CHAPTER THIRTEEN
THE CHANGING PROLIFERATION THREAT AND THE INTELLIGENCE RESPONSE

Summary & Recommendations

The threat of chemical, biological, and nuclear weapons proliferation has transformed over the past two decades. The technical expertise required to produce these weapons has become increasingly widespread, while many of the materials needed to make them are widely available on the open market. Meanwhile, terrorists have expressed a growing demand for these weapons and demonstrated their willingness to use them. The Intelligence Community has not kept pace with these events.

Rather than attempt a top-to-bottom assessment of the chemical, biological, and nuclear weapons threat, here we focus on relatively new aspects of the threat that present specific intelligence challenges, and that—in our view—require additional Intelligence Community reforms beyond those discussed in our other chapters.

We recommend that:

- The DNI take several specific measures aimed at better collaboration between the intelligence and biological science communities;
- The National Counter Proliferation Center develop and ensure the implementation of a comprehensive biological weapons targeting strategy. This entails gaining real-time access to non-traditional information sources; filtering open source data; and devising specific collection initiatives directed at the resulting targets;
- The Intelligence Community, along with other relevant government bodies, support a more effective framework to interdict shipments of chemical, biological, and nuclear proliferation concern; and
- The Intelligence Community better leverage existing legal and regulatory mechanisms to improve collection and analysis on chemical, biological, and nuclear threats.

INTRODUCTION

We live in a world where the most deadly materials created by man are more widely available than ever before. Over the past decade or so, the proliferation of nuclear, biological, and chemical materials, and the expertise to weaponize them, has become a global growth industry.

Grim evidence of this abounds. For instance, the Soviet Union may have been relegated to the dustbin of history, but its nuclear materials—under uncertain control, and sought by rogue states and terrorists alike—still imperil our present. At the same time, terrorists who have already demonstrated their intent to attack us with anthrax seek more advanced biological and nuclear weapons. Perhaps worst of all, the biotechnology revolution is rapidly making new, previously unimagined horrors possible, raising the specter of a modern-day plague, spawned from a back room or garage anywhere in the world.

There is no single strategy the Intelligence Community can pursue to counter the "proliferation" menace. As we discuss in this chapter, any weapon capable of causing mass casualties presents a unique set of challenges. Our study of this subject indicates, however, that there are themes common to all. First, the Intelligence Community's efforts with regard to the spread of nuclear, biological, and chemical weapons have not kept up with the pace of proliferation, and urgently require improvement. We believe that catching up will likely require prioritizing counterproliferation over many other competing national security issues. It will also require more aggressive and innovative collection techniques, and the devotion of resources commensurate to the seriousness of the threat and the difficulty of the collection challenge.

Second, the Intelligence Community must reach outside its own confines to tap counterproliferation information, authorities, and expertise resident in the government and nation at large. The Community cannot expect to thwart proliferators on its own; counterproliferation is a team sport, and our squad must draw on the rest of the U.S. government and the full weight of its regulatory and diplomatic powers, as well as on scientific and technical experts from academia and private enterprise.

We begin our discussion of the proliferation problem by examining these themes within the context of the threat posed by biological weapons. Of all the potentially catastrophic threats facing the United States, those related to

biological substances are changing the most quickly, metastasizing in recent years to include a variety of new potential users and substances. Unlike nuclear or chemical weapons, a biological weapon has actually been used to attack the United States, in the form of the anthrax attacks of 2001. In our view, biological weapons are also the mass casualty threat the Intelligence Community is least prepared to face. We therefore have focused on developing recommendations that can immediately improve our capabilities in this area—by bringing into the Community much-needed scientific experience, sharpening collection techniques, and harnessing regulatory authorities to bolster intelligence efforts.

We then survey the threat landscape with regard to nuclear and chemical weapons, and follow this with a series of recommendations designed to improve overall Intelligence Community support to the interdiction of materials of proliferation concern. We close with recommendations that recognize the importance of more generally leveraging legal and regulatory mechanisms to aid in the service of intelligence.

The stakes for the Intelligence Community with regard to all weapons of mass destruction are self-evidently high. It is not hyperbole to suggest that the lives of millions, and the very fabric and fate of our society, may depend on the way in which the Community is configured, and the powers it can bring to bear against the challenges posed by proliferation. Our recommendations do not purport to solve the proliferation problem; no commission can claim to do that. We do hope, however, that the recommendations can help better configure the Community to cope with an increasingly fluid and volatile threat environment.

BIOLOGICAL WEAPONS

Introduction: "The Greatest Intelligence Challenge"

For many years, the U.S. intelligence and policy communities did not take the biological weapons threat as seriously as the dangers posed by nuclear weapons. Many felt that states might experiment with biological weapons, but would not use them against the United States for fear of nuclear retaliation. Similarly, terrorists who promised to bring "plagues" upon the United States were thought to be merely indulging in grandiose threats; they lacked the technical expertise to actually develop and deploy a biological weapon.

These views changed suddenly in September and October of 2001 when anthrax attacks in the United States killed five people, crippled mail delivery in several cities for over a year,[1] and required decontamination efforts costing more than $1 billion.[2] The still-unsolved attack was striking in its asymmetry: the anthrax could have been produced for less than $2,500.[3]

Even more striking is how lucky we were. A determined terrorist group could do far worse with only a little more effort and a bit of luck. Even allowing for imperfect dissemination techniques, if a gram of the same anthrax used in the 2001 attacks had been disseminated outdoors in an urban area, between 100 and 1,000 people would likely have been infected, and many would have died.[4] A kilogram might infect tens of thousands of people.[5] And because biological weapons have a delayed effect, terrorists could execute multiple or campaign-style attacks before the first attack is even noticed and the warning sounded.[6]

We are concerned that terrorist groups may be developing biological weapons and may be willing to use them. Even more worrisome, in the near future, the biotechnology revolution will make even more potent and sophisticated weapons available to small or relatively unsophisticated groups.

In response to this mounting threat, the Intelligence Community's performance has been disappointing. Its analyses of state and non-state biological weapons programs often rest on assumptions unsupported by data. This is in large part because traditional collection methods do not work well, or at all, against biological threats. Even though scientists, academics, and government officials routinely describe an attack with biological weapons as one of the most terrifying and probable disasters the United States faces, the Intelligence Community is lagging behind in looking for new collection strategies, and has not sought sufficient help outside the halls of intelligence agencies. The Community cannot defeat what one senior policymaker told us was "the greatest intelligence challenge" by itself.[7]

We recommend three ways of changing the Intelligence Community's overall approach to biological weapons: (1) better coordination with the biological sciences community; (2) more aggressive, targeted approaches to intelligence collection; and (3) effective use of new regulatory mechanisms to create collection opportunities.

Biological Threats*

Terrorism

Despite the possibility that terrorists have gained access to biological weapons, a large bioterrorist attack has not yet occurred. Why not? First, executing a large-scale biological attack is still fairly difficult as a technical matter; it requires organization and long-term planning. Second, biological agents can be highly infectious; working with them is dangerous. Finally, the war on terrorism may have derailed nascent attack plans. But these thin lines of defense are rapidly eroding. Some terrorist groups may have the financial resources to purchase scientific expertise. Even without sophisticated expertise, a crude delivery system would be sufficient to inflict mass disruption and economic damage.[8] Moreover, extremists willing to die in a suicide bombing are not likely to be deterred by the dangers of working with biological weapons. As a result, a senior intelligence official told the Commission that we should consider ourselves "lucky" we have not yet suffered a major biological attack.[9] And the terrorist threat will only grow, as biological weapons are rapidly becoming cheaper, easier to produce, and more effective.

