Proliferation Papers

Dangerous Weapons in Dangerous Hands

Responding to the Challenges of Chemical and Biological Terrorism

In collaboration with the Atomic Energy Commission (CEA)

Michael Moodie

Summer 2009

ifri Security Studies Center

The Institut Français des Relations Internationales (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit organization.

As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience.

Using an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

With offices in Paris and Brussels, Ifri stands out as one of the rare French think tanks to have positioned itself at the very heart of European debate.

The opinions expressed in this text are the responsibility of the author alone.

ISBN : 978-2-86592-586-5

Ifri
27 rue de la Procession
75740 Paris Cedex 15 – FRANCE
Tel : 33 (0)1 40 61 60 00
Fax : 33 (0)1 40 61 60 60
Email : ifri@ifri.org

Ifri-Bruxelles
Rue Marie-Thérèse, 21
1000 – Brussels – BELGIUM
Tel : 32 (0)2 238 51 10
Fax : 32 (0)2 238 51 15
Email : info.bruxelles@ifri.org

Website : www.ifri.org

Summer 2009

Dangerous Weapons in Dangerous Hands

Responding to the Challenges of Chemical and Biological Terrorism

Michael Moodie

Proliferation Papers

Though it has long been a concern for security experts, proliferation has truly become an important political issue with the last decade, marked simultaneously by the nuclearization of South Asia, the weakening of international regimes and the discovery of frauds and traffics, the number and gravity of which have surprised observers and analysts alike (Iraq in 1991, North Korea, Libyan and Iranian programs or the A. Q. Khan networks today).

To further the debate on complex issues that involve technical, regional, and strategic aspects, Ifri's Security Studies Center organizes each year, in collaboration with the Atomic Energy Commission (CEA), a series of closed seminars dealing with WMD proliferation, disarmament, and nonproliferation. Generally held in English, these seminars are structured around the presentation of an international expert.

Proliferation Papers is a collection, in the original version, of selected texts from these presentations. An anonymous peer-review procedure ensures the high academic quality of the contributions. Download notifications are sent to an audience of several hundred international subscribers upon publication.

About the Author

Michael Moodie is an independent consultant on international security affairs, specializing in issues at the intersection of security, science, technology, and politics, especially biological and chemical weapons, terrorism, nonproliferation, the security implications of globalization, and the evolving conflict environment.

In the policy research community, from 1993 to 2005, he served as President of the Chemical and Biological Arms Control Institute (CBACI), a nonprofit research organization he co-founded. Under his leadership, CBACI became the first Washington "think tank" to focus on the nexus of CBRN weapons and terrorism. Mr. Moodie also led the Institute's ground-breaking study for the Centers for Disease Control on U.S. preparedness for bioterrorism.

Michael Moodie currently serves as Executive Editor of *WMD Insights*, an on-line publication focused on non-US perspectives on critical proliferation issues. He also holds the position of Director of Proliferation Issues for the Long-Range Analysis Unit of the *National Intelligence Council*. He is also an Associate Fellow in the International Security Program at the *Royal Institute of International Affairs* (Chatham House) in London and a Visiting Professor at George Mason University.

In government, Michael Moodie served from 1990 to 1993 as Assistant Director for Multilateral Affairs of the U.S. Arms Control and Disarmament Agency (ACDA). From 1983 to 1987, he was Special Assistant to the Ambassador and Assistant for Special Projects at the U.S. Mission to NATO. Mr. Moodie was educated at Lawrence University and the Fletcher School of Law and Diplomacy, Tufts University.

Contents

Introduction ____ 9

Looking Back and Looking Forward ____ 13

- Will the Future Look Like the Past? ____ 16
- The Challenge of Advancing Science and Technology ____ 17
- Other Key Science-related Trends ____ 21
- The Impact of Globalization ____ 22

New Dimensions of the CBW Terrorist Challenge ____ 27

- Intent and Capabilities: A More Complex Relationship ____ 27
- The Challenge of Terrorist CBW Campaigns ____ 30
- Amplifying a "Weapon of the Weak" ____ 30
- Coping with Uncertainty ____ 32
- Managing an Action-Reaction Cycle ____ 33
- Innovation, Adaptation, and Learning ____ 34
- Implications for Multiple Interests ____ 35

What Do We Do? Responding to CBW Terrorism ____ 41

- Foster Conceptual Shifts ____ 41
- Promote National Dialogue ____ 43
- Bolster Public Resilience ____ 43
- International Cooperation ____ 45

Introduction

The suicide of Bruce Ivins, a researcher at the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID), appears to have prompted the closing of the door on history's longest-running and most deadly case of biological terrorism. The Federal Bureau of Investigation has made it clear that it believes Ivins was responsible for the mailings of anthrax in the autumn of 2001 that led to the deaths of five people. Coming on the heels of the attack on the World Trade Center, the "Amerithrax" case reinforced perceptions among policy makers and the public alike that the United States was vulnerable to terrorist attack and that those attacks could entail the use of so-called "weapons of mass destruction," including chemical, biological, radiological, or nuclear (CBRN) weapons.

Growing concerns about biological weapons – as well as their chemical counterparts – coincided with the end of the Cold War. For the previous forty years, WMD issues were, not surprisingly, overwhelmingly focused on nuclear weapons. In the late 1980s and early 1990s, however, a number of developments raised the profile of chemical and biological weapons (CBW) for Western policy makers and security analysts. The three primary motivators were the chemical weapons dimension of the Iran-Iraq war and the subsequent worry about potential Iraqi CBW use during Operation Desert Storm, the 1992 conclusion of negotiations of the Chemical Weapons Convention (CWC), and the revelations from defectors regarding the massive, illicit, and unknown biological weapons (BW) program of the Soviet Union.[1] All these factors fostered legacies through the 1990s: the first provoked new attention to possible CBW use on the battlefield; the ratification of the CWC became a major hurdle for the Clinton administration and was not achieved until 1997; and the former Soviet Union's (FSU) CBW programs, combined with concerns about its "loose nukes," prompted Senators Sam Nunn and Richard Lugar to launch what became the Cooperative Threat Reduction Program to promote the safety and security of the FSU's WMD legacy.

Through the mid-1990s, CBW concerns focused almost exclusively on state programs. March 1995 changed that. The use of sarin gas in the

[1] For background on chemical weapons in the Iran-Iraq war, Desert Storm, and the CWC, see Jonathan Tucker, *War of Nerves: Chemical Warfare from World War I to al-Qaeda*, New York, Random House, 2007. For information on the impact of the Soviet defectors' revelations, see James Adams, *The New Spies*, London, Hutchinson, 2004; and Ken Alibek and Stephen Handelman, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World*, New York, Random House, 1999.

Tokyo subway by the Japanese cult Aum Shinrikyo, killing twelve people and injuring hundreds more, brought the prospect of CBW use by non-state actors to the fore. In the past, terrorist use of nuclear weapons had received very sporadic attention from analysts, but it had never risen very high on the policy agenda; terrorist use of chemical and biological weapons had garnered virtually no interest. The close proximity in time of the Aum's attack in Tokyo and the tragic bombing of the Murrah Federal Building in Oklahoma City, however, fundamentally altered that perspective. The conflation of those events in the minds of policy makers and the public fostered a view that became quickly widespread that the United States was no longer immune from terrorism, that terrorist attacks could involve WMD, and that, perhaps most importantly, should such an attack occur, the United States was not prepared to respond to it effectively. In terms of time and money, WMD terrorism soared up the policy agenda, a trend that was only intensified by the events of 9/11 and the "Amerithrax" attacks. Concerns about WMD terrorism have now become a permanent aspect of the nation's high priority fight against terrorism generally, and while the issue has moved off the front pages, at least for now, it continues to receive significant resources, both in terms of attention and financial support. While it is extremely difficult to identify precisely how much money the United States has spent in this arena over the last fifteen years, in the biological arena alone, estimates range from between $50 and $100 billion, just since 2001.[2]

Since the Aum Shinrikyo's attack fourteen years ago, policy makers and analysts have developed a much better understanding of the issues associated with potential terrorist use of CBW. They appreciate more deeply the historical context of the issues. They have parsed the technical details. They have elaborated a broad spectrum of useful and often innovative responses. So, considerable progress has been made.

Progress, however, does not equal success. Few experts would argue that either the United States nationally or the international community globally are where they should be with respect to baseline capabilities needed to be confident about an effective response to a WMD terrorist attack. Moreover, like much of the rest of the global security landscape, the issue is in flux, changing as the underlying factors that shape it continue to evolve. The challenge of CBW terrorism does not stand today where it did even a decade ago; like much of the international security environment, it has become more complex and uncertain. Complexity, uncertainty, and change are raising new questions and forcing new answers to old ones. While the level of understanding is much better than when the CBW terrorism problem first hit the headlines, no room exists for complacency.

[2] See, for example, Michael Moodie, *Fighting Bioterrorism: Tracking and Assessing U.S. Government Programs*, Washington, Chemical and Biological Arms Control Institute, 2004. This study estimated at the time – five years ago – that costs related to addressing the biological challenge already exceeded $50 billion. For a more recent, and more conservative estimate, see Crystal Franco, "Billions for Biodefense: Federal Agency Biodefense Funding, FY2008-FY2009," *Biosecurity, Bioterrorism, and Biodefense: Strategy and Practice,* Vol. 6, No. 2, June 2008, pp. 131-146.

Many issues related to CBW terrorism continue to be hotly debated, and new ones have yet to be assessed in detail. Much work – both conceptual and operational – remains to be done. This paper seeks to highlight some of those key issues that continue to need attention, such as the overlooked question of the stress created and challenges posed by terrorist conduct of CBW campaigns.

As a contribution to this work, this paper addresses three major themes. First, it considers the relationship between past and future, seeking to identify those elements in the evolving CBW terrorism problem that represent continuity with what has gone before and those dimensions that are new and pose novel challenges. Second, it highlights aspects of CBW terrorism that have not been examined in detail. In particular, it considers CBW terrorism campaigns, a dimension of the issues that, to date, has received inadequate attention. Such campaigns would pose a range of demanding political, social, economic, and security issues that must be better understood and for which policy makers and the public must be better prepared. Finally, the paper offers thoughts on an agenda for action, suggesting a number of efforts that could help to diminish the risks that lie ahead and manage them more effectively.

Looking Back and Looking Forward

One reason issues related to CBW terrorism continue to be hotly debated is the relatively small data base on which assessments can be conducted and from which conclusions can be drawn. Terrorists have made very few attacks, and even fewer have been "successful" in either causing fatalities (even in small numbers) or provoking panic. Among the cases that are usually cited are:

- The 1984 spreading of salmonella on salad bars in The Dalles, Oregon by members of the Rajneeshi cult;
- The 1995 Aum Shinrikyo sarin attack as well as the cult's efforts to develop and use biological weapons with anthrax and botulinum toxin;
- The 1990 Tamil Tigers chlorine gas attack against Sri Lankan military forces;
- The early 1990s attempt by the right-wing Minnesota Patriots' Council militia group to use the castor bean-derivative ricin against local government authorities;
- The fraudulent acquisition of the causative agent of plague by Larry Wayne Harris allegedly to conduct personal research on weaponizable pathogens; and
- The "Amerithrax" case.[3]

Although they yielded little or no result, each of these cases have received attention because they highlight different aspects of the issue: technical, financial, and organizational requirements, links between motives and means, sources and methods of acquisition, necessary levels of competence, ideological orientation or lack of it, ease or difficulty of attack, challenges in identifying an attack and the attacker, and several others.

