemical and, especially, biological weapons threats.

I would like to address three inter-related issues: the need for better threat assessments; the linkage between state and non-state threats; and the need for a strategic response in which export controls continue to play an important role.

My starting point is the recommendation of the Gilmore Commission (The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction) that we must improve our threat assessments. This is true not only with respect to the threat of terrorism but also for the challenge of proliferation at the state level.

Traditionally, threat assessments have been overly simplistic. They have tended to focus on only a single factor such as the agent that might be used or the motivations of the state or terrorist who might use them. In addition, threat assessments have emphasized vulnerabilities rather than risks, which are a combination of vulnerability and likelihood.

The emphasis on vulnerabilities that derives from a focus only on a single factor such as the agent has several drawbacks:

First, vulnerability assessments, especially those focused on BW, portray dangers

that are virtually infinite. As a result they provide no criteria or metric against which to plan. The result is either policy paralysis in the face of an overwhelming challenge or pressure to commit enormous funds that will never be enough. Second, they foster worst case thinking that skews resources toward high-consequence, low probability contingencies. Third, vulnerability assessments transform “what ifs” into tangible contingencies. They provide no sense of whether what is theoretically possible in fact matches the reality of what is likely to happen.

An example of this kind of vulnerability assessment is one that often focuses on the agent smallpox. A scenario is posited that begins, “Assume a terrorist has smallpox...,” and it proceeds to describe events that lead to a global smallpox pandemic. While it is possible that use of smallpox could have such consequences, the assessment itself says nothing about the likelihood of such an occurrence. And yet, appreciating the likelihood of an event is critical to effective policy planning. Where, for example, would the terrorist get the smallpox initially? Unlike anthrax, smallpox is not present in nature since it was eradicated as an infectious disease by the World Health Organization. There are potential sources of smallpox, but the scenario of the kind posited above does not address the issue of acquisition. Would not the issue of availability have some bearing on the likelihood of that particular scenario and, hence, be of interest and concern to a decision maker?

Conducting more complex threat assessments is not easy. It demands good intelligence and creative analysis. But a better threat assessment will do three things. First, it describes a “threat envelope” that identifies the most plausible contingencies. Such contingencies may be far-reaching. We have tended to focus on smallpox and anthrax, for example, to the detriment of looking in detail at the implications of use of many other potential agents. These could include such traditional BW agents as plague or hemorrhagic fevers, simple agents such as salmonella, e-coli, or industrial chemicals, or more exotic possibilities that lie at the edge of advancing science and technology.

Second, it provides a means to identify those contingencies that require hedging, in that, due to the severity of their consequences, some preparation for them should be undertaken, even if they are relatively unlikely. The combination of the threat envelope and the hedging contingencies should give policy makers some measure for making decisions regarding policy priorities and resource allocations.

Third, a good threat assessment will highlight the fact that the threat is not unidimensional; rather, it is composed of several elements, including

Who: the actor—his motivations, intentions regarding casualties, and capabilities

What: the agent

Where: the target

How: issues regarding the mode of attack, such as the dissemination mechanism, and other operational considerations.

Each of these elements, in turn, entails a significant array of possibilities. The key to successful threat assessment is disaggregating the threat into these component elements and assessing the possibilities that various combinations of them produce. Some combinations of factors will yield significant consequences; others will produce no consequences at all.

Historical examples illustrate how the various elements that make up the threat interact to produce varying results. The Rajneeshis in Oregon in the mid-1980s, for example, combined the goal of incapacitating but not killing a significant number of people with a relatively common agent (salmonella) and simple delivery system (pouring the agent on salad bars) to produce a reasonably effective outcome (from their perspective). In contrast, the Aum Shinrikyo was motivated to take mass casualties, selected an appropriate target, and committed both considerable money and scientific effort to the enterprise. It only had access, however, to an attenuated strain of anthrax and its attempts to use biological weapons were totally unsuccessful.

This approach to threat assessment leads to important findings that should inform policy decisions.

First, a key relationship exists between the degree of risk and the level of casualties desired in an attack. This relationship, however, is not the straightforward one that higher risk is associated with catastrophic casualty scenarios. Indeed, the degree of risk declines as the level of desired casualties increases, insofar as it becomes less likely.

Second, despite the low probability of catastrophic attacks in the United States, there is still ample cause for concern because we do not know how “massive” a mass attack has to be. Worst-case scenarios need not happen to stress the response system to the point of collapse. It is unlikely that any regional or local response system, and perhaps even a national one, will be capable of dealing with an attack that produces catastrophic levels of casualties. But it is critical to raise the systems’ “breakpoints” by expanding capacity on a realistic basis to deal with low-to-middle size CBW incidents.

Moreover, the danger and harm inherent in the use of chemical and, especially, biological weapons is not limited to physical casualties. As we have seen with the anthrax attacks, psychological impacts and social and economic disruption are also

potentially severe.

Third, the connections between states with CBW programs and non-state actors warrant increased attention. State-sponsored terrorists are among the few actors who could assemble the requisite resources, skills, and materials to conduct a successful attack in the United States that produces mass casualties. Linkages between states and non-state actor could also take less direct forms, such as terrorists' employment of scientists who once worked in a state program.

The events of September 11 and the subsequent anthrax attacks suggest that the state-non-state actor connection is more important than ever before. Analysts have tended to conceptualize and address the state CBW proliferation challenge and chemical and biological terrorism along separate tracks. Today, however, we must appreciate that we confront a new challenge that is neither war nor terrorism as we have known them. The distinction between the two has become blurred; in fact, war and terrorism have become inextricably linked as has been demonstrated by the fact that Osama bin Laden has both depended on and provided support to various national governments. Our challenge is to see the problem as a whole.