States

States pose another biological weapons threat, and the weapons they produce are potentially more sophisticated—and therefore more lethal—than those made by terrorists. We can only speculate as to why countries have not yet used biological weapons on a large scale. In part, there is the risk of blowback—infection could spread to the state's own population. The United States may also be protected by the threat that it will respond violently to a biological attack. As President Nixon said when he terminated the United States biological weapons program and embraced an international ban, "We'll never use the damn germs, so what good is biological warfare as a deterrent? If somebody uses germs on us, we'll nuke 'em."[10]

Covert use, however, is an entirely different matter. If the United States is attacked with biological weapons and cannot identify the attacker, the threat of nuclear retaliation will be of little use. States might attack the United States or its military installations overseas and avoid retaliation by posing as terrorists. If the spread of illness is the first sign that such an attack has taken

* The classified version of this section contains a more detailed discussion of the nature of the biological weapons threat, and also provides examples that could not be included in an unclassified report.

place, the U.S. government may have difficulty responding effectively. In many attack simulations, U.S. biodefense capabilities struggle to simultaneously administer medical countermeasures, quarantine infected individuals, and decontaminate large areas.[11]

Biotechnology

A third biological weapons threat lies not far in the future. Terrorists may soon be able to cause mass casualties that are now possible only for state-run biological weapons programs. Scientists can already engineer biological weapons agents to enhance their lethality either through genetic engineering or other manipulations.[12] Such weapons of science fiction may soon become a fact. Given the exponential growth in this field and access to its insights through the Internet, our vulnerability to the threat might be closer at hand than we suspect.

The Intelligence Gap: What We Don't Know

The Intelligence Community has struggled to understand the biological weapons threat. According to a senior official in CIA's Counterproliferation Division, "We don't know more about the biological weapons threat than we did five years ago, and five years from now we will know even less."[13]

Analysis: Assumptions Abound

Assessments of state and non-state programs rely heavily on assumptions about potential biological weapons agents, biological weapons-adaptable delivery systems, and fragmentary threat reporting. Unsurprisingly, this leads to faulty assessments. For example, in October 2002, the Intelligence Community estimated with "high confidence" that Iraq had an active biological weapons program.[14] Yet the Iraq Survey Group's post-war investigation "found no direct evidence that Iraq had plans for a new biological weapons program or was conducting biological weapons-specific work for military purposes" after 1996.[15] In Afghanistan, the story is the reverse. Despite suspicions that al-Qa'ida had biological weapons intentions, the Intelligence Community was unaware of the ambitious scope of its efforts.[16]

Biological weapons analysis also suffers from the litany of problems we have identified elsewhere in our report, including insufficient outreach to technical experts in the CIA's Directorate of Science and Technology and the Department of Energy's National Labs, as well as those in the business community,

public heath sector, and academia.[17] With limited interaction between technical experts and political analysts, the Intelligence Community "does a poor job of matching capabilities with intent" to develop realistic biological attack scenarios for state and non-state actors alike.[18] As one National Intelligence Officer told us, biological weapons analysts have an "institutional bias against creative war-gaming" and rarely engage in systematic testing of alternative hypotheses.[19]

*Collection: Continued Frustration and a Glimmer of Hope***

The weaknesses of analysis, however, pale beside the Intelligence Community's inability to collect against the biological weapons target. We found that the Community's biological weapons collection woes result from both the technological limits of traditional collection methods and a poorly focused collection process that is ill-equipped to gather and sort through the wealth of information that could help alert the Community to crucial indicators of biological weapons activity. In our classified report, we discuss these intelligence collection limitations at length; unfortunately, these details cannot be included in our unclassified report.

At bottom, the gap in collection on the biological threat is largely attributable to the fact that the Community is simply not well configured to monitor the large stream of information—much of it publicly available—relevant to biological weapons. In our classified report, we illustrate how considerable information about al-Qa'ida's pre-war biological weapons program in Afghanistan could have been known through public or government sources; we cannot, however, provide these details in an unclassified format. We emphasize here simply that the Community must focus on doing a better job of collecting and connecting similar indicators of biological weapons personnel and activity in the future. Moreover, as we point out in our Chapter Eight (Analysis), it is essential that the Community improves its access to and use of open source intelligence—the challenges posed by the biological weapons threat reinforce that conclusion.

However, before the Community can begin to effectively monitor such vital indicators of biological activity, it must develop a basic understanding of the threat landscape. We were disappointed to discover that, three-and-a-half

**A considerable majority of information contained in this section of our classified report could not be discussed in an unclassified format.

years following the anthrax attacks, the Intelligence Community has still not taken many of the most rudimentary steps necessary for this sort of collection. In our classified report, we offer examples of how particular intelligence agencies have failed to take these steps, but these details cannot be discussed in an unclassified format. We also describe a (classified) nascent effort at CIA that we believe to be worthy of praise. In all events, the Intelligence Community must ensure that any new efforts support a comprehensive collection effort across different regions, groups, and biological threats. Just as in other areas of intelligence, agencies at times jealously guard their most sought-after information. This fragmentation and parochialism highlights the importance of integrating the government's efforts against proliferators as well as the need for naming a deputy to the Proliferation Mission Manager, as recommended below, to focus exclusively on biological weapons issues.

The United States Response: The Biodefense Shield

Although resources have flowed freely into biodefense since the 2001 anthrax attacks, only a fraction of these resources has gone to funding new intelligence collection strategies.[20] A senior official at the National Security Council laments that, with regard to biological weapons intelligence, "there's still a sense that it's too hard to do."[21] Although future biodefense technologies and medical countermeasures may allow the United States to neutralize the effects of biological attack, intelligence is one of the few tools today that holds out hope of avoiding attack, rather than just limiting the damage. Biodefense is critical, but it should not be our first line of defense. As a senior Centers for Disease Control and Prevention (CDC) official states, we "need to move upstream from the event"—a reactive biological weapons posture will not suffice.[22]

One positive outgrowth of U.S. biodefense programs is that they have bred new intelligence customers, beyond the traditional military and foreign policy users. Technical experts, who include the CDC, Department of Homeland Security, the United States Army Medical Research Institute for Infectious Diseases (USAMRIID), the National Institute for Allergies and Infectious Diseases (part of the National Institutes of Health, or NIH), and the Department of Agriculture, now need biological weapons threat information to inform their biodefense efforts.[23] The existence of these customers presents an opportunity to encourage more focused biological weapons intelligence, and in turn to provide the Intelligence Community with much needed expertise.