[3] A number of other largely unsuccessful cases have also been assessed in some of the excellent analytical literature that has been produced on this issue since it became a focal point following the Aum attack, but they have not received as much attention as those cases cited in the text. See, for example, Jonathan B. Tucker, *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, Cambridge, MIT Press, 2001.

They also underline the broad range of entities, all with different priorities and perspectives, that comprise the spectrum of potential attackers, from groups to individuals, from cults to right-wing extremists to classic separatist insurgents or more novel eco-terrorists. Few if any of the major incidents, in fact, have been conducted by what terrorism experts would consider classic terrorist groups as they have been defined historically. No important examples of CBW efforts have come to light, for example, by such groups as the Irish Republican Army (IRA), Fatah or other Palestinian terrorist groups such as the Popular Front for the Liberation of Palestine (PFLP), the Baader Meinhoff Gang, the Red Brigades, the Japanese Red Army, or any other of the groups that provided the face of terrorism for most of the forty years following World War II.

The sparse yet multifaceted historical record has spawned extensive disputes over many aspects of CBW terrorism. No question has been more intensely debated, for example, than whether or not terrorists have the technical capability to conduct these kinds of attacks, and biological attacks in particular. Since Aum Shinrikyo's 1995 sarin gas attack on the Tokyo subway, the question has raged as to whether the Aum experience is representative or not. Some argue the Aum Shinrikyo is indeed representative of the difficult challenges that non-state actors face in trying to harness the life sciences and related technology. Others contend Aum was a unique case, a one-of-a-kind combination of profound bad luck and organizational dysfunction that will not be repeated.[4]

Some experts argue that terrorists are both unwilling and unable to exploit the life sciences. Milton Leitenberg, for example, says with respect to biological weapons that, "Advanced genetic engineering capabilities are not likely to become available to real world terrorist groups in the near future. Judgments based on the prevalence of genetic engineering competence in the general academic molecular research community are still not useful guides to terrorist capabilities."[5] Other commentators disagree – or at least are not so sure. One assessment contends, for example, that increasingly sophisticated practical knowledge related to the life sciences is available to many Advanced Placement Biology students in high school.[6] David Relman agrees, arguing that today, "anyone with a high school education can use widely available protocols and prepackaged kits to modify the sequence of genes or replace genes within a microorganism; one can also purchase small, disposable, self-contained bioreactors for propagating viruses and microorganisms." Relman concludes that the full potential of past programs was never unleashed, and BW use by small

[4] James A. Russell and Christopher Clary, *Globalization and WMD Proliferation Networks: Challenges to U.S. Security*, Report of a Conference sponsored by the Naval Postgraduate School, June 29-July 1, 2005, p. 9.
[5] Milton Leitenberg, *Assessing the Biological Weapons and Bioterrorism Threat*, Carlisle, Strategic Studies Institute, U.S. Army War College, 2005, p. 64.
[6] Robert Carlson, "The Pace and Proliferation of Biological Technologies", *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science,* Vol. 1, No. 3, 2003, p. 7.

groups historically was relatively unsophisticated and "far from representative of what moderately well informed groups might do today."[7]

Of course, having a basic scientific and technological capability does not necessarily automatically translate into having an effective chemical or biological weapon that can kill tens of thousands of people. That is why the debate exists. But the trends do suggest that rapid change in the environment is underway and that the future might not necessarily resemble the past.

Moreover, even if terrorists cannot exploit the most cutting-edge scientific and technological capabilities, it does not mean they can do nothing. Terrorists do not need the most advanced capabilities. They do not demand the same operational performance from their technology that militaries require.[8] Less demanding operational needs translate into less rigorous technical requirements. Their science and technology has to be just "good enough." One need only keep in mind the images of the devastation caused by the explosion at a chemical production facility in Toulouse, France in late 2001 to appreciate what could happen. The incident killed 30 people, including 10 individuals living in the neighborhood of the plant. It also razed the plant, destroyed 11,000 homes, damaged 16,000 additional structures, and generated monetary losses estimated to be at least $850 million.[9] Attacking a chemical facility that, like the facility in Toulouse, has tons of toxic chemical materials, is a more traditional terrorist operation than attempting to develop and disperse the agents themselves and may not involve as sophisticated and advanced capabilities.[10] The impact, however, need be no less devastating.

Analysts have tended to resort to a traditional lens through which to evaluate the problem. In fact, terrorists may seek to use such weapons for reasons that have little to do with casualty levels. Consider, for example, the contingency of a terrorist chemical attack against commercial shipping in the Straits of Malacca. If successful, such an attack would have the benefits for the group conducting the attack of high visibility, a demonstration of technological prowess, a well-defined target that yields little "collateral damage" and hence is not politically alienating to potential supporters, and potentially significant economic disruption, at least in the short-term.

Given this situation, Malcolm Dando contends that terrorists pose real threats even today, but that their current level of threat is likely to fall

---

[7] David A. Relman, M.D., "Bioterrorism: Preparing to Fight the Next War", *The New England Journal of Medicine,* Vol. 354, No. 2, p. 113.

[8] For more, see Gary A. Ackerman and Kevin S. Moran, "Bioterrorism and Threat Assessment", Paper No. 22, The Weapons of Mass Destruction Committee (The Blix Commission), November 2004, www.wmdcommission.org, p. 3.

[9] Margaret Kosal, "Terrorism Targeting Industrial Chemical Facilities: Strategic Motivations and the Implications for U.S. Security", *Studies in Conflict and Terrorism*, Vol. 29, No. 1, 2006, pp. 737-738.

[10] For discussion of the history of terrorist interest chemical facilities as targets, see *Ibid.*, pp. 719-751.

short of a mass-scale impact.[11] But terrorist threats at this level must not be dismissed, particularly since their potential impact could extend beyond a limited number of casualties to a more profound psychological effect. One must remember that only twelve people died in the Tokyo subway incident and only five fatalities resulted from the Amerithrax mailings. Yet, both of these incidents had a major psychological impact, and they prompted the expenditure of tens of billions of dollars. The U.S. government continues to invest significant amounts in biosecurity and biodefense. As only one example, the FY2010 budget request for the Department of Health and Human Services stood at $4.6 billion, an increase of $206 million over the FY 2009 request. This money is to be appropriated to the Public Health and Social Services Emergency Fund (PHSSEF). An additional $3.7 billion is requested outside the PHSSEF in appropriations for the Centers for Disease Control, the Food and Drug Administration, the National Institutes of Health, and other DHHS elements.[12]

Moreover, if concerns extend to cases that do not necessarily involve mass effects, the problem of "just good enough" technology is thrown into even sharper relief. Looking ahead, Dando further points out, "we face the threat in the coming decades of a much more systematic application of the new biology to hostile purposes… [I]n the future… it seems likely that sub-state groups, and perhaps even deranged individuals, may gain the capabilities to cause more human casualties."[13]

Will the Future Look Like the Past?

Some people take comfort from the historical record regarding chemical and biological terrorism. But should we expect the future to resemble the past? In most regards the future does not usually represent a clear break with things that have gone before; it does not typically offer discontinuities so profound that we have few, if any, landmarks by which to chart the way forward. The future is always a mixture of continuity and change. With respect to CBW terrorism, which of the two is likely to be dominant? Given the potential stakes involved and the adverse evolution of several trends, it is probably not wise to bet on continuity.

This challenge is especially noteworthy if policy makers make their focus the *risk* of CBW terrorism. Risk is the product of the severity of the consequences *if* something happens and the likelihood *of* it happening. Likelihood, in turn, is a function of the intent and capabilities of those who want to take those actions. Current trends are interacting in ways that affect all of these factors – consequences, intent, and capability. Together these trends are reshaping the nature of the CBW terrorism challenge, not least in creating novel dimensions to which policy makers must give more attention. These developments may not result in game-changing incidents next week or even next year. But if they are not examined and understood,

[11] Malcolm Dando, "Bioterrorism: What is the Real Threat?", *Risk Case Studies*, Nuffield Trust Global Programme on Health, Foreign Policy and Security, p. 3.
[12] Department of Health and Human Services, "FY2010 Budget Brief," May 2, 2009, pp. 108-109.
[13] Malcolm Dando, "Bioterrorism: What is the Real Threat", *op. cit.*, p. 35.

policy makers are likely to awaken one day to an unfamiliar environment in which the dynamics are unrecognizable, the options uncertain, and the policy approaches and tools on which they relied in the past largely irrelevant.

Two factors are especially important in shaping this more complex and uncertain challenge: 1) advances in science and technology that are creating new and sometimes unforeseen opportunities and options for potential adversaries and 2) the process of globalization, which is already profoundly altering CBW dynamics.

The Challenge of Advancing Science and Technology

The world is witnessing a life sciences revolution. An explosion in knowledge about the processes of life at the molecular level is underway. The speed of advance in certain branches of the life sciences is remarkable, moving faster even than Moore's Law that describes the incredible velocity of change in information technology.[14] As a result, many people are suggesting that biology will have as big an impact on the 21st century as information technology had on the 20th.

The heart of this revolution is genomics, the growing ability to manipulate genes. It does not stop there, however, but extends to proteomics, the study of proteins, as well as systems biology and brain and cognitive science.[15] An area that has received particularly strong attention in the last few years is synthetic biology, which has been described as "another transformative innovation that will make it possible to build living machines from off-the-shelf chemical ingredients, employing many of the same strategies that electrical engineers use to make computer chips…[S]ynthetic biology envisions the redesign of natural biological systems for greater efficiency, as well as the construction of functional genetic circuits and metabolic pathways for practical purposes."[16] If the goals of those who advocate synthetic genomics are achieved, biology will be "translated from a science into an engineering platform with standardized parts, devices, and systems engineering manuals."[17]

The speed at which the life sciences and associated technologies are translated into "commodities" is also increasing. Many governments around the world see biotechnology as a key driver of their future economic growth, and developments such as those in synthetic biology demonstrate

[14] Robert Carlson, "The Pace and Proliferation", *op. cit*., pp. 1-3.
[15] It is particularly interesting that China's president, Hu Jintao, has indicated that brain and cognitive science will be one of that country's next scientific research frontiers. National Research Council, *Globalization, Biosecurity, and the Future of the Life Sciences* (hereafter NRC, *Globalization)*, Washington, National Academies Press, 2006, p. 115.
[16] Jonathan B. Tucker and Raymond A. Zilinskas, "The Promise and Perils of Synthetic Biology", *The New Atlantis*, No. 12, Spring 2006.
[17] Anne G. K. Solomon, "Introduction", in Anne G.K. Solomon (ed.), *Technology Futures, and Global Power, Wealth, and Conflict,* Washington, Center for Strategic and International Studies, May 2005, p. xviii.

how rapidly people are looking to transform cutting edge science into increasingly standardized commercial products. One example of this "commoditization" is the worldwide explosion of "gene foundries" whose goal is to provide made-to-order DNA segments on request – for profit.[18]

This accelerating rate of change combines with the surprise inherent in scientific discovery to generate phenomena that are unexpected and even unknowable. A National Research Council study makes the point that scientific progress in the 20th century was marked by successive serendipitous discoveries that in some cases forced the complete revision of our understanding of natural phenomena. The life sciences, then, will continue to advance quickly, in a variety of directions, and "new and previously unanticipated paradigm shifts are very likely to occur…"[19]

Innovation in the use of technology is also important in that it can promote technological surprise. That technology need not be cutting edge, but could be what Paul Bracken calls "sidewise technology," older technology whose use is innovative with respect to processes, areas of application, or hitherto unforeseen combinations.[20] This point leads to the important realization that devastating harm need not come only from state-of-the-art chemical or biological technology or techniques, but that modest levels of capability can, especially if used in unexpected ways, foster considerable damage.