We do not confront terrorism as we have witnessed it for the last 30 years, that is, the discrete use of violence to achieve defined, limited political objectives. Rather, our adversaries have declared war on the West, and the United States in particular, and they are using terrorist tactics as part of their campaign. And we confront an adversary that is not a state but, nevertheless, has chemical and biological weapons potential (at a minimum). State involvement, however, cannot be ruled out. Press accounts have raised the possibility that the anthrax used in the recent attacks can perhaps be linked to weapons programs in Iraq, the former Soviet Union, or some other states pursuing a CBW capability (including North Korea, Syria, or Libya). These reports may be true. But they still highlight the need to understand better the links between states and non-state actors who may be joined by a common interest in chemical and biological weapons.

As this war unfolds, then, the United States may find itself at war against one or more CBW-armed adversaries, whether state or non-state. How do they think about the strategic and tactical utility of chemical, and especially biological weapons? Their willingness to resort to such capabilities depends, of course, on their strategic objectives. Certainly, CBW's role in asymmetric strategies of adversaries who seek to avoid direct confrontations with overwhelming U.S. conventional military power is an important consideration. But saying CBW capabilities will be part of an asymmetric strategy is not enough. Different strategic goals point to different CBW uses. A number of alternative possibilities – each of which has both a limited and

ultimate form – suggest themselves as examples:

The desire to generate fear among the U.S. population, ultimately pushing such fear to the point that it raises questions about the integrity of U.S. society; slowing military action, or ultimately crippling U.S. strategies, for example, that depend on power projection and coalition warfare; or disrupting the U.S. economy, or ultimately undermining it by attacking such critical components as the agricultural sector (a threat that has received insufficient attention) or the financial centers of the country.

The importance of understanding the strategic objective, whether of the leadership of a terrorist group or of a nation-state, underlines the need for better intelligence about and analysis of the strategic cultures of our adversaries.

What does this approach to defining the threat suggest about the needs for responding effectively to that threat?

First, because the threat is multidimensional and complex, an effective response must be strategic in nature. Effective action depends on the existence of a strategy that – for both the military and domestic defense dimensions – defines the contribution of each individual tool of policy, relates them to one another, and integrates them in such a way that they all work together toward the achievement of defined goals and objectives.

A strategic response addresses requirements that span a spectrum: deterrence-prevention-defense-preparedness-response. Today, to perform each of these strategic missions effectively, difficult challenges must be overcome. Although there is a temptation to rely on deterrence, for example, because the problem has often looked too hard, the concept of deterrence cannot be translated easily from its Cold War context. We need to understand better the requirements of deterrence and how to do it in the current, more complex environment. Similarly, effective responses – whether on the battlefield or in terms of homeland defense – demand meeting both short-term needs such as adapting military concepts of operations or upgrading the public health systems, and long-term measures, including an effective research and development program.

Second, a strategic response is also a multifaceted response. A range of tools must be exploited. These include intelligence, defenses (both passive and active), diplomacy, legal measures, preparedness efforts, financial measures, and military options. Arms control is also important, but, particularly with respect to biological weapons, classic multilateral arms control (of the kind reflected in the Chemical Weapons Convention) is unlikely to yield significant results. The combination of

politics, science and technology, and treaty language that surrounds the Biological Weapons Convention (BWC) and efforts to negotiate a legally binding protocol to the BWC argue for an approach that goes beyond the traditional modalities of arms control to new ways of thinking about how to strengthen the Convention and the norm against BW which the treaty embodies.

Export controls also have an important role to play, but it is not necessarily the traditional contribution of the past. Export control regimes – which do not really control but rather regulate through licensing systems – can be effective in delaying the acquisition of sensitive technologies, but in the longer term they cannot realistically be expected to stop the transfer of technology that may be used for weapons purposes, particularly since so much of that technology also has legitimate commercial, medical, and other uses. If Iraq was capable of assembling the necessary materials and equipment for a robust CBW program as much as 15 years ago, how much more difficult will it be to deny access to technology to a determined player in an era of rapidly expanding knowledge and accelerating global dissemination of capabilities?

But this does not mean that export controls should be abandoned; they perform other functions. Regulation through export controls facilitates the global dissemination of materials and equipment. By defining the rules of the game by which companies must abide, for example, export controls is easier for those companies to engage in international trade and cooperation. As Brad Roberts, chair of the CBACI Research Council, has argued, export controls can, in fact, be trade enablers rather than trade constraints. It is this role for export controls that should be emphasized in the future. At the same time, the United States must maintain open markets and avoid neoprotectionist practices that deny or severely limit access to markets or appropriate technology which would make key states less inclined to pursue cooperative measures.

Each tool of policy contributes something to an effective response to the CBW proliferation challenge. But each tool also has shortcomings that must be overcome, and none of them constitutes a silver bullet that provides the total answer. Rather, for an effective response, the individual tools of policy – including export controls – must be integrated into a coherent strategic framework that realizes the synergies among the various tools of strategy, and facilitates tradeoffs among them so that they do not work at cross-purposes but maximize their potential contribution.

The CBW threat is not static and will continue to evolve. Changing actors and evolving technology – especially in biology-related areas – will be major drivers of

such change. In this fluid environment, like the offense-defense relationship in military affairs, the relationship between CBW proliferators – whether state or non-state – and responders is constantly in flux. It is not always possible to state precisely at any given time how the balance stands between them. The important point, however, is that certainty will only be achieved if we take ourselves out of the game and do nothing. Then we are certain to lose. It is not a loss that the nation or the world can afford.