Regrettably, new biodefense customers are largely unaware of what intelligence can bring to the table. A senior NIH official, for example, expressed frustration with the quality of biological weapons intelligence that NIH receives, as well as the lack of a structured venue for receiving and assessing such information. This has made the effort to set vaccine research and development priorities more difficult and, worse yet, may have divorced vaccine research from what is known about the current threat.[24] Yet at the same time, demonstrating the cultural gap that still divides the biodefense and intelligence communities, this same official expressed immediate reluctance when told that NIH could perform its own intelligence analysis of open sources to identify the most likely biological threats.[25]

CIA analysts observe that their agency in particular does a poor job of interacting with outside experts,[26] but there are promising initiatives elsewhere within the Community. One effort aimed at increasing such interaction is the Defense Intelligence Agency's Bio-Chem 2020, a small-scale attempt at discussing emerging biotechnology threats with outside experts, usually at the unclassified or secret level. These scientists publish periodic papers on general biological threats rather than reviewing specific biological weapons analysis.[27] A senior National Security Council official praises Bio-Chem 2020 but is quick to note that it is a "cottage program," not part of a broader Intelligence Community endeavor.[28] Another useful initiative is a plan for a National Interagency Biodefense Campus at Fort Detrick, Maryland, with personnel from USAMRIID, NIH, and the Departments of Agriculture and Homeland Security. The campus, which is designed to coordinate biodefense research and serve as a central repository for expertise, will not be complete until 2008.[29] In our view, the culture gap between the biological science and defense communities is so large that housing them together is essential to fostering a common strategy. The extent of Intelligence Community participation at the campus, however, remains undetermined.[30]

Going Forward: Improving Biological Weapons Intelligence Capabilities

If the Intelligence Community does not improve its foreign and domestic collection capabilities for biological weapons, the risk of catastrophe will only grow. We see a need for three broad changes: (1) tighter Intelligence Community coordination with the biological science community both inside government and out; (2) far more emphasis on integrated and aggressive intelligence

targeting; and (3) stronger regulatory efforts to control potential biological weapons technologies, which would enable more intelligence collection than any go-it-alone effort by the Intelligence Community.

Working with the Biological Science Community

Recommendation 1

The DNI should create a Community-wide National Biodefense Initiative to include a Biological Science Advisory Group, a government service program for biologists and health professionals, a post-doctoral fellowship program in biodefense and intelligence, and a scholarship program for graduate students in biological weapons-relevant fields.

When an intelligence analyst wants to understand a foreign nuclear weapons program, the analyst can draw on the expertise of thousands of Americans, all of whom understand how to run a nuclear program—because that is what they do, day in and day out. If an analyst wants the same insight into biological weapons programs, working bio-weaponeers are simply not available. The last offensive American biological weapons program ended 35 years ago.

The United States faced a similar dilemma in the late 1950s with regard to nuclear physics. The World War II physicists at Los Alamos were aging, and the younger generation did not have strong ties to the U.S. government. In response, the Defense Department founded the JASONs, an elite group of distinguished nuclear scientists that interacts with senior policymakers, receives intelligence briefings, and provides classified studies on pressing national security issues.[31] Considering the number of Nobel laureates in the group, the opportunity for rising stars to interact with leading scientists in their field, and the financial compensation that members receive, membership to the JASONs remains highly coveted.

According to a CIA report summarizing a conference of life science experts, "a qualitatively different relationship between the government and life sciences communities might be needed to most effectively grapple with the future biological weapons threat."[32] Although DIA's Bio-Chem 2020 is a successful interaction mechanism with academia and the private sector, it is insufficient compared to what is required. The Intelligence Community needs more consistent advice than that provided by unpaid professionals, and more

contemporary advice than that provided by intelligence scientists who have not published research in over a decade.

We therefore recommend that the new DNI create a National Biodefense Initiative composed of several programs aimed at strengthening the Intelligence Community's biological weapons expertise. Such an initiative could be composed of the following four components:

- An elite Biological Sciences Advisory Group, administered by the DNI's Director of Science and Technology, which would be composed of the nation's leading life science experts. The group would be compensated for their work and asked to examine and advise the DNI on biological threats;
- A part-time government service program for select biologists and health professionals to review biological weapons analysis and answer Community queries;
- A post-doctoral fellowship program that funds scientists for one to two years of unclassified research relevant to biodefense and biological weapons intelligence; and
- A scholarship program that rewards graduate students in the biological weapons-relevant hard sciences in exchange for intelligence service upon completion of their degrees.

Recommendation 2

The DNI should use the Joint Intelligence Community Council to form a Biological Weapons Working Group. This Working Group would serve as the principal coordination venue for the Intelligence Community and biodefense agencies, including the Department of Homeland Security's National Biodefense and Countermeasures Center, NIH, CDC, the Department of Agriculture, and USAMRIID.

In addition to reaching *outside* the government to develop a more robust and mutually beneficial relationship with the biological science community, the Intelligence Community needs more effective links with biological experts and authorities inside the government. Nurturing this relationship will help

ensure that relevant science is informing actual intelligence collection and better serving new customers. We believe that the DNI could utilize the Joint Intelligence Community Council, established by the intelligence reform legislation, to convene a working group of agencies with interest in biological weapons intelligence to serve as a kind of "consumer council."[33] This working group would have the added benefit of helping both sides—the intelligence and biological science communities—understand the needs of the other so that they can more effectively work in parallel. The DNI might consider moving the biological weapons working group, or other biological weapons intelligence units, to the National Interagency Biodefense Campus once it is completed in 2008.

Targeting Biological Weapons Threats

Recommendation 3

The DNI should create a deputy within the National Counter Proliferation Center who is specifically responsible for biological weapons; this deputy would be responsible to the Proliferation Mission Manager to ensure the implementation of a comprehensive biological weapons targeting strategy and direct new collection initiatives.

As our previous discussion of the Community's collection woes starkly illustrates, the Intelligence Community needs more aggressive, targeted approaches to intelligence collection on biological threats. Systematic targeting of potential biological weapons personnel and programs is critical. CIA's Directorate of Science and Technology is funding some promising efforts, but they remain in their initial stages, and the Directorate lacks the authority to implement a program across the Community. Much more needs to be done.

First, the Intelligence Community needs a targeted, managed, and directed strategy for biological weapons intelligence. We strongly suggest designating an office within the NCPC to handle biological weapons specifically. It is also essential that this designee (or deputy) for biological weapons work in tandem with his or her counterparts at the National Counterterrorism Center.

With visibility across the Intelligence Community, the biological weapons deputy in the National Counter Proliferation Center (NCPC) could draw on different pockets of relevant expertise. But if CIA's Directorate of Operations

(DO) is any kind of microcosm of the biological weapons intelligence world, then a daunting task lies ahead. Within the DO, the Counterterrorist Center collects against bioterrorism; the Counterproliferation Division collects against most state biological weapons programs, and the geographic area divisions collect against the remainder.[34] Such fragmentation leaves serious potential gaps.[35]

Devising and implementing a biological weapons targeting strategy will require not only that the Intelligence Community begin to think as a whole, but also that the Intelligence Community think beyond itself. Part of the challenge involves drawing on personnel and databases housed in non-Intelligence Community agencies such as Commerce's Bureau of Industry and Security and Homeland Security's Customs and Border Protection. Data from non-intelligence sources needs to be cross-referenced with the Intelligence Community's biological weapons databases, and filtered through a set of developed biological weapons indicators to direct intelligence collection. FBI and Homeland Security personnel need training in intelligence targeting and access to this system to identify homeland threats.

A comprehensive and strategic approach to biological weapons targeting will also involve open source exploitation to drive collection and warning strategies, and a multi-year research and development plan for the development and deployment of emerging collection technologies. In our classified report, we offer several suggestions for improving the Intelligence Community's capabilities which cannot be discussed in an unclassified format. Elements within the Community deserve praise for having taken steps to implement these suggestions.