Another aspect of scientific and technological trends that will have a major impact is the convergence of various scientific fields. Dramatic advances are made possible often as a result of the interaction of different disciplines. As Alexander Kelle has noted, "many of the products flowing from the biotechnology revolution… are basically chemical compounds."[21] A *Nature* magazine survey of leading chemists resulted in a clear consensus that many of chemistry's most urgent questions are ones that address aspects of biology.[22]

The increasingly blurred lines between biology and chemistry are especially apparent in new processes for drug discovery using combinatorial chemistry and high-throughput screening to generate significant numbers of potentially highly toxic chemical compounds. While

---

[18] See, for example, Emily Singer, "DNA Factories", *Technology Review*, April 4, 2007, and Rob Carlson, "Global Distribution of Commercial DNA Foundries", *Synthesis*, http://synthesis.typepad.com/2005/07/global_distribu.html.

[19] NRC, *Globalization*, *op. cit.*, p. 25.

[20] Paul Bracken, "Sidewise Technologies: National Security and Global Power Implications", in Anne G.K. Solomon (ed.), *Technology Futures, op. cit.*, pp. 91-100.

[21] Alexander Kelle, "The Changing Scientific and Technological Basis of the CBW Proliferation Problem", *Bradford Science and Technology Reports*, No. 7, University of Bradford, 2007, p.7.

[22] For example, Stanford University physical chemist Richard Zare commented, "To me, the big unanswered question concerns the chemistry of life processes." Philip Ball, "What Chemists Want to Know", *Nature*, Vol. 442, No. 7102, August 3, 2006, p. 501.

these results may be rejected as the basis for new drugs, information about these toxic substances is maintained in corporate or other databases. Were those interested in doing harm able to access such information, they may be able to identify new opportunities.

Equally important is the convergence of biology and chemistry with other scientific and technological disciplines, particularly information technology, materials science, nanoscience and nanotechnology, as well as imaging and sensor technology. This convergence is creating new fields such as "bioinformatics" and "bionanotechnology." These new areas of study are also combining with other technology-related trends and patterns such as automation and miniaturization. In the minds of some people, the result of this process of convergence is a transformation potentially "as powerful as the industrial revolution."[23]

The National Research Council report summarized these developments by combining the advancing life sciences and related technology into four categories of advances that "share important features that are relevant to their potential to contribute to the future development of biological weapons":

- Acquisition of novel biological or molecular diversity.
  E.g., DNA synthesis, DNA shuffling, high throughput screening
- Directed design
  E.g., Synthetic biology, genetic engineering of viruses
- Understanding and manipulating biological systems
  E.g., Systems biology, RNAi, bioinformatics
- Production, delivery, and "packaging"
  E.g., microfluidics, nanotech, aerosol tech, gene therapy techs[24]

All of the manipulations that characterize this work are already underway in research programs conducted for legitimate purposes, and they are interacting with one another in ways that could yield significant synergies.[25]

These trends are combining to alter one's understanding of what constitutes a chemical or biological weapon, and to increase the potential range of options available to those who want to do harm. Biological weapons were traditionally defined in terms of living organisms (or the chemical byproducts of living organisms, i.e., toxins) found in nature that caused diseases in people as well as in plants and animals. Traditional agents (e.g., smallpox, anthrax, tularemia, plague, botulinum toxin) cannot be dismissed – as the experience with the anthrax letters in 2001 so clearly underlines – but today, other possibilities are also emerging.

[23] NRC, *Globalization*, *op. cit.*, p. 195.
[24] *Ibid*., pp. 139-213.
[25] *Ibidem*., p. 155.

One dimension of this expansion is the potential to use new science – particularly genetic engineering – to enhance traditional CBW agents. Many discussions can be found of how advanced techniques might be exploited to bolster the pathogenicity or virulence of an organism, allow for the transfer of antibiotic resistance, boost its aerosolization, or shore up its stability. Moreover, someone interested in doing harm need not look to nature as the source for such organisms; science is increasingly making it possible to synthesize them artificially.

A second way in which the spectrum of options is expanding is through the growing ability to recover organisms from old tissues, as was the case with the 1918 Spanish influenza. Third, natural selection will complicate the challenge. The World Health Organization (WHO) reported almost a decade ago that more than 30 new infectious diseases threatening to human health have appeared in the last two decades, and even more new microbial diseases are likely to emerge over the next two, as the current "swine flu" so graphically reminds us. [26]

Concerns have also emerged that "future biological agents could be rationally engineered to target specific human biological systems at the molecular level."[27] These advances would allow BW developers "to identify biochemical pathways critical for physiological processes and engineer specific [advanced biological weapons] agents to exploit vulnerabilities… [Such agents] will be able to target specific biological systems, such as the cardiovascular, immunological, neurological, and gastrointestinal systems… and produce a wide range of effects including death, incapacitation, or neurological impairment."[28] Some people even see the prospect of ethnically targeted weapons as drawing closer.[29] The concept of biologically-related threat agents, therefore, must now go beyond "bugs," or disease-causing microbes, to include substances such as bioregulators that make it possible to manipulate behavior or thought processes.[30]

According to one study, the result of this growth in potential BW options is "a diffuse and fundamentally unknowable range of potential agents."[31] A 2003 unclassified CIA report on the possibilities of these "advanced biological agents" concluded dramatically that the "resulting

---

[26] Michael Moodie and William J. Taylor, *Contagion and Conflict: Health as a Global Security Challenge*, Washington, Center for Strategic and International Studies, 2000, p. 3.

[27] James B. Petro, Theodore R. Plasse, and Jack A. McNulty, "Biotechnology: Impact on Biological Warfare and Biodefense", *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, Vol. 1, No. 3, 2003, p. 162.

[28] *Ibid.*

[29] The Sunshine Project, "Emerging Technologies: Genetic Engineering and Biological Weapons", *Background Paper*, No. 12, November 2003, http://www.sunshine-project.org/publications/bk/bk12.html, pp. 11-16.

[30] See, for example, Mark Wheelis and Malcolm Dando, "Neurobiology: A Case Study of the Imminent Militarization of Biology", *International Review of the Red Cross*, Vol. 87, No. 859, September 2005.

[31] Kathryn Nixdorff, Neil Davison, Piers Millett, and Simon Whitby, "Technology and Biological Weapons: Future Threats", *Bradford Science and Technology Reports*, No. 2, University of Bradford, 2004, p. 1.

diversity of new BW agents could enable such a broad range of attack scenarios that it would be virtually impossible to anticipate and defend against."[32]

A second aspect of this changing concept of a chemical or biological weapon relates to delivery systems. As the NRC study points out, the materials, equipment and technology for "disseminating and delivering the agent to their intended recipient(s) are equally, if not more important than the agents themselves in terms of their dual use risks."[33] The standard notion of "delivery" has evolved from the military context in which traditional munitions and missiles were the primary means for putting CBW "on the target." As a result of various scientific and commercial efforts, however, such as those to find new mechanisms for drug delivery (e.g., cutaneous absorption and improved aerosolization), potential new BW delivery systems may also become available. In many cases, the new devices are intended for drug delivery to individuals, and are therefore probably not suitable for "mass effect" applications. In a context in which the perceived utility of certain chemical and biological weapons uses is changing, however, such limited impact should not be denigrated. But thus far policy makers and analysts have paid insufficient attention to this point, focusing instead on the agents themselves. These developments must not be ignored.

Other Key Science-related Trends

It is not just the science and technology itself that is shaping the evolving environment; the way that science is conducted is also an important feature. Today, for example, key scientific advances are rarely reported by individual scientists, but by teams of collaborators. As a result, alliances, partnerships, and other forms of collaboration are increasingly important. Moreover, given that the life sciences enterprise has achieved global proportions in both science and commercialization, more and more of these cooperative relationships, whether they are among companies or individual scientists, occur across international borders. Myriad examples could be cited: Cuba has technical agreements with at least fourteen countries, including Algeria, Brazil, China, India, Iran, Malaysia, Mexico, and Tunisia; a trilateral forum with Brazil, India, and South Africa fosters dialogue on critical biotechnology issues;[34] the Economic Cooperation Organization, created initially by Turkey, Iran, and Pakistan and which now includes a number of other central Asian states, is creating an Agricultural Biotechnology Network hosted by Iran;[35] and the South African Bioinformatics Initiative is not only seeking to connect researchers at national universities, government facilities, and startup private

[32] Central Intelligence Agency, "The Darker Biological Weapons Future", November 3, 2003, p. 2.
[33] NRC*, Globalization*, p. 48.
[34] "Science and Technology Minister Discusses Nuclear, Space, and Other Priorities", Open Source Center, original published in *Brasilia InfoReal* in Portuguese, April 6, 2006.
[35] "Experts Meet in Tehran for Establishment of ECO Agricultural Biotechnology Network", Islamic Republic News Agency, April 25, 2006.

biotechnology firms, but to provide access to state-of-the-art bioinformatics throughout the African continent.[36]

A second important trend is the emergence of *clusters*. Biotechnology clusters might be described as geographic concentrations of interconnected companies, specialized suppliers, service providers, firms in related industries, and institutions (for example, universities, standards agencies, and trade associations) in particular fields that compete but also cooperate. Clusters represent networks based on physical proximity. They are driven by the appeal of both "learning by interacting" and sharing knowledge on best manufacturing or laboratory practices as well as by the cost reductions resulting from jointly sourcing services and supplies. Biotechnology clusters appear almost everywhere in the world, even in Africa. In many places, developing countries in particular, they may be small, but what is noticeable is that, common to all of them, biotechnology companies have direct associations with university-based research and development.[37]

The Impact of Globalization

The second major trend shaping the future landscape within which CBW terrorism could occur is globalization, which is characterized by inter-relationships and transactions that are distinguished by their worldwide scope, accelerating speed, growing magnitude, thickening density, and increasing complexity. The general impact of globalization is hard to exaggerate. The National Intelligence Council study of the trends and factors shaping the world of 2020, for example, called globalization a "force so ubiquitous that it will substantially shape all the other major trends," and argued that the magnitude and speed of change fostered by globalization will itself be a defining feature of the future.[38]

The life sciences have felt the impact of globalization as much as any other endeavor. The chemical industry has been a global enterprise for decades, but the explosion in the number of biotechnology enterprises around the world is more recent. Its global dimensions are almost endless:

- India already has the twelfth largest biotechnology sector in the world as measured by the number of companies,[39] and New Delhi's

[36] Helen E. Purkitt, "Biowarfare Lessons, Emerging Biosecurity Issues, and Ways to Monitor Dual-Use Biotechnology Trends in the Future", *INSS Occasional Paper*, No. 61, U.S. Air Force Institute for National Security Studies, September 2005, pp. 40-41.
[37] John Mugabe, "International Trends in Modern Biotechnology: Entry by and Implications for African Countries", *ATPS Special Paper Series*, No. 15, African Technology Policy Studies Network, 2003, p. 6.
[38] National Intelligence Council, *Mapping the Global Future*, A Report of the National Intelligence Council's 2020 Project, December 2004, p. 10.
[39] Nandini K. Kumar, Uyen Quach, Halla Thorsteinsdottiir, Hemlatha Somsekhar, Abdallah S. Daar, and Peter A. Singer, "Indian Biotechnology – Rapidly Evolving and Industry Led", in *Health Biotechnology Innovation in Developing Countries*, p. DC31. See also, Parveen Arora, "Healthcare Biotechnology Firms in India:

Department of Biotechnology hopes to expand India's biotechnology sector five-fold in five years, creating ten new biotechnology parks by 2010.[40]

- Singapore has created "Biopolis," a research and industrial park dedicated to the life sciences where both government and private sector research and development will occur.

- In Brazil, the number of biotechnology companies increased from 76 in 1993 to 354 in 2001. Today, the Brazilian government claims there are as many as 1,700 groups in the public, academic, and private sectors working on biotechnology,[41] and the Brazilian government has pledged $479.5 million for future biotechnology research.[42]

- In 1995 Mexico adopted a plan to establish and develop a genomic medical platform, including creation of a new Institute of Genomic Medicine that it hopes will become a model for wider adoption throughout Latin America.[43]

- In the Middle East, an area generally considered to be behind in biotechnology, Egypt now has more than three thousand scientists active in biological research fields, and it directs $100 million annually to biotechnology research and development projects.[44]

- South Africa hopes to use regional initiatives, such as its New Partnership for African Development, as a springboard to make it the biotechnology leader in Africa.[45]

Globalization has transformed patterns of industrial production at both national and international levels, including in life sciences industries. Together with new production processes, agile manufacturing, miniaturization, lower technology costs, and increased productivity of a global talent pool, these trends are restructuring business enterprises in fundamental ways, such as creating flatter organizational pyramids with more empowered employees.

Another important trend might be called the global "diffusion of knowledge," which, in the life sciences can be seen in a number of different ways. More players, for example, are becoming scientifically productive.

Evolution, Structure and Growth", *Current Science*, Vol. 89, No. 3, August 2005, pp. 458-463.

[40] David Kang and Adam Segal, "The Siren Song of Techno-nationalism", *Far Eastern Economic Review*, March 2006, http://www.feer.com/articles1/2006/0603/free/p005.html.

[41] "Brazil to Seek Global Leadership in Biotechnology", Brazil-Arab News Agency, February 8, 2007.

[42] *Ibid*.

[43] National Research Council, *An International Perspective on Advancing Technologies and Strategies for Managing Dual-Use Risks: Report of a Workshop*, 2005, p. 6.

[44] Mugabe, *International Trends in Modern Biotechnology, op. cit*., p. 10.

[45] Helen E. Purkitt, *Biowarfare Lessons, op. cit*., pp. 40-41.

The United States continues to lead in the production of academic papers, but the percentage of such papers authored by U.S. scientists has declined while increases have occurred elsewhere. Scientists from states such as China and Turkey, for example, have boosted their academic scientific output by twenty to thirty percent.[46]

Another measure of the diffusion of knowledge relates to the dispersion of expertise. One important trend in this regard is the increase in the number of students trained in the United States who are returning to their home countries, frequently induced to go back by government incentives promoting an appealing quality of life. From a security perspective, this mobility could pose a challenge if scientists who received their training from Western academic and other scientific institutions participate in illicit WMD-related activities.

Another point to make about this pattern is that fewer of the most talented foreign-born scientists and engineers are studying in the United States. Competition for the best scientific and engineering scholars is now global, including institutions even in developing countries. In most of South Africa's major research universities, for example, foreign students in graduate programs comprise an even larger percentage of the student body than they do in the United States. The impact of this trend in the security arena, according to one analyst, may be that it will foster programs in which many of "tomorrow's BW scientists will be trained in non-Western institutions in Asia, Latin America, and Africa."[47]

Finally, the growth of the international scientific community underlies the fact that globalization has spurred the emergence of non-governmental entities operating on a global basis. The impact of this growth and diversity is to increase the number of channels within and among societies through which action can be taken and influence exerted. More and more these increasingly empowered non-state actors are able to express their singular interests through the tools and channels globalization provides, allowing them to operate beyond the control of any single government. The result is that even relatively weak actors can have disproportionate impact both positively and negatively.

This changing scientific and technological landscape has critical implications for security. The accelerating pace of discovery in the life sciences and the widespread diffusion of the life sciences and related technology around the globe have fundamentally altered the CBW risk spectrum, which is now exceptionally broad and continually evolving:

- The number of regions of the world where people can be found with the requisite ability to exploit knowledge that can do harm has obviously grown significantly. That people might know how to apply this knowledge for malign purposes does not, of course, mean automatically that they will. An increase in the number of people

[46] NRC, *Globalization, op. cit.*, p. 99.
[47] Helen E. Purkitt, *Biowarfare Lessons*, *op. cit.*, p. 34.

with the requisite knowledge, however, does imply an increase in the burden of potential risk that must be managed.

- These trends have created lower entry costs for getting into the CBW business as well as the potential to enter that process at a higher point on the learning curve.

- The new structures of commercial and scientific enterprises will provide a wider range and more diverse array of legitimate dual-use covers for malign activities. They could also create multiple, parallel, possibly non-traditional pathways to the development of critical biological or chemical weapons-related capabilities.

In such an environment, serious challenges exist with respect to governments' abilities to oversee, control, and prevent prohibited behaviors. Government bureaucracies are notoriously slow to adapt. So too are international institutions. How then can governments and international institutions keep pace with the speed at which science and technology is moving, with the growth in the number of people who have access to it, with the flexibility of the networks through which those people act, and with the geographic scope across which they operate? In other words, how does one manage the risks attached to the possible use of chemical and biological weapons in a world in which key actors, including, and perhaps especially terrorists, through the diffusion of science and technology developed for legitimate purposes, are coming closer to at least a "virtual" chemical and biological weapons capability?

This is not to argue that "virtual" capabilities will inevitably translate into highly effective weapons. Yet, it is important to recognize that developing CBW capabilities is potentially easier today than it was in the past, and it is harder today than it will be in the future. Still, the question remains: Will non-state actors be able to overcome the barriers that will continue to inhibit development of such capabilities? One would be foolish to give a definitive "yes." But, given the trends suggested here, one should take little comfort that the future will necessarily resemble the past.

A related issue that has been the subject of concern is whether states will ever help terrorist groups overcome the barriers they encounter in their search for unconventional weapons capabilities or even sponsor terrorists in a CBW (or other) attack. Given the minimal historical record, on this question, too, almost no data is available. Like many others related to CBW terrorism, it can be approached only with considerable speculation.

The issue of state sponsorship of terrorism in general is complex, suggesting both potential benefits and costs for both sides. From the terrorist viewpoint, for example, facilitation of its efforts by states and greater tactical flexibility that may result has to be balanced against the prospect of greater state-imposed constraint and control. A similar calculus of possible gains and complications is also in play for the states themselves.

In terms of CBRN, the leverage rests almost exclusively with the potential state sponsor, and the balance of expert opinion seems to be that for potential state sponsors, the costs outweigh the possible benefits. With respect to sharing nuclear capabilities, for example, Brian Jenkins points out in his book, *Will Terrorists Go Nuclear?*, that governments are not about to hand over their crown jewels to organizations that "are not entirely under state control" whose reliability "is not certain." Second, "giving them a nuclear weapon almost certainly exposes a state sponsor to retaliation."[48] This position was reinforced by U.S. Defense Secretary Robert Gates in a speech to the Carnegie Endowment:

> The United States will hold any state, terrorist group, or other non-state actor or individual fully accountable for supporting or enabling terrorist efforts to obtain or use weapons of mass destruction – whether by facilitating, financing, or providing expertise or safe haven for such efforts. To add further to the deterrent goal of this policy, we are pursuing new technologies to identify the forensic signature of any nuclear material used in an attack – to trace it back to the source.[49]

Without question it would be more difficult to trace the origin of a biological or chemical weapons terrorist attack back to a state sponsor. If that were the only reason that states do not provide such capabilities to terrorists or support their CBW efforts, the prospect of anonymity may be enough to at least bring them to consider the possibility. Yet, some risk of being identified as the source does exist, and even a small chance may be deemed too risky. Moreover, risk of exposure does not appear to be the only reason they have thus far refrained from promoting CBW-related terrorist activity. Some of the same concerns Jenkins notes for the nuclear dimension may also hold for potential sponsors with respect to CBW capabilities, particularly the lack of total control of both the terrorist group and the weapons as well as their uncertain reliability. In addition, CBW terrorist attacks may not serve the potential state sponsors tactical or strategic interests, which may be satisfied just as readily with conventional terrorist tools.

[48] Quoted in Peter Bergen, "Commentary: WMD Terrorism Fears are Overblown", CNN, December 5, 2008.
[49] Secretary of Defense Robert M. Gates, "Speech to the Carnegie Endowment for International Peace", October 28, 2008, http://www.defenselink.mil/speeches/speech.aspx?speechid+1305.pdf

New Dimensions of the CBW Terrorist Challenge

Intent and Capabilities: A More Complex Relationship

If CBW capabilities are potentially coming within the grasp of terrorists at an accelerating pace, the issue of intent becomes more important. In this context, Brian Jenkins has made the important point that "terrorists have not fulfilled our (or their) darkest fantasies. Despite the appearance of mass destruction scenarios in books, broadcasts, and screenplays for 30 years, terrorists have not tried to implement most of those scenarios. Why?"[50]

The reasons that terrorists might refrain from a particular course of action are many: morality, self-image as a legitimate military combatant, fears of provoking deadly backlashes, risks of tactical failure, perceptions of high technical difficulty, concerns about group cohesion and the need to prevent fragmentation, and worries about perceived constituents. In the case of CBW, the technical difficulties have already been mentioned, although differences of opinion exist as to how strong such constraints will remain in the face of scientific and technological advance. Do any other constraints hold?

History demonstrates that a variety of non-state actors have shown interest in chemical and biological weapons. As pointed out earlier, however, most groups to do so have not been traditional terrorists, but millenarian-motivated groups or cults, the right-wing U.S. militia movement, or loners. This has led some analysts to suggest that it is largely only those groups who do not perceive or perhaps accept that they are subject to political, social, or moral constraints, who are more likely to be interested in CBW.[51] Hence, they suggest the likelihood of CBW use is even further diminished because such groups are few in number and those that do exist are not likely to enjoy the technical, organizational, or financial wherewithal for such operations, even if they would like to.

---

[50] Brian Michael Jenkins, *Unconquerable Nation: Knowing the Enemy, Strengthening Ourselves*, Santa Monica, RAND Corporation, 2006, p. 11.

[51] See, for example, Jonathan B. Tucker, *Toxic Terror*, *op. cit*. See also Gary Ackerman, "CBRN Terrorism: Motives and Malefactors", presentation at the DHS University Network Summit, 2007, www.orau.gov/dhssummitt/2007/Presentations/Ackerman.pdf.

In this regard, al Qaeda poses an interesting case. For some analysts, al Qaeda falls squarely into the millenarian category with its rhetoric of accountability only to Allah and its goal of a global Caliphate.[52] Other analysts do not necessarily lump al Qaeda with Aum Shinrikyo or the Rajneeshis, however, but place them in a category of essentially post-modernist terrorists who exploit all of the tools globalization provides (including science and technology) to conduct operations with global impact that are not seen by its leadership through traditional political, social, or moral lenses but are informed nonetheless by some sense of such factors.[53]

Both groups of analysts suggest that al Qaeda's documented interest in CBW should not be surprising. Al Qaeda's leadership, and Osama bin Laden in particular, has developed an elaborate rationale to justify the use of such capabilities, perhaps because the question of CBW use is not necessarily fully accepted by the broader Islamic community, including its religious leadership.[54] Its interest in CBW capabilities has been publicly articulated by second-in-command Ayman al-Zawahiri and others, and attempts to acquire and use materials and equipment have been reported.[55]

Zawahiri's oft-cited comment that al Qaeda was not especially focused on biological weapons until witnessing then Secretary of Defense William Cohen's discussion of the problem with a bag of sugar as a prop underlines an important insight into the increasingly complex relationship between capability and intent. Conventional wisdom holds that "intent drives capability," in that an actor first will decide that a CBW capability would be of value and then takes steps to acquire it. The Zawahiri comment suggests that another dynamic may also be at work, that is, that "capability shapes intent," insofar as awareness of what advancing life sciences may make possible apparently could drive the decision at least to explore what the group might be able to accomplish if it successfully acquired such a capability.