It is our hope that through a Target Development Board, the NCPC's deputy for biological weapons can drive the Intelligence Community to pursue the necessary multifaceted collection approach. We encourage the Community to continue to explore and develop new approaches to collection, and we expect that these efforts would be dramatically furthered by the Mission Manager and Target Development Board devices.

Leveraging Regulation for Biological Weapons Intelligence

Recommendation 4

The National Security Council should form a Joint Interagency Task Force to develop a counter-biological weapons plan within 90 days that draws upon all elements of national power, including law enforcement and the regulatory capabilities of the Departments of Homeland Security, Health and Human Services, Commerce, and State.

The United States should look outside of intelligence channels for enforcement mechanisms that can provide new avenues of international cooperation and resulting opportunities for intelligence collection. The National Counter Proliferation Center will be able to do a great deal to expand outreach to the biological science, biodefense, and public health sectors, but an even broader effort is required to draw on departments and agencies outside of the Intelligence Community. We believe the National Security Council or perhaps the Homeland Security Council is the most appropriate venue for convening different national security elements to devise such national-level strategies. Intelligence will be able to most effectively operate in a national security environment that is organized around and cognizant of its combined efforts to work against the biothreat.

We suggest that the Joint Interagency Task Force consider, as part of its development of a counter-biological weapons plan, the following two recommendations—which involve developing beneficial relationships with foreign states and applying regulatory powers to foreign entities that do business with the United States.

Recommendation 5

The State Department should aggressively support foreign criminalization of biological weapons development and the establishment of biosafety and biosecurity regulations under the framework of the United Nations Security Council Resolution 1540. U.S. law enforcement and intelligence agencies should jointly sponsor biological weapons information sharing events with foreign police forces.

Developing close relationships with foreign governments on the biological weapons issue will be imperative if the United States is to better achieve its goals of monitoring and containing biological threats. Perhaps most importantly, the United States can bring its powers of suasion to bear on states to adopt domestic legislation that criminalizes biological weapons and establishes domestic controls to prevent proliferation—as they are obligated to do under the terms of United Nations Security Council Resolution 1540.

Criminalization will facilitate cooperation from liaison services, which are more likely to assist the United States in contexts where their domestic laws are violated. U.S. law enforcement and intelligence agencies should make cooperation with foreign officials a priority, and should establish regular information sharing events with foreign police forces to assist them in honing their awareness of the biological weapons threat and encouraging cooperation.

Recommendation 6

The United States should remain actively engaged in designing and implementing both international and regulatory inspection regimes. It should consider extending its existing biosecurity and biosafety regulations to foreign institutions with commercial ties to the United States, using the possibility of increased liability, reduced patent protection, or more burdensome and costly inspections to encourage compliance with appropriate safeguards.

International inspections will—at least with respect to state programs—remain an important counterproliferation tool in the future.[36] Arguably, designing effective inspection regimes will become all the more critical in a future where proliferation increasingly involves countries with small (and therefore difficult to detect) chemical, biological, and nuclear weapons programs. The benefits to having on-the-ground access to suspect facilities could be substantial.

There is little prospect in the near future for an international biological weapons inspection regime, however. The United States should therefore seek to obtain some of the benefits of inspections through the use of creative regulatory approaches. One such approach would involve a traditional regulatory model of imposing obligations on international businesses. The approach would build on Executive Order 12938 as amended,[37] which directs the Sec-

retary of Treasury to prohibit the importation into the United States of products produced by a foreign person or company who "materially contributed or attempted to contribute to" the development, production, stockpiling, or acquisition of weapons of mass destruction.[38] More vigorous enforcement of this order would begin to reduce the biological weapons proliferation vulnerabilities that arise through lax internal controls in the private sector.

How might such a regime work? All companies that handle dangerous pathogens could be required to meet security standards and provide data about their facilities, as is already being done inside the United States. This need not be a unilateral undertaking. Objections from major trading partners could be reduced through cooperative inspection agreements with, for example, the United States, the European Union, and Japan. Compliance by individual companies could be ensured with a mix of carrot and stick—such as "fast lane" border controls, whereby companies that adhere to United States standards are granted speedier customs processing at our ports and airports; with the possibility of reduced liability protections and patent protections for the uncooperative.

Conclusion

Improvements in intelligence are no guarantee against a successful biological attack, but they could make such an attack substantially less likely to succeed. There are no perfect solutions, but there are better solutions than the ones we have today. For now, better is all we can do. Given the potential costs of a biological weapons attack, better is what we must do.

NUCLEAR WEAPONS

Introduction

For the Cold War-era Intelligence Community, the challenge of nuclear proliferation was menacing but manageable. The Community focused primarily on intelligence collection against a few states seeking to join the "Nuclear Club"—with an especially watchful eye directed toward states aligned with the Soviet Union.

Although tracking proliferation developments was an important and large-scale enterprise, the world's accumulated storehouse of nuclear material and

knowledge was relatively well accounted for (at least internally) by nuclear states. Moreover, the number of potential nuclear proliferators and their prospective state clients were relatively few, and the potential pathways for transferring nuclear material were reasonably well known and could be monitored—in theory at least—by traditional collection platforms.

Today's nuclear proliferation threat is much more diverse, and the challenges are more difficult. The state-based threat remains, and has been joined by the nightmarish possibility that non-state actors like terrorist groups could obtain a nuclear weapon or a "dirty bomb" and detonate it in the heart of a major American city.[39] Simultaneously, the sources of nuclear materials and expertise have themselves dramatically proliferated. The breakup of the Soviet Union has left a large body of poorly secured, dubiously inventoried nuclear materials and weapons, about which the Community knows precious little. Meanwhile, shadowy, non-state proliferation networks have appeared, quietly peddling their products to the highest bidder. These new nuclear proliferators and their customers operate under a veil of secrecy, including the use of front companies to mask their intentions and movements. It is the misfortune of our age to witness the globalization of trade in the ultimate weapon of mass destruction.

There are many facets to the nuclear proliferation problem; here we focus on but two of the most important—the availability of unsecured nuclear weapons and materials, or "loose nukes," and the appearance of non-state nuclear "brokers." We believe that the Intelligence Community must do much more to improve its collection capabilities with regard to both, for the purpose of halting nuclear proliferation at the *source*. That said, we recognize the inherent difficulty of both targets, as well as the limitations on our ability to contribute much in the way of concrete operational recommendations as to how the community can improve in this regard (other than the understandable, but rather unhelpful, advice, to "try harder" and "spend more" on the endeavor). Consequently, as we discuss later in this chapter, our recommendations focus on improving the process for interdicting nuclear materials once they are in transit from the proliferators or, as a last resort, on their way to the United States.

Loose Nukes: The Great Unknown

The single greatest hurdle to a terrorist's fabrication of a nuclear device is the acquisition of weapons-usable nuclear material.[40] If terrorists are able to pro-

cure such material intact, they can skip this most difficult part of the nuclear weapons development cycle. Just as Willie Sutton robbed banks "because that's where the money is," terrorist groups are most likely seeking nuclear material from the former Soviet Union because that is where the most material is available.[41] (Additional information concerning terrorist efforts to obtain nuclear material is presented in the classified report but cannot be discussed here.) Tracking this nuclear material in the former Soviet Union is exceedingly difficult. However, we would like to emphasize that the United States has not made collection on loose nukes a high priority.