Al Qaeda is not the only terrorist group to demonstrate an interest in CBW. In 2004, for example, in the southern Philippines a police raid on the house of an alleged operative of the Indonesian group Jemaalia Islamiyah

---

[52] See James F. Rinehart, "The Millenarian Ideology of al Qaeda", Paper presented at the annual meeting of the International Studies Association, San Diego, March 2006, www.allacademic.com/meta/p_mla_apa_research_ictation/1/0/0/2/9/pages100291/p100291-1.pdf.

[53] See, for example, Bruce Hoffman, "CBRNB Terrorism Post-9/11", Research Brief, Jebsen Center for Counterterrorism Studies, Fletcher School of Law and Diplomacy, Tufts University, 2007 http://fletcher.tufts.edu/jebsencenter/researchbrief/JCCTS_Hoffman_CBRN_01-2007.pdf See also, Jean Guillemin, *Bioterrorism and the Threat of Proliferation: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism*, New York, Columbia University Press, 2005, pp. 159-160.

[54] For a detailed discussion of that rationale, see Lewis A. Dunn, "Next Generation Weapons of Mass Destruction and Weapons of Mass Effect Terrorism"*, ASCO Final Report*, Defense Threat Reduction, January 31, 2008.

[55] *Ibid*., p. 3.

(JI) discovered a JI training manual on chemical and biological terrorism.[56] In addition a key JI planner, Hambali, told interrogators following his arrest that Yazid Sufaat, a California State-trained biochemist who became a JI member shortly after its founding in 1993, sought a "leading role" for his pathology laboratory in CBW development for al Qaeda. Sufaat, who was arrested in 2001 (and recently released[57]), became one of al Qaeda's major researchers on anthrax, which he tried to weaponize.[58]

The fact that Sufaat did his anthrax research directly for al Qaeda rather than JI raises some interesting questions. Most importantly, it suggests that, despite shared goals, al Qaeda and JI did not necessarily see the issue of CBW use in the same way. Indeed, JI was more concerned about local reactions deeming even al Qaeda's conventional attacks excessive. If JI members saw some of those attacks using conventional explosives as counter-productive to their goal of transforming Indonesia into an Islamic state because it could undermine their local legitimacy, how much more concern did they have about CB use?[59]

The JI-al Qaeda differences have led one analyst to conclude that "affiliate groups may have sources of self-restraint above and beyond the restraint of movement components more closely aligned with al Qaeda's fundamental and operational goals", and that these "sources of disharmony may be a vulnerability that can be exploited", especially to serve the goal of deterring CBW terrorism.[60] Almost since the time the issue of CBW terrorism emerged, the question has been debated whether terrorists could be deterred from using CBW. Early conventional wisdom held that "if they have them, they will use them." Deterrence was not seen as possible. More recent analyses, however, have taken a more nuanced view. That view recognizes that deterrence is not "a foundational strategy in the way that it was in the Cold War."[61] Nevertheless, it argues that by thinking more in terms of "shaping" behavior than in terms of classic deterrence, and by disaggregating the various categories of terrorist-related actors who would be involved in the CBW enterprise, one might find points of leverage that could be exploited to influence the choices of at least some of those involved or to limit the impact of such efforts.[62] Hardcore leaders of a group like al Qaeda, for example, are deemed probably less susceptible to such "deterrence" than "aiders and abetters." Whether this assessment is in fact

---

[56] Gillian Bird, Deputy Secretary of the Department of Foreign Affairs and Trade, "Global Threats and Key Challenges: An Asia-Pacific Perspective", Australia Group Plenary, Sydney, April 20, 2005.
[57] Mark Hosenball and Michael Isikoff, "A Germ Warfare Guru Goes Free", *Newsweek*, December 17, 2008.
[58] National Commission on Terrorist Attacks Upon the United States, *9/11 Commission Report*, 2004, p. 151.
[59] See Brad Roberts, "Deterrence and WMD Terrorism: Calibrating Its Potential Contribution to Risk Reduction", *IDA Paper P-4231*, Institute for Defense Analyses, June 2007, pp. 17-18.
[60] *Ibid*., p. 18.
[61] *Ibidem*., p. 1.
[62] For more details on this approach, see *Ibid*. See also Lewis A. Dunn, "Next Generation WMD and WME Terrorism", *op. cit*.

correct, it nevertheless underlines the reality that the old notion that nothing could be done to deter such developments no longer holds sway.

The Challenge of Terrorist CBW Campaigns[63]

Another dimension of the CBW terrorism challenge is the prospect that terrorists will not be satisfied with one-off events, but will eventually seek to use such capabilities in an extended campaign. In November 2006 the Director General of the British Security Service MI 5, Dame Elizabeth Manningham-Buller, described the challenge: "tomorrow's threat may include the use of chemicals, bacteriological agents, radioactive materials end even nuclear technology… It is a sustained campaign, not a series of isolated incidents. It aims to wear down our will to resist." Dame Elizabeth's point relates to terrorist efforts generally, but in including reference to CBRN, she makes an important and often overlooked point. Since 9/11, enormous amounts of time and money have been expended in response planning and bolstering response capacity for terrorist events involving CBRN. That planning, however, has too often revolved around a terrorism *incident* – a terrorist's single use of a CBRN weapon. Planning and capacity building efforts have given far less attention to the possibility of a series of interconnected incidents in the form of a terrorism *campaign*.

Addressing the issue of CBW terrorist campaigns is important because, even at lower levels, terrorist campaigns with unconventional weapons pose questions not confronted in a campaign waged with bombs and bullets. These novel and challenging questions relate to developing appropriate preparedness and response requirements, making difficult tradeoffs regarding the allocation of limited resources, reconciling competing political and economic interests, promoting international cooperation, and reassuring publics. Answers to these questions that might be suitable for dealing effectively with a single incident or a bombs and bullets campaign are likely to fall short in addressing CBW campaigns.

Amplifying a "Weapon of the Weak"

Why think about terrorism campaigns? Because terrorists do. Indeed, it is hard to identify a specific act of genuine terrorism that has been a single stand-alone incident rather than part of a broader set of orchestrated events.[64] Terrorism is understood as a weapon of the weak, and terrorist leaders seem to understand that single acts will have limited impact both because of the circumscribed physical damage a single act can produce and the resilience of a population in its response. Even the level of fatalities and injuries on 9/11 and the physical destruction of the Twin Towers, as horrific as those tragedies were, did not produce a collapse of society, governance, institutions, or infrastructures.

---

[63] This section is based in part on the author's, "Reflections on the Implications of Terrorism Campaigns", in Lewis A. Dunn, "Next Generation WMD and WME Terrorism", *op. cit*., Annex 4.

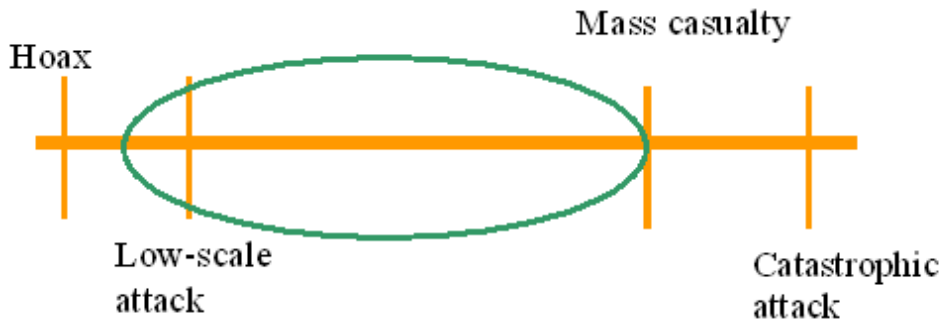
[64] This is true for individuals just as much as groups, as demonstrated by the "campaigns" of the ABC Bomber and the Unabomber.

Terrorists wage campaigns then, to generate outcomes that, in their cumulative effects, cannot be produced by single events. Their goal is at least three-fold:

- to change facts on the ground through ongoing destruction, hopefully making life for the targets increasingly difficult;
- to generate new political dynamics in the target to force accommodation with a seemingly unending sequence of violence; and,
- perhaps most importantly, to alter the adversary's psychological state by eroding his willingness to engage in a prolonged confrontation involving the use of violence,[65] both through fear and anxiety fostered by anticipating the next blow and through exhausting his resources.

It is useful to think about the CBW threat as a continuum in which a hoax and/or small scale, low-impact event stand at one end of the continuum and a catastrophic casualty event is at the other (See Figure 1). The plausible "threat envelope," that is, those contingencies with a higher probability of occurring against which most planning efforts should be directed, rests at the lower end of the spectrum.

Figure 1:
"Plausible Threat Planning Envelope"



Those cases, however, are also ones that may lend themselves best to campaign contingencies. For example, a terrorist may be capable of producing a BW agent but only in small quantities. He may choose, therefore, to use that agent sparingly to carry out multiple events. Similarly, a terrorist may be able to produce low-grade agent of multiple types – anthrax, botulinum toxin, tularemia, etc. – but does not possess the technical capability to make them of a quality high enough to kill people in large numbers. In such scenarios the terrorist may choose to use small amounts of agent or one particular agent at a time in a series of attacks, producing low casualties but considerable uncertainty and fear about what

[65] See Brad Roberts, "Deterring Terrorism: Terrorism Campaigns and Prolonged Wars of Mutual Coercion", Institute for Defense Analyses, December 31, 2003.

might come next. In many cases, human casualties could be very limited, but the accumulating economic, psychological, and, hence, political impact could be significant.

The amplifying impact of a terrorism campaign could be increased by hoaxes and false alarms. Both phenomena are almost certain to accompany a CBW attack. In the months following the Amerithrax mailings, for example, the participants in the U.S. Laboratory Response Network had to analyze more than 100,000 samples of "white powder" and other substances, overloading their capabilities.[66] It is not hard to imagine the amplifying affect that would have been produced had the perpetrators(s) combined the real anthrax letters to the Senate with hoax letters sent to other Senators over a period of weeks. Not only would such a tactic have produced widespread fear and insecurity among Congressional staff and other federal employees, but a major branch of the federal government would have been even more disrupted than it was.[67]

Coping with Uncertainty

A single data point does not make a trend, and it is virtually impossible to predict that a single terrorist attack constitutes the onset of a campaign. It is only as the campaign unfolds that uncertainty may be dispelled, perhaps quickly, perhaps slowly, but perhaps not at all. Yet, it is at the onset of a campaign that decisive action may have its greatest impact.

Two factors in particular signal that a campaign is underway: repetitiveness and signature attacks. Each one is problematic, however, in removing uncertainty. If a series of similar attacks were conducted in the same geographic area over a short period of time, uncertainty will be diminished regarding the likelihood that a campaign has begun. But comparable events occurring in close proximity in time and place is the easy case. The time that elapses between attacks in a campaign could be quite lengthy, as was the case of the Unabomber, whose campaign extended for more than a decade. Indeed, some terrorists may take a long view, not feeling a sense of urgency. Some commentators suggest this was al Qaeda's view in its formative and early operational periods when the group saw its continuing pressure fostering the unraveling of its adversaries in the West, but it spaced its attacks sufficiently far apart to ensure they were effectively planned and conducted.