In our classified report we discuss in greater detail the reasons why our efforts to collect intelligence in this area have struggled, and we offer suggestions for improvement that cannot be discussed in an unclassified format. While we have generally shied away from simply recommending "more" effort or funding, we believe that some of these techniques may require additional funding.

The loose nukes problem is in many ways indicative of problems facing the Intelligence Community as a whole. Analysts and collectors are too consumed with daily intelligence requirements to formulate or implement new approaches. The war on terrorism and ongoing military operations have distracted the Community from longer-term threats of critical importance to national security. The perception is that there is no "crisis" until a weapon or fissile material is stolen. The problem, of course, is that we might not know this was the case until we are jolted by news of a catastrophe in Washington, D.C. or midtown Manhattan.

Established Nuclear Powers: China & Russia

While the discussion in this section has focused on the emerging intelligence challenges resulting from the proliferation of nuclear weapons and related materials, we recognize that the traditional threat of nuclear weapons in the hands of determined state adversaries remains alive and well and requires the continued attention of policymakers and the Intelligence Community. The nuclear arsenals and emerging capabilities of China and Russia, in particular, pose a challenge to the United States—a challenge about which the Intelligence Community today knows too little. In our classified report we detail some of the struggles the Intelligence Community has had in developing information about these more traditional targets—but we cannot elaborate upon our findings in this area in this report.

The Khan Network: "One-Stop Shopping" for Proliferation

Private proliferators and the "grey market" for nuclear trafficking pose another emerging threat. States no longer have a monopoly on sophisticated nuclear technology, materials, and expertise. The insecurity of nuclear materials, combined with diffusion of the technical knowledge necessary to construct or assemble a nuclear device, has resulted in a burgeoning industry for entrepreneurial middlemen. As demonstrated in our Libya case study, this threat requires new intelligence approaches.

Former Director of Central Intelligence George Tenet has spoken publicly about the "emerging threat" posed by private proliferators like A.Q. Khan.[42] As the father of Pakistan's atomic bomb, Khan helped pioneer the practice of clandestine nuclear procurement. Through front companies, subsidiaries, and a network that stretched from Pakistan to Europe,[43] Khan sought to provide countries with "one-stop shopping" for nuclear goods. We now know that Khan's network supplied nuclear equipment and expertise that "shav[ed] years off the nuclear weapons development timelines of several states including Libya."[44] Among other things, Khan's network supplied Libya with nuclear centrifuge technology.[45]

Working alongside British counterparts, CIA's Directorate of Operations was able to penetrate and unravel many of Khan's activities through human spies. They deserve great credit for this impressive success. However, the effort dedicated to bringing down the network demonstrates how rare and hard-fought future successes may be. It is possible, although unlikely, that Khan is unique. Private dealers, after all, control many of the materials needed for nuclear weapons production.

The A.Q. Khan achievement also suggests that the Intelligence Community will meet with limited success if it acts alone. Combating proliferation networks requires insight into the networks' modes of operation; for example, understanding the front companies through which they operate. As we discuss more fully in the interdiction section below, the Intelligence Community must reach out to non-traditional partners elsewhere in the government to augment its own capabilities.

Conclusion

There is little more frightening than the thought of terrorists detonating a nuclear device within the United States. And events of the past decade—including the questionable security of former-Soviet nuclear material, the emergence of private proliferation threats like A.Q. Khan, and the rise of terrorist groups determined to strike U.S. territory—have added to the threat. Furthermore, there is no good reason to expect that North Korea and Iran will be the last states to try to acquire nuclear weapons. Indeed, acquisition by these two countries might set off a cascade of efforts by others in East Asia and the Middle East. (Nor is there a good reason to expect that states of concern will only be the neighbors of these two countries and others possessing nuclear weapons. It is worth remembering that South Africa, remote in many ways from the central regions of the Cold War, made them.) We believe that our recommendations for reform discussed elsewhere in the report, in combination with this chapter's discussion of intelligence support to interdiction and leveraging regulatory mechanisms for intelligence, will at least help the Intelligence Community be as prepared as it can be.

CHEMICAL WEAPONS

Even when unintentionally released, poisonous chemicals can have terrible effects. An accidental release of poisonous gas from a chemical plant in Bhopal, India, killed thousands in 1984.[46] Deliberate chemical attacks, of course, have the potential to be even worse. In 1995, the Japanese cult Aum Shinrikyo released the chemical nerve agent sarin on the Tokyo subway, killing twelve people, sending more than 5,500 to the hospital, and sowing fear throughout the city.[47] Commentators attributed the relatively low number of fatalities to the poor quality of the agent and Aum Shinrikyo's inefficient dispersal devices.[48] In our classified report, we offer further examples of suspected chemical weapons plots that cannot be discussed in an unclassified format.

While biological and nuclear weapons could cause the worst damage, terrorists could kill thousands of Americans by simply sabotaging industrial chemical facilities. And, due to the large volume and easy accessibility of toxic chemicals in the United States, a chemical attack causing mass casualties may be more likely than a nuclear or biological attack in the near term.

As with biological and nuclear threats, the Intelligence Community is poorly positioned to meet the challenges posed by chemical weapons. Historically, it has focused on state programs and has only recently turned its attention to potential uses of chemical weapons by terrorist groups. The Community's task is complicated by the ubiquity of toxic chemicals—which are available for sale across the United States and the world—and the relative ease with which other, even more deadly substances can be manufactured from common chemical precursors. Moreover, given the increasing sophistication of the chemical industry and the various dual uses of its products, the Community will face an increasingly difficult task in differentiating legitimate from potentially hostile manufacturing efforts. Finally, as is the case with biological weapons, many small-scale chemical production facilities can be concealed in nondescript facilities that are not easily detectable through conventional collection means, such as imagery.

The Intelligence Community certainly needs to do everything possible to collect on the plans and intentions of those terrorist groups that would use chemical weapons in an attack on the United States. Moreover, because of the easy accessibility of toxic chemicals and chemical precursors, it is essential that the Community develop strong links with the FBI, which may be better suited to monitor and respond to suspicious purchases of chemicals on the state and local level and to interface with local law enforcement for the same purpose.

Such traditional intelligence activities are necessary. But as our discussion about nuclear proliferation above demonstrates, traditional methods of intelligence collection have not proved particularly adept at monitoring "loose nukes," and there are serious questions as to whether the Community will be able to detect and disrupt new, diffuse proliferation networks that acquire and traffic in nuclear materials. Without admitting defeat, we must acknowledge the possibility that nuclear materials and perhaps nuclear weapons will find their way into the international transportation stream; bound for terrorists or rogue states, who will in turn attempt to bring them to the United States. A similarly disturbing state of affairs exists with regard to chemical weapons—as the sheer volume and availability of chemicals at home and abroad indicate that it is likely such weapons or materials will come into the hands of those who would do us harm.

As a result, it seems clear that in addition to improving its traditional collection capabilities, the Intelligence Community should also focus on improving

its capabilities with regard to directly supporting interdiction activities, both inside and out of the United States, and to fully utilizing the regulatory and legal mechanisms at our disposal for controlling proliferators. It is to these tasks that we now turn.

THE INTERDICTION CHALLENGE: INTELLIGENCE FOR ACTION

Introduction

The United States has articulated a broad and aggressive policy that emphasizes the seizure or disruption of proliferation-related materials bound for states or individuals.[49] However, the Intelligence Community is currently ill-equipped to support this policy. As one senior national security official told the Commission, counterproliferation interdiction requires "a whole intelligence support mechanism…that we don't have."[50]

First, the Intelligence Community must collect information from a wide variety of non-traditional sources, ranging from customs officials to private parties. Second, the Community must provide information to a wide variety of non-traditional customers, ranging from foreign partners to law enforcement. But perhaps most importantly, the intelligence process—collection, analysis, and dissemination—must be much faster and more action-oriented than has traditionally been the case. If intelligence officials detect information about an illicit nuclear shipment, they cannot wait weeks for their analytical units to produce "finished intelligence," or for policy entities to approve an interdiction response. In this regard, support to interdiction must resemble counterterrorism or counternarcotics intelligence support; it must be quick, integrated, and accurate.

In this section we will address the broad theme of intelligence support to the interdiction of weapons of mass destruction, and make recommendations designed to address these basic requirements. We propose a new model for coordinating and executing interdiction, as well as several specific suggestions that could improve the Community's collection efforts and help to protect our borders.

Although the discussion below could apply to any weapon of mass destruction, in the near-term it is likely to pertain primarily to nuclear devices and

chemical materials; detection and interdiction of biological substances is particularly difficult given the dual-use nature of biological equipment and the lack of discernible signatures attributed to biological materials. As was demonstrated in 2001, a biological weapon can be effectively delivered, undetected, in an envelope.

Improving the Flow of Information

To support interdiction, the Community must tap into a wide variety of information networks that are, in many cases, outside of the Intelligence Community. Counterterrorism and counternarcotics intelligence have already taken significant steps in this regard. Counterproliferation intelligence must follow suit.

One critical information source is the Department of Homeland Security, which controls several databases that can help tip off analysts and operators looking for proliferation targets. For example, two main components of Homeland Security—Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP)—operate a variety of databases that follow flows of people and goods across U.S. borders. These databases provide a rich source of data for relationship mapping and link-analysis among foreign companies and individuals. Yet our interviews with operators have revealed serious information sharing problems between Homeland Security and the Intelligence Community that dramatically limit their usefulness. Our classified report offers examples of these information sharing difficulties and of one successful program run by the Office of Naval Intelligence.

Developing Tools to Do It in Real Time

Effective interdiction also requires that policymakers and operators have new analytical tools that can extract information from the Intelligence Community in real time.[51] Ships carrying nuclear material will not wait for a lengthy analysis to run its course before delivering their cargoes.

For example, to support counternarcotics interdictions Joint Interagency Task Force-South has link-analysis tools that, if shared on a government-wide basis, would permit operators to quickly establish connections among terrorist organizations, proliferation networks, and other dubious international activities.[52] Rather than starting with such existing assets, nearly every intelligence, law enforcement, or military entity involved in counterproliferation is also

developing similar tools. A National Security Council-commissioned report by the Community's Collection Concepts Development Center concluded in November 2003 that these efforts composed a "'Balkan gaggle' of sometimes redundant programs with little coordination and incomplete operational integration."[53] The DNI should use his authority to encourage development of these tools and coordinate agency efforts.

Carrying out effective interdictions also requires real time awareness of activities in the sea and the air.[54] The Coast Guard's Maritime Domain Awareness program and the recent National Security Presidential Directive articulating a Maritime Security Policy are steps in the right direction.[55] There is also an urgent need to share at least some portion of our air and maritime domain awareness information, and our computer-based tools, with international partners who will assist the United States in carrying out interdictions.

The scope of these activities demonstrates that successful interdiction requires a vision that stretches far beyond the Intelligence Community. To restate one of the primary themes we found in our study of proliferation: the Intelligence Community cannot win this battle on its own. Coordination and integration will be necessary.[56]

Going Forward: A Different Model

Currently, interdiction efforts are not sufficiently coordinated across agencies. This is particularly true with respect to operational planning and execution. We do not believe that the National Security Council is the proper locale for managing daily operations—counterproliferation or otherwise. Although the National Security Council plays a critical role in helping to develop government-wide counterproliferation policy, it should not become the center for interagency operations as the United States ramps up its interdiction capability.

Recommendation 7

The President should establish a Counterproliferation Joint Interagency Task Force to conduct counterproliferation interdiction operations; to detect, monitor, and handoff suspected proliferation targets; and to coordinate interagency and partner nations' counterproliferation activities.

A new Joint Interagency Task Force for counterproliferation would fill the role of planning and executing interdiction operations, drawing on the full range of military, law enforcement, and intelligence capabilities of the United States. Ideally, a Counterproliferation Joint Interagency Task Force would be flexible enough to support the operational needs of U.S. Strategic Command[57] or any other entity tasked with stopping, seizing, or destroying a given cargo.[58] The Task Force would contain diplomatic, military, intelligence, law enforcement, and other representatives from across the government. We recommend that it:

- Plan and execute the full range of overt and clandestine interdiction operations;
- Seek approval from the National Security Council for interdiction operational plans through the real-time decisionmaking process described below;
- Provide tactical and operational intelligence, air, and sea support to the Department of Defense Unified Commands to carry out particular operations;
- Establish the legal basis for all interdiction operations, including through agreements with consenting private sector actors and partner nations that have signed ship-boarding agreements;
- Coordinate country team and partner nation initiatives in order to defeat the flow of materials of proliferation concern; and
- Conduct regular interdiction gaming exercises with international partners to develop new operational plans and concepts.

Recommendation 8

The DNI should designate the National Counter Proliferation Center as the Intelligence Community's leader for interdiction-related issues and direct the Center to support the all-source intelligence needs of the Counterproliferation Joint Interagency Task Force, the National Security Council, and other customers.

As described in Chapter Six (Leadership and Management), our proposed National Counter Proliferation Center (NCPC) will serve a variety of functions. With regard to interdiction, the NCPC will fulfill the requirements of the Counterproliferation Joint Interagency Task Force, the National Security Council, and a growing body of counterproliferation intelligence users. Through a Target Development Board, the NCPC would prioritize and target for interdiction those proliferation networks of greatest strategic concern. Finally, the NCPC would ensure that the Intelligence Community provides the Task Force and the National Security Council with real-time proliferation intelligence support.

Recommendation 9

The President should establish, probably through a National Security Presidential Directive, a real-time, interagency decisionmaking process for counterproliferation interdiction operations, borrowing from Presidential Directive 27, the interagency decisionmaking process that supports counternarcotics interdictions.

The National Security Council currently holds a weekly interdiction sub-Policy Coordinating Committee meeting to identify potential interdiction targets and determine courses of action.[59] Since counterproliferation interdiction targets may often involve sensitive diplomatic and legal issues, the National Security Council will want to approve operational interdiction plans prior to execution. The time sensitivity of certain interdiction operations suggests that the National Security Council should adopt a virtual decision-making process-—one in which parties can consult remotely-—to accomplish this oversight function.

To streamline and clarify the counterproliferation interdiction process, we recommend a set of procedures similar to those established by Presidential Directive 27 for dealing with counternarcotics interdictions and other "types of non-military incidents."[60] Because interdictions may involve military operations that would conflict with covert activities, we recommend a separate National Security Presidential Directive that outlines the National Security Council process for supervising the planning and execution of interdiction operations. To make these decisions, National Security Council staff and senior policymakers will need intelligence to answer a range of questions.