Use of the same agent in the same way, or more generally a "signature" method of attack, could be another indicator of a campaign. The attacks in Iraq using chlorine and explosives in suicide truck bombs

[66] Gregory D. Koblenz, "Bioterrorism: Understanding the Threat and America's Response," in Arnold M. Howitt, Robyn L. Pangi (eds.), *Countering Terrorism: Dimensions of Preparedness*, Cambridge, MIT Press, 2003, p. 139.

[67] One can also imagine a case, however, in which, being exposed to recurrent, very limited CBW attacks, people become more resilient to it, and Governments might devise better strategies to prevent it and react to it.

provides an example of a similarity in mode of attack that leaves little doubt that a sustained initiative was underway. The Unabomber's devices, while delivered at widely spaced points in time, also so resembled one another that the conclusion could be drawn that they were the work of the same party, although his devices did become more sophisticated over time.[68]

Should a series of attacks involve multiple agents, however, such as first anthrax and then plague, uncertainty as to the nature of the initiative could be much greater. Uncertainty will also remain regarding whether subsequent attacks will occur and what agents will be used. Likewise, if a terrorist employs a strategy of gradual escalation whereby the first attack is small and subsequent attacks gradually escalate in terms of casualties, considerable uncertainty might exist regarding when the terrorists have reached their technical limits. Is the current attack the worst case? Or can the terrorist continue to escalate with even deadlier attacks? Will the next one be the "big one?"

Uncertainty about the scale and intensity of a CBW terrorism campaign, or perhaps even its existence, is important because the inability to determine how much more pain is yet to be felt is likely to fuel significant debates, particularly regarding whether and how limited resources should be deployed. Lacking any additional information, allocating available resources to deal with a single attack is a rather straightforward exercise. The belief that a new incident is part of a series of attacks whose geographic scope, level of destructiveness, and frequency cannot be determined, however, is likely to generate demands beyond the immediate locale of that attack for response capabilities, such as medical supplies. Everyone will want some form of protection and some means to ameliorate the impact of an attack should it occur in their area. This level of demand would rapidly run up against the reality that protective measures, supplies, and other needs are insufficient to meet demand. An emotional debate about "equity" is then likely to ensue. This is as true at the international level as it is on the national level.

Managing an Action-Reaction Cycle

The history of terrorism reveals that in many cases the specific dynamics of a given campaign are shaped by the way governments react to it. Indeed, many campaigns are intended to provoke a series of reactions from the governmental adversary that change the political and psychological milieu in the terrorists' favor. The goal is to induce responses that are seen as excessive and thus discredited. The accumulation of effects from governmental responses is one component of the overall cumulative impact that campaigns are intended to produce.

The British experience with the Irish Republican Army (IRA) demonstrates how this action-reaction cycle during a campaign can be managed. Despite sometimes intense violence, neither the British nor the

[68] Cynthia Hubert and Elisa Roche, "Unabomb Toll: 3 Dead, 2 Dozen Hurt", *Sacramento Bee*, April 25, 1995.

IRA ruled out a potential political settlement, and neither wanted to risk eliminating this option by fostering an unacceptable level of violence. What emerged was a delicate balance in which the IRA carried out relatively small-scale bombings, for which they provided forewarning, but without crossing the threshold that would elicit an all-out British response. The strategy of the British, on the other hand, was not to seek to destroy the IRA (because this was impossible), but to shape the IRA's behavior and guide it into more acceptable political forms.

In the face of CBW terrorism campaigns, it would likely be more difficult to achieve this kind of calibrated action-reaction dynamic. If the argument is correct, however, that CBW campaigns are more likely to involve attacks that produce limited rather than mass or catastrophic levels of casualties, then such calibration might still be possible. Achieving that calibration, however, requires both a reasonable level of capabilities to ameliorate the consequences of a specific attack and, perhaps more importantly, an effective public information effort aimed at shaping a well-informed and resilient public response (which is discussed in more detail below). The latter is particularly important in light of the potential risk that, regardless of the limited nature of the attack, the breaking of a taboo will be seen to constitute a major escalation.

Some terrorists may not be interested in engaging its governmental adversary in such a calibrated back-and-forth, and will use CBW to multiply destruction and intensify psychological pressure. Government reactions in these cases are still important, as the terrorists will be paying attention to the government's response in order to learn either what the government might be doing well so that they can devise a "workaround" for subsequent attacks or to exploit what the government does poorly.

Innovation, Adaptation, and Learning

Terrorists who have successfully waged campaigns of some duration are those who have a strong ability to learn and adapt. Historically, however, these groups are not ones committed to apocalyptic violence.[69] This phenomenon may further suggest that CBW terrorism campaigns will have limits. The innovation, learning, and adaptation that characterize more successful terrorist groups, however, do pose some difficult dilemmas in the context of CBW campaigns.

Al Qaeda materials found in caves in Afghanistan suggest that its understanding of unconventional weapons capabilities was rather unsophisticated.[70] The combination of rapidly advancing science and technology in fields relevant to CBW capabilities, proper recruitment, and the global diffusion of such knowledge, however, suggests that that level of understanding is only likely to increase.

---

[69] Brad Roberts, "Deterring Terrorism", *op. cit.*, p. 16.
[70] Sammy Salama and Lydia Hansell, "Does Intent Equal Capability? Al-Qaeda and Weapons of Mass Destruction", *Nonproliferation Review*, Vol. 12, No. 3, November 2005, pp. 615-653.

The scenario of a terrorist group that "learns" over time and improves on each subsequent attack until it is capable of attacks that generate large-scale casualties is especially challenging. Such a scenario, however, is not something that is likely to emerge overnight, but is only likely to evolve over time. That time must be exploited, in terms of both bolstering preventive and preparedness measures to improve response capabilities and seeking to disrupt the terrorists' learning cycle.

Implications for Multiple Interests

In an environment in which multiple attacks occur against different sectors with different interests or in different geographical areas, decision makers will confront severe challenges in balancing these competing interests. Under the strain of a CBW terrorism campaign all interests may not be treated equally. In fact, with limited response resources, many difficult tradeoffs will have to be made, and some of these decisions are not likely to be well received by those who feel that more could and should be done to protect their interests. Areas that are first to be attacked, for example, could receive the "lion's share" of resources as policy makers scramble to deal with the crisis and use every tool available to minimize the damage. If this happens, areas attacked later will be left to respond with whatever resources remain.

Another difficult tradeoff could arise regarding quarantine in which areas attacked early in a biological campaign are quarantined and thus suffer economic damage. That negative result, in turn, leads decision makers not to impose quarantines in areas attacked later. A tabletop exercise involving just this scenario saw states and even regions put increased political pressure on their members of U.S. Congress to influence executive branch decision making to ensure that their areas receive their "fair" portion of available resources, creating a divide between executive and legislative branch officials. Another example is a scenario in which a metropolitan area falls victim to a small-to-medium-scale bioterrorist attack and many if not all available federal assets, including components of the Strategic National Stockpile, are deployed to the area. Subsequently, over the next several days or weeks additional attacks occur elsewhere. How would the federal government respond in such a situation? How much does it deploy to the site of the initial attack and how much should it hold in reserve as a hedge against subsequent attacks elsewhere? Or will it deploy everything it has to the site of the initial attack and then just hope for the best and try to "make do" with whatever it can if additional attacks occur?[71]

Private sector interests may also conflict with government interests and with each other. For example, if shopping malls across the country were targeted at the same time as brokerage houses, or if private sector buildings are targeted at the same time that federal buildings are hit, who should get priority for what are clearly insufficient decontamination capabilities? Would continuity of government receive a higher priority than

[71] Brad Roberts, "Campaign-Style CBW Terrorism: May 2003 Tabletop – Overview Summary of Key Insights Gained", Chemical and Biological Arms Control Institute, June 11, 2003.

the resumption of business? Meanwhile, the law enforcement community will be reluctant to decontaminate any facilities too quickly for fear of destroying evidence that may be useful in an investigation. Reconciling these interests in the middle of a crisis will not be easy.

Political Implications

The implications of a CBW campaign for the polity are potentially enormous, not only because such a campaign could threaten a variety of interests that would place pressure on decision makers to protect them, but also because intrinsically a "campaign" will not necessarily have a clear end in sight. In the case that the government is unable to halt the CBW terrorist campaign, the loss of confidence in the government could significantly change the political environment. Some of the political divisions that may arise could impair decision-making. Regional political tensions could arise over how resources are allocated, for example, as multiple events unfold. These impacts are not necessarily unique to CBW terrorism campaigns; they can also result from classic campaigns using the traditional terrorist weapons of guns and bombs. A CBW campaign, however, could make them more intense. Disputes over the allocation of limited, specialized resources, such as medicines and other treatments, for example, could become more severe during a campaign using biological weapons

Economic Implications

Economics and trade will almost certainly be affected by a CBW terrorism campaign. Hospitals, manufacturing, construction, repair, food service, and many others sectors are dependent on just-in-time business models. When one link in the chain breaks, it disturbs the downstream flow and other associated businesses. A series of CBW attacks could significantly disrupt business operations, especially if multiple but related sectors are targeted, creating a ripple effect across the economy. Moreover, if the motivation and objective of a terrorist is to disrupt a nation's economy, there is no reason not to target multiple sectors.

Likewise, in the face of a CBW campaign, the financial sector will be negatively impacted as well as investor confidence. Because of the uncertainty surrounding a campaign, particularly regarding the next target, the financial sector could become hesitant to invest in anything other than the safest options. The good news is that after September 11th $7 trillion was taken off the market overnight and the market did not collapse. Similarly, the 2001 anthrax attacks did not cripple the economy, and the Japanese market did not collapse as a result of the Aum Shinrikyo's sarin attacks. But a discernable negative impact on markets was noted because of these isolated attacks. A campaign of CBW attacks for an extended period could magnify this impact. Alternatively, markets could factor in repeated attacks into their operations, reducing the shock they create over time.

Some sectors of the economy are especially vulnerable to a CBW campaign. Agriculture, for example, accounts for about 15 percent of the U.S. Gross Domestic Product (GDP). A biological attack against high

concentrations of livestock and poultry that are susceptible to contagious animal disease such as foot-and-mouth disease (FMD) or avian influenza could have a devastating effect. FMD outbreaks in the United Kingdom and Taiwan illustrate the enormous economic impact of an infectious disease outbreak in livestock.

Another vulnerable economic sector is the biotechnology industry. The public's view of biotechnology as a result of debates over genetically modified food, stem cells, and other issues makes this industry already somewhat fragile. Popular books and movies demonstrate how biotechnology has become a new paradigm for a potential Armageddon, particularly when biotechnology industry executives are portrayed as unscrupulous villains. Should a terrorist deliberately release a BW agent near a biotechnology firm and then publicly suggest that the firm and industry were responsible for the event, it could severely undermine trust in this sector, erode capital investment, and perhaps even cause its collapse.

International Implications

A series of CBW terrorist campaigns, for instance in the United States, will generate significant international political implications. In the case of bioterrorism, for example, particularly if it involves a contagious pathogen, other countries and the World Health Organization (WHO) would need to take measures to prevent the spread of the outbreak. This could mean restrictions on trade and travel originating in the United States, fostering potentially significant impacts on the U.S. economy. The outbreak of Severe Acute Respiratory Syndrome (SARS) is an example of how an infectious disease outbreak can quickly become an international issue and impact trade and travel. Even when a bioterrorism attack is not conducted with a contagious agent, victims who become sick might travel abroad. In such cases, governments will need to communicate with one another regarding the risk that an exposed traveler poses and the appropriate treatment, gather relevant clinical and criminal data, and even determine if the individual was a perpetrator. Should a sick traveler be suspected of involvement in a crime, issues regarding expatriation and the role of international and regional law enforcement authorities, for example, Interpol and Europol, will arise.

Beyond communications, international cooperation could suffer from other strains. One is the challenge of distributing or sharing of limited medical resources. Understandably, most states will have a predisposition to retain their medical stockpiles for their own populations rather than sharing with an ally that has been the object of an attack (unless the first state can be certain that it will not be a target). While international cooperation has improved through such efforts as better coordinated national approaches to a global influenza pandemic, it is not clear that states share the same set of expectations regarding the burden that international cooperation should bear in the event of a CBW terrorist campaign.

Psychological Implications

Despite the fact that society is often more resilient than commentators give it credit for, life at prolonged Code Red could produce deep stresses. If CBW attacks appear to be part of an unrelenting campaign that the government is unsuccessful in stopping, an intense debate about making concessions to the terrorists could create political rifts. Even if a sense of solidarity prevails early in the campaign, as the campaign progresses this solidarity may give way to a desire to end the attacks through concessions. This could be difficult, of course, if the terrorists do not ask the government to concede anything politically or financially. With nothing to offer, officials will have little assurance to provide the public other than that all efforts are being made to capture the perpetrator(s). Though such a promise may be true, it will do little to calm fear if attacks continue. Growing frustration or desperation could also prompt the infringement of civil liberties or a hunt for supporters, "fellow travelers," or anyone "disloyal."

CBW terrorism campaigns represent both risks and opportunities. The biggest challenges derive from the simple fact that decision makers can make some very damaging mistakes that fuel fear or heighten public skepticism regarding the government's competence or credibility. After Robert Stevens came down with the first case of anthrax in the fall of 2001, Tommy Thompson, Secretary of Health and Human Services (HHS), said that it was unlikely that he had contracted the disease from a deliberate release, but that he probably had done so while fishing, despite no hard evidence to support the claim. As a result of issuing inaccurate information, albeit in an attempt to maintain calm, Secretary Thompson undermined his credibility with the public and thus his ability to manage the crisis from a public health and medical perspective. The destruction of trust and the creation of an environment of fear that can result from such mistakes, as the anthrax case suggests, only plays into the terrorists' hands.[72]

In the environment of a CBW campaign, in which the number of attacks is potentially unlimited whereas resources for preventing and mitigating them are finite, decision makers will find themselves in a situation in which they risk committing too many resources or too few. Particularly challenging is a strong likelihood that the response to the first event is abundant, leaving fewer resources available for response to subsequent attacks. Dedicating resources to the second, third, fourth and subsequent events with some sense of rationing would seem to make sense, especially as local communities facing later attacks will likely demand that they receive the same resources as did locales that fell victim to earlier attacks. At the same time, decisions to keep some resources in reserve as a hedge against future contingencies are also likely to be hotly disputed.

Although CBW terrorism campaigns will pose sharp challenges, they also create important opportunities. As one study points out, "the opportunities presented by terror campaigns are principally those to learn

[72] Michael Powers, et al., *What Should We Know? Whom Do We Tell? Leveraging Communication and Information to Counter Terrorism and Its Consequences*, Project Report, Chemical and Biological Arms Control Institute, December 2002.

and adapt, gain the initiative, and exploit mistakes the terrorists make."[73] Seizing the initiative by attacking the terrorists' ability to adapt is especially important. That adaptation is as much about the way terrorists do business as it is about the tools they use. Disrupting that adaptive capability includes cutting off information sources, terminating financing, destroying sanctuaries, and eliminating 'coalition partners.'

Another important opportunity will be successfully meeting the chance to demonstrate that responses can and do get better. Targets of terrorism can adapt as well, and a campaign will test a nation's ability to learn. Passing that test is important, not least because it is a major contributor to public confidence and trust. Doing better each time depends not only on shoring up one's own vulnerabilities and bolstering response capabilities but more fundamentally on having institutional and intellectual resources oriented toward and capable of learning and adaptation.

[73] *Combating the WMD Challenge for the Next 10 Years,* Center for the Study of Weapons of Mass Destruction, National Defense University, February 2005, p. 20.

What Do We Do?
Responding to CBW Terrorism

Trying to predict precisely what form CBW terrorism will take is a non-starter. Rather, the goal should be to be prepared for a wide range of possible contingencies by developing a robust set of critical response capabilities. One set of capabilities focuses on *prevention*, including measures in such critical areas as law enforcement, intelligence, pathogen security, export controls, and cooperative threat reduction. Necessary *preparedness* capabilities also span a wide spectrum and include such elements as effective disease surveillance and reporting, health monitoring, quality epidemiology, robust laboratory-based analysis, appropriate diagnostics and medical countermeasures, and sufficient medical stockpiles, among others. A national effort to develop these capabilities also requires *a robust research and development (R&D) agenda* and *an effective communication strategy*.

While identifying the components of an effective response is relatively straightforward, placing those capabilities into an effective strategic architecture is not easy. It entails the difficult tasks of establishing criteria to determine the appropriate levels of relevant capabilities, balancing a wide set of competing interests, and involving the right set of players. It also requires the management of a number of difficult trade-offs such as balancing prevention and preparedness, determining the relative investments that should be made in people vs. technology, and identifying the relative importance that should be given to immediate requirements vs. longer-term needs. The following concrete steps might be considered.

Foster Conceptual Shifts

Developing more effective response capabilities could be facilitated if those addressing the CBW terrrorism challenge shift their conceptual approach in at least two ways. First, emphasis should be placed not on threat elimination but risk management. The possibility of terrorist use of CBW can never be completely eliminated. In the area of biological weapons, for example, work in the life sciences will continue and should do so for important, legitimate reasons. This means, however, that the potential for misusing advances in the life sciences to make and use biological weapons remains a permanent reality. The objective therefore should not be the unachievable goal of driving the probability of such a contingency to zero, but reducing the risk as low as possible, or at least to a level acceptable to society.

A risk perspective also introduces the important sense of probability. As was noted earlier, if the terrorist goal in using CBW is catastrophic casualties or widespread disruption, fewer pathways are available to achieve that goal and those that do exist are more difficult than those pathways that will produce less significant results. A risk assessment would, then, conclude that the degree of risk declines as the level of desired casualties or disruption increases, insofar as they become less likely. Such a finding should have important implications for planning and resource allocation decisions. It allows for planning efforts to focus on the "plausible risk envelope," while hedging against less likely, but more high consequence possibilities.

The second conceptual shift that should be entertained is one from traditional institutional/hierarchical responses to more network-based approaches. Such a shift may be especially important with respect to both disrupting terrorist learning and adaptation and promoting innovation and learning by those who confront them.

Jean-Francois Rischard, the former World Bank Vice President for Europe, argues that "[t]raditional institutions are incapable of addressing the growing list of complex global issues."[74] He argues further that changes of the kind fostered by globalization "put existing human institutions (nation states, governments, ministries, international institutions, any large hierarchy)... under massive pressure – and tend to overwhelm them."[75] CBW terrorism certainly represents the kind of complex phenomenon Rischard describes. Rather than relying on stovepiped, top-down measures, efforts should be made to exploit what globalization now makes possible. As Anne-Marie Slaughter has pointed out, "Networked threats require a networked response."[76] Fostering such a dynamic must be the objective in building relationships among those communities with responsibility for managing risks associated with CBW terrorism. Moreover, promoting a disaggregated approach not only accommodates but facilitates the multiple forms of response that are needed – local, national, regional, multilateral, global, formal, and informal.

Doing so, however, will not be easy. So far, "using networks to fight networks" is a mantra, a slogan without content. One of the most crucial areas in which new thinking is needed is how this networking approach can be operationalized and put into action. The attempt should be made, therefore, to develop new network theory-based analytical and policy tools.

---

[74] Jean-Francois Rischard, "Global Issue Networks", *The Washington Quarterly*, Vol. 26, No. 1, Winter 2002-3, p. 17.

[75] Jean-Francois Rischard, "My Views on What the Helsinki Process Should Stand For: Accelerated Global Problem-Solving", Personal Contribution to the Helsinki Process on Globalization and Democracy, p. 1.

[76] Anne-Marie Slaughter (formerly at Princeton University and now Director of Policy Planning at the U.S. Department of State), "Government Networks, World Order, and the G20", prepared for the meeting on *The G20 at Leader's Level*, Ottawa, February 29, 2004, p. 2.

Promote National Dialogue

Just as the prospect of non-state use of CBW reflects a growing numbers of players who could do harm, those actors with some responsibility for managing proliferation risks are also increasing. Many communities beyond government nonproliferation officials or the military are now involved in ways that they had not been even a decade ago – health, law enforcement, industry, civil society, and scientists among them. Each of these communities has some role in managing CBW risks, but none of them has that mandate as its primary responsibility. As a result, each community must reconcile that responsibility with its other requirements. Equally important, these communities must find means of developing and maintaining effective working relationships with one another. To date, few incentives have existed for some of these communities – industry, for example - to engage on the terrorism agenda.[77]

That must change. As Francis Fukuyama argues, "the problem is no longer to ensure …control over a large and complex centralized system, but rather to determine how much governance is needed for a decentralized, distributed system and how we can accomplish this goal."[78] In a sense, each of these communities (and the key actors within them) represents a node in a nonproliferation network. As a result, the basis exists for a disaggregated and distributed response to a disaggregated and distributed problem.

Bolster Public Resilience

Public intimidation is among the terrorists' top priorities. Campaigns in particular are intended to achieve "social amplification of risk." To respond to this challenge, governments should seek to draw from a concept developed by the British (among others) to emphasize national resilience.[79] Resilience is more than infrastructure redundancy. It is also about the psycho-social attitudes of the public in the face of prolonged stress. Although history tells of many occasions in which societies have collapsed in face of continued intense stress, it is also replete with times in which societies confronting tremendous pressure have survived. The London blitz and the history of Israel are only two examples. Resilient societies seem to have been those that manage to cope with loss while keeping or recovering hope. Governments must work continually with publics to ensure both.

Bolstering public resilience, therefore, emerges as one of, if not the key area in successfully countering terrorist campaigns. Many studies have concluded that mass panic, that is, irrational panic leading to the breakdown of normal constraints on social behavior, is less likely than often

---

[77] Ken Luongo and Isabelle Williams, "The Nexus of Globalisation and Next Generation Nonproliferation: Tapping the Power of Market Based Solutions", *Nonproliferation Review*, Vol. 14, No. 7, 2007, p. 469.

[78] Francis Fukuyama and Caroline S. Wagner, *Information and Biological Revolutions: Global Governance Challenges – Summary of a Study Group*, Santa Monica, RAND Science and Technology Institute, 2000, p. ix.

[79] Among its other definitions, "resilience" in materials science relates to the property of withstanding a shock and bouncing back.

feared. But a resilient response is not necessarily automatic, and steps can be taken – or avoided – to foster a more resilient public.

In the first instance, resilience entails avoiding what John Steinbruner has called the "societal autoimmune effect," in which the damage that society does to itself is greater than the damage produced by the terrorists' action.[80] A public that flees an area, for example, could yield greater casualties than one that stays in place. Looting or an increase in other crimes following an incident would only exacerbate the social tensions and the drain on the mechanisms for maintaining public order that will already be stressed by the pressures of a campaign. Given that one possible goal of a terrorist CBW campaign is to elicit government responses that are perceived as excessive and therefore illegitimate, governments must be sensitive to the need not to worsen the physical or psychological damage produced by an attack. One British commentator following the July 2005 London bombings made the point succinctly: "The bombs made more than enough victims; it is important that we do not inadvertently create more."[81]

On the positive side, several studies have shown that public resilience can be enhanced by a number of factors, including preparation, a perception of an ability to cope, and successful recovery from a past trauma.[82] These traits are fostered through a combination of positive individual perspectives, strong social connectedness developed through the creation of supportive networks, and effective problem solving skills. Lessons from military experience reinforce these findings, showing that soldiers overcome their fear if they have appropriate information, training, and cohesion.