Unlike the existing intelligence paradigm, which is heavily reliant on the production of "finished" intelligence products, interdiction may require, for example, that military commanders or customs officials communicate directly with collectors and analysts.

Recommendation 10

The State Department should enter into additional bilateral ship-boarding agreements that also help to meet the tagging, tracking, and locating requirements of the Intelligence Community and its users.

The State Department is currently charged with responsibility to secure bilateral ship-boarding agreements in support of the Proliferation Security Initiative.[61] To date, the Department has secured three important agreements.[62] We do not believe, however, that sufficient strategic thought has been directed toward how these agreements can be structured to serve intelligence purposes.

Through such bilateral agreements or related customs regulations, the State Department could, for example, require ships and aircraft to declare their locations through GPS and satellite uplink. Failure to report location information could be viewed as the rough equivalent of driving with a broken taillight, and might establish reasonable suspicion to conduct an interdiction. Such agreements and the imposition of other tracking requirements would enable intelligence to draw on new sources of data to monitor potential cargoes, vessels, and aircraft of proliferation concern.[63]

Protecting our Borders: The Department of Homeland Security

Recommendation 11

The DNI should ensure that Customs and Border Protection has the most up-to-date terrorism and proliferation intelligence. In turn, Customs and Border Protection should ensure that the National Counterterrorism Center and National Counter Proliferation Center have real-time access to its databases.

It may not be possible in all cases to identify and halt biological, nuclear, or chemical weapons shipments before they reach the United States. In such

cases, our last line of defense is detecting and stopping these shipments as they cross our border. The Department of Homeland Security, through Customs and Border Protection, collects information on incoming cargo shipments that the Intelligence Community must learn to exploit. The flip side of this equation is equally important—Customs and Border Protection needs threat information from the Intelligence Community to target shipments of concern headed to the United States. Plainly, Homeland Security and the Intelligence Community need to strengthen their relationship. A discussion of ways in which this relationship can be improved is in the classified version of our report, but cannot be discussed in an unclassified format.

If we are to increase our chances of detecting proliferation materials before they enter the United States, it is critical that Homeland Security work closely with the Intelligence Community in developing its plans for screening materials coming into the United States. Moreover, once the plans are instituted, Homeland Security and the Intelligence Community must maintain a close relationship to ensure that homeland security policies reflect the Intelligence Community's most current assessments.

Recommendation 12

The DNI and Secretary of Homeland Security should undertake a research and development program to develop better sensors capable of detecting nuclear-related materials. The effort should be part of a larger border defense initiative to foster greater intelligence support to law enforcement at our nation's borders.

The Intelligence Community's collaboration with the Department of Homeland Security should not stop at targeting cargoes. A comprehensive border defense initiative would employ an array of advanced technologies to protect our borders. For example, reconnaissance satellites, unmanned aerial vehicles, nuclear detection technologies, and biometric identification cards could all play a role in border protection.

Many critical technologies to protect the border, are still in their infancy. A senior official at the Department of Homeland Security laments that the sensors deployed at our borders are "way below ideal."[64] Customs and Border Protection officials complain that some detectors are imprecise and prone to

false alarms.[65] A concerted research and development effort is necessary to bring these technologies to maturity. A new sense of urgency is required.

ENLISTING COMMERCE AND TREASURY TO COMBAT PROLIFERATION

Introduction

The Intelligence Community will be most effective at combating chemical, biological, and nuclear threats if it works in concert with non-traditional government partners. Legal and regulatory regimes can help enable better intelligence gathering and disrupt proliferation-related activity.

On several occasions throughout our inquiry, departments and agencies outside of the Intelligence Community asked why our Commission was interested in their work. These comments illustrate the lack of connection between the Intelligence Community and large parts of the government. The Community often sees itself as a world apart, and it is viewed by outsiders as an unapproachable exotic.

In the area of proliferation in particular, such a failure to see beyond the Intelligence Community's borders—and a failure to acknowledge what intelligence can and cannot do—has deprived the country of anti-proliferation levers that it badly needs. As we saw with biological weapons, the lack of an effective (and truly reciprocal) relationship between intelligence and biological sciences has limited the Community's efforts. Similarly, the Community has not sufficiently harnessed the power of legal and regulatory regimes, and the synergies that could result from working more closely with them. While we did not seek to reach beyond the scope of our mandate, which is to study the Intelligence Community, the Commission did look at some ways in which legal and regulatory regimes might enhance intelligence collection specific to the counterproliferation issue.

We do not pretend to have weighed fully every non-intelligence interest at work in many of these regimes. For that reason, many of our recommendations only suggest areas for possible action by both the affected agency and the Intelligence Community. But regardless of whether specific regimes are instituted, we believe that closer cooperation between the Intelligence Community and the Departments of Commerce and Treasury could result in many

mutually beneficial relationships and improved collection against difficult proliferation-related targets. The Intelligence Community will be most effective at combating chemical, biological, and nuclear threats if it works in concert with non-traditional government partners.

Department of Commerce: Enforcing the Export Control Regime

The Department of Commerce's Bureau of Industry and Security (BIS) administers and enforces the Export Administration Regulations, which govern the export of dual-use items. BIS's law enforcement authorities place it in a position to collect large amounts of information that could be of great use to the Intelligence Community.

In order to obtain the cooperation of export control violators, however, BIS needs stronger law enforcement powers, something it has lacked in recent years, mainly because some of BIS's law enforcement authorities lapsed when the Export Administration Act expired. BIS could also assist the Intelligence Community more fully if it had authority to impose increased penalties for export violations and more authority to conduct undercover activities of potential intelligence value. The Administration has supported a renewal of the act that would confer these authorities, and congressional action on renewal would make cooperation between BIS and the Intelligence Community more productive.

The Export Administration Regulations provide additional opportunities to support counterproliferation efforts. Specifically, BIS inspections, the conditions BIS imposes on export licenses, and BIS's possible access to corporate records may provide valuable intelligence and counterproliferation opportunities. We discuss these and other related matters, including two classified recommendations, more fully in our classified report.

Recommendations 13 & 14

These recommendations are classified.

Department of the Treasury: Stopping Proliferation Financiers

The Treasury Department can also provide more support to counterproliferation than it does today. The Department currently has two powerful authorities with respect to terrorism that do not now apply to proliferation. The first is the authority to freeze the assets of terrorists and their financiers; the second is the authority to take action against foreign financial institutions that allow their services to be used to support terrorism. We see no reason why these same authorities should not be enhanced to also combat proliferation.

Recommendation 15

The President should expand the scope of Executive Order 13224 beyond terrorism to enable the Department of the Treasury to block the assets of persons and entities who provide financial support to proliferation.

Pursuant to the International Emergency Economic Powers Act, the President authorized the Department of the Treasury to block the assets of persons who sponsor terrorism.[66] However, Treasury lacks a similar tool to block the assets of proliferators. To fill this gap, we recommend the President take steps to allow the Secretary of the Treasury to take the same action against persons "who provide financial or other material support to entities involved in the proliferation of weapons of mass destruction." In light of the virtually universal recognition that the greatest threat the United States faces is the intersection of terrorism and proliferation, we see no reason why Treasury's authority should extend to only half of this potentially catastrophic combination.