The Importance of Public Information Efforts

Information and social networks are key to shaping public resilience. These requirements, in turn, call for strong government communication efforts. Clearly, these must include direct communication with the public about why and how they should be prepared.

Public communications has become an intense battleground between terrorists and their government adversaries. Terrorist organizations use communication strategies to attract recruits, win political, moral and other forms of support, and shape the will of its governmental targets and their populations.

---

[80] John Steinbruner, "Terrorism: Practical Distinctions and Research Priorities", *International Studies Review*, Vol. 7, No. 1, 2005, p. 139.

[81] Gino Verley, Pieter Maeseele, Isabelle Stevens, and Anne Speckhard, "Resilience in an Age of Terrorism: Psychology, Media and Communication", prepublication copy, p. 4.

[82] Michael T. Kindt, "Building Population Resilience to Terror Attacks: Unlearned Lessons from Military and Civilian Experience", Cou*nterproliferation Papers, Future Warfare Series*, No. 36, USAF Counterproliferation Center, Air University, November 2006, p. 2. Kindt also captures these same notions in his use of the terms "optimism," "self-efficacy," and "mastery." *Ibid*., p. 6.

Governments increasingly recognize the critical role that good information sharing between intelligence and law enforcement agencies as well as between response communities plays in effectively managing the threat of terrorism. Governments also attempt to communicate to terrorists to manipulate their cost-benefit calculations. For example, the U.S. government's public discourse regarding homeland security-related activities is intended in part to send the message to terrorists that conducting a successful CBW attack is either unlikely to succeed or will produce unacceptable consequences for the terrorists.

Communication with the public in the face of a CBW campaign is a particularly critical task. It involves not just informing the public of useful measures they can take to reduce risk but appropriate attitudes to adopt. Such measures are critical to managing public perceptions before, during, and after an attack to ensure that fear and panic does not complicate and impede critical responses. Without a coherent line of argument and explanation from credible government officials, the field will be wide open for wildly divergent and unhelpful assessments, rumors, and "expertise." Crisis exercises have identified a number of other significant challenges in shaping effective public information efforts including:

- Understanding that not all officials have the same degree of credibility, even those who seem to be in the right bureaucratic "slot"; exercises show, for example, that local officials are deemed more credible when it comes to health-related information.[83]

- Recognizing that telling the "whole truth" may, in fact, not always be helpful, especially in times of uncertainty. This is not to suggest that incorrect information should be provided; honest information is essential for maintaining credibility. Rather, it is to argue that when key information is not available, an "I'll get back to you" might be the best answer.

- Overcoming the reluctance to discuss "taboo" subjects which, if not considered beforehand, could undermine response efforts. Questions such as quarantines, the potential for imposing martial law, and health and medical priorities (e.g., who gets immunized and who does not when vaccine supplies are limited) are only some of those issues.

International Cooperation

Combating CBW terrorism demands effective international cooperation. This is the case for several reasons:

- International efforts to defeat terrorism represent the first line of defense of the homeland for all countries. An effective anti-terrorism strategy extends outward to defeat threats and manage the risks as far away from one's shores as possible. Doing so requires thorough cooperation with and from friends and allies.

[83] Powers et. al., *What Should We Know?*, *op. cit.*, pp. 30-32.

- Efforts by other countries could have important implications for dealing with a domestic challenge. How other countries act in a crisis could influence a domestic situation in several ways. First, friends or allies may have resources or assets on which a country might wish to draw. Knowing what other countries are doing and what resources they could bring to bear is a vital planning factor in domestic preparedness and response efforts. Other countries' response capabilities – or lack of them – could also have an important impact on a country's domestic situation. The inability to contain an infectious agent elsewhere, for example, could result in a widening attack. Moreover, differences in national preparedness and response efforts could influence terrorists' cost/benefit assessments. Finally, one can learn lessons from others. Although efforts to confront the biological challenge are not as well developed in many countries as they are in the United States, some U.S. friends and allies have conducted valuable exercises and other activities. Sustained exchanges with those who have engaged in such efforts would provide benefits to all.

- International cooperation can modulate potential perturbations resulting from national initiatives. Because work in the life sciences – whether academic or business – has become a global enterprise, national efforts to restrict, control, or regulate it may cause turbulence within the community. Researchers, corporations, or investment could gravitate to those parts of the world less stringently regulated than places where security-related limitations have been introduced. Such an outcome would not only diminish the security benefits of restrictions, but it could also reduce economic and scientific progress in the life sciences sector for countries or regions where such regulation exists. Some people, for example, believe that U.S. regulations related to work with "select agents" are excessive. While they certainly have complicated day-to-day scientific research, it is too soon to determine their long-term impact on the attractiveness of the United States as a place to do some kinds of research or conduct some areas of business. Nevertheless, it is a valid concern.

- Building bridges and raising awareness among constituencies not traditionally engaged in security is critical. Much of the international cooperation so far has occurred on the basis of "like-with-like:" entities such as law enforcement or public health officials have interacted with each other, but rarely with relevant practitioners across institutional or "professional" functional boundaries. More cooperation of this kind is needed to facilitate essential integrative efforts – both globally and domestically. This includes, for example, close cooperation among law enforcement officials and emergency responders, or intelligence professionals and health care officials. Enhanced cooperation between the government and the private sector on both a national and international basis is also crucial, but lacking.

If the need for international cooperation is clear, its promotion nonetheless remains challenging for a number of reasons. The absence of

common perceptions of threats and risks results in an insufficient basis for developing shared priorities that can guide strategic planning efforts. No agreed criteria provide guidance for answering the crucial question of how much is enough – nationally or internationally. Homeland security requirements in every country confront competing domestic priorities, especially in the social sector, and different countries reconcile that competition differently. Similarly, both the United States and its friends and allies pursue wide-ranging non-security interests, especially in the economic and commercial sphere, that can bear heavily on decisions concerning homeland security investments. Examples include corporate competition in important developing countries, differing approaches to improving global health, or the priorities of national science policy.

Finally, international institutional mechanisms remain inadequate to promote cooperation. Although a number of forums exist – e.g., the G-8, the Global Health Security Action Group, Interpol, and the World Health Organization – they either attend to narrow aspects of the problem or generally lack follow-through to match their rhetoric.

One benefit of expert discussions in recent years has been to make it crystal clear where the success or failure of international efforts to deal with the biological challenge will rest, that is, with individual nations. The Biological Weapons Convention (BWC) work program since 2003, for example, has been about what states can do – now – to address the problem. There is no dearth of ideas for action.

In focusing responsibility where it belongs, the BWC work plan reinforces thinking that underlies other recent initiatives, most notably UN Security Council Resolution 1540, a vital measure in combating WMD terrorism. Both of these efforts also highlight the reality that progress will be made in the fight against the misuse of the life sciences only if national governments are willing to take the problem seriously and commit themselves to action.

Capacity Building

Many countries, however, lack that capability to act. The United Nations among others has identified strengthening state capacity to prevent the acquisition of WMD and related materials as a priority.[84] As a result, many of the more recent initiatives include the prospect of some states providing assistance to those who need it.

Progress on providing assistance would certainly help alleviate the lack of resources and technical capacity that currently plagues multilateral efforts to manage CBW and other WMD-related risks, especially among developing countries. It may indeed be in the realm of assistance that some of the greatest gains can be made in leveraging limited resources to

[84] United Nations, “Uniting Against Terrorism: Recommendations for a Global Counter-Terrorism Strategy”, *Report of the Secretary General*, 06-33088, April 27, 2006.

produce concrete results. But here too delivery has fallen short of potential. Providers and recipients often have different views of both the nature and priority of the problem and the best means by which to address it. A mismatch also appears to exist between offers of help and the types of assistance requested, that is, requests are often more for financial support while offers tend to be more technical in nature. In some cases, requests for help (for implementing UNSCR 1540, for example), are often in such general terms that it is difficult for those who are willing to provide help to know what it is they need to do.

The Henry L. Stimson Center, however, has identified several key insights that are relevant to attempts to provide assistance of the kind called for in Resolution 1540 and other recent initiatives.[85] These include the following:

- Without mutual agreement on the underlying threat or risk, assistance is not sufficiently valued by the recipient state to sustain the measures adopted.

- "Whole of government" responses are not available or even readily attainable in many countries to address complex, multifaceted issues.

- Successful implementation of measures requires a baseline of good governance that simply does not exist in many developing countries.

- Sustainability of assistance, therefore, requires incorporating traditional development objectives of long-term institution building and capacity building.

The Stimson Center analysis concludes, therefore, that what is perhaps most important is promoting a methodology that "targets developing states' own priorities to foster ownership of the assistance rendered."[86]

Such an approach could also help to bridge the gap in the priority currently given to fighting WMD terrorism by developed and developing states. It would convey a nuanced understanding of the perspectives of developing countries and foster a more sophisticated linkage between their agenda and that of those countries in the forefront of the fight. By offering something that will benefit developing countries according to their lights as to what is most important rather than someone else's, prospects are enhanced that they will also buy in to the specifics on which they are being asked to engage.

---

[85] Elizabeth Turpen, "Non-State Actors and Nonproliferation: The NGO Role in Implementing UNSCR 1540", Cooperative Nonproliferation, Henry L. Stimson Center, www.stimson.org/cnp/?SN=CT200708061436

[86] Ibid.

Obviously, not everyone can do everything. But everyone can do something, including ensuring at the national level that the basic legal, regulatory, and operational fundamentals are in place. Each can, sometimes with help, conduct assessments that highlight which dimensions of today's challenges are most relevant to its situation as a way to determine what critical gaps exist and what priorities should be adopted. Each can assume a cooperative posture, at least with regional neighbors, even if they cannot offer a high global profile.

Information

All published issues of the Proliferation Papers series can be downloaded from the Ifri website :

www.ifri.org

The latest contributions include :

- Mark Fitzpatrick, *The World After. Proliferation, Deterrence and Disarmament if the Nuclear Taboo is Broken*, Proliferation Papers n°27, Ifri, Spring 2009

  http://www.ifri.org/files/Securite_defense/PP27_Fitzpatrick_Spring2009.pdf

- James A. Russell, *Strategic Stability Reconsidered: Prospects for Escalation and Nuclear War in the Middle East*, Proliferation Papers n° 26, Ifri, Spring 2009

  http://www.ifri.org/files/Securite_defense/PP26_Russell_2009.pdf

- Chung-Min Lee**,** *The Evolution of the North Korean Nuclear Crisis: Implications for Iran,* Proliferation Papers n°25, Ifri, Winter 2009

  http://www.ifri.org/files/Securite_defense/Prolif_Chung_Min_Lee_NK.pdf

- Ariel E. Levite, *Heading for the Fourth Nuclear Age,* Proliferation Papers n° 24, Ifri, Winter 2009

  http://www.ifri.org/files/Securite_defense/Levite_Fourth_Nuclear_Age.pdf

- William Walker, *President-elect Obama and Nuclear Disarmament,* Proliferation Papers n° 23, Ifri, Winter 2009

  http://www.ifri.org/files/Securite_defense/Walker_Obama_nuclear_disarmament.pdf

- George Perkovich, *Principles for Reforming the Nuclear Order,* Proliferation Papers n° 22, Ifri, Fall 2008

  http://www.ifri.org/files/Securite_defense/Perkovich_Reforming_Nuclear_Order.pdf

For further information on the *Proliferation Papers* collection, please feel free to contact Ifri's Security Studies Center : thomas@ifri.org