Recommendation 16

The President should seek to have Congress amend Section 311 of the USA PATRIOT Act in order to give the Department of the Treasury the authority to designate foreign business entities involved in proliferation as "primary money laundering concerns."

Currently, section 311 of the USA PATRIOT Act authorizes the Secretary of the Treasury—in consultation with other federal officers, including the Secretary of State and the Chair of the Board of Governors of the Federal Reserve System—to designate a foreign jurisdiction or financial institution a "primary

money laundering concern," and to require that U.S. financial institutions take certain measures against the designee.[67] This power can be used when the Intelligence Community determines that a foreign financial institution is involved in proliferation-related activity. And by doing so, the Department can effectively cut the foreign institution off from the U.S. banking system. This authority is limited, however to financial institutions that assist proliferation. It would be more effective if it could also be applied to *non-financial* business entities involved in proliferation.

The reason for this suggested change is simple—many aspects of proliferation involve non-financial institutions, such as pharmaceutical, petrochemical, and high-tech companies. By limiting the Treasury Department's designation authority to financial institutions, the current law effectively addresses only one part of the business-related proliferation challenge. Expanding Treasury's authority would thus allow the U.S. government to also take action against the very businesses that supply the materials that make proliferation possible.

Specifically, we believe the Secretary's authorities should extend to the designation of individual businesses involved in proliferation as "primary money laundering concerns." Once a business was so designated, U.S. financial institutions could be required by the Treasury Department to take certain steps to avoid engaging in business transactions with the designated companies. The Secretary of the Treasury might also be able to affect whether foreign financial institutions are willing to conduct business with business entities involved in proliferation. If so, the Secretary of the Treasury could help cut off proliferators from their financial lifeblood.

Conclusion

Legal and regulatory mechanisms are valuable tools the Intelligence Community should use to their full extent. But proper use of these mechanisms requires extensive interagency cooperation. This will not be an easy task. But we believe it is a worthwhile endeavor, and one that may—in the long run—prove invaluable in combating the proliferation of nuclear, biological, and chemical weapons.

ENDNOTES

[1] Center for Counterproliferation Research, *Anthrax in America: A Chronology and Analysis of the Fall 2001 Attacks* (Nov. 2002) at p. 2.

[2] Interview with FBI official (Nov. 19, 2004).

[3] Interview with Dugway Proving Ground official (Dec. 30, 2004); *Final Report of the National Commission on Terrorist Attacks Upon the United* States (authorized edition) (2004) at p. 172 (hereinafter "9/11 Commission Report").

[4] The anthrax letter mailed to Senator Patrick Leahy had 1 trillion spores per gram. Interview with FBI special agent (Nov. 19, 2004). Inhalation of 8,000 to 10,000 spores is generally regarded as lethal, but this figure derives from studies of healthy "middle-aged" primates. Thomas V. Inglesby et al., "Anthrax as a Biological Weapon, 2002: Updated Recommendations for Management," *Journal of the American Medical Association*, vol. 287 (May 1, 2002) at pp. 2236-2252. If we accept this lethality estimate, a gram perfectly disseminated under optimal weather conditions could theoretically kill 100,000 people. Optimum weather conditions and highly efficient dissemination are unlikely, however, since weather patterns and aerosolization efficiency, among numerous other factors, would significantly alter lethality figures. National Research Council, *Making the Nation Safer* (2002) at p. 81. It is a reasonable assumption, however, that liquid or powder dissemination could kill one-thousandth to one-hundredth of those people (*i.e.*, 100 to 1,000 people). Richard Danzig, *Catastrophic Bioterrorism—What Is To Be Done?* (Aug. 2003) at pp. 1-2.

[5] In this example, a kilogram would contain 1,000 trillion anthrax spores.

[6] Richard Danzig, *Catastrophic Bioterrorism—What Is To Be Done?* (Aug. 2003) at p. 2; Brad Roberts, Institute for Defense Analyses, *Defining the Challenges of Campaign-type Responses to Campaign-type Terrorism* (Jan. 2, 2004).

[7] Interview with senior administration official (Dec. 16, 2004).

[8] NIC, Title Classified (NIE 2004-08HC/I) (Dec. 2004) at p. 24.

[9] Interview with senior intelligence official (Oct. 14, 2004).

[10] Tom Mangold and Jeff Goldberg, *Plague Wars: the Terrifying Reality of Biological Warfare* (2001) at p. 61.

[11] Tara O'Toole, Michael Mair, and Thomas Inglesby, *Shining Light on 'Dark Winter'* (2002).

[12] For example, in 2002, researchers at the University of Pittsburgh identified key proteins in *variola* (smallpox) that contribute to its virulence and demonstrated how to synthesize the virulence gene via genetic modification of smallpox's less deadly cousin *vaccina*. A. M. Rosengard, Y. Liu, Z. P. Nie, and R. Jimenez, "Variola Virus Immune Evasion Design: Expression of a Highly Efficient Inhibitor of Human Complement," *Proceedings of the National Academies of Sciences of the United States of America* (Vol. 99) (June 25, 2002) at pp. 8808-8813.

[13] Interview with senior intelligence official (Dec. 6, 2004).

[14] NIC, *Iraq's Continuing Programs for Weapons of Mass Destruction* (NIE 2002-16HC) (Oct. 2002) at pp. 5, 35. The Intelligence Community also judged that Iraq maintained delivery systems for its biological weapons agents. *Id.* at p. 7.

[15] Iraq Survey Group, *Comprehensive Report of the Special Advisor to the DCI on Iraqi*

WMD, Volume III, "Biological Warfare" (Sept. 30, 2004) at p. 1.

[16] NIC, Title Classified (NIE 2004-08HC/I) (Dec. 2004) at p. 59.

[17] Interview with senior intelligence officer (Nov. 18, 2004).

[18] Interview with senior analyst, Institute for Defense Analyses (Jan. 28, 2005).

[19] Interview with senior intelligence officer (Nov. 18, 2004).

[20] The United States spent about $14.5 billion on civilian biodefense between FY 2001 and FY 2004, and there is an additional $7.6 billion requested for FY 2005. The funds have primarily gone to the Departments of Health and Human Services (HHS) and Homeland Security (DHS), and have supported numerous initiatives to develop vaccines, environmental sensors, and emergency response capabilities. Ari Schuler, "Billions for Biodefense: Federal Agency Biodefense Funding, FY2001-FY2005," *Biosecurity and Bioterrorism: Biodefense, Strategy, Practice, and Science* (Vol. 2) (2004) at p. 86. Interview with CIA senior scientist (Jan. 18, 2005); Interview with CIA DS&T official (Jan. 19, 2005).

[21] Interview with senior administration official (Jan. 5, 2005).

[22] Interview with senior CDC official (Nov. 19, 2004).

[23] Observation made by Seth Carus, National Defense University, as related in NIC, Title Classified (NIE 2004-08HC/I) (Dec. 2004), at pp. 60-61.

[24] Interview with senior NIH official (Feb. 4, 2005).

[25] *Id.*

[26] Interview with senior intelligence official (Nov. 18, 2004); CIA has one promising effort that is in its nascent stages.

[27] Interview with CIA senior scientist (Jan. 25, 2005); Interview with biosecurity expert (Feb. 4, 2005).

[28] Interview with senior National Security Council official (Jan. 5, 2005).

[29] Interview with the Department of Homeland Security's Directorate of Science and Technology official (Nov. 15, 2004).

[30] *Id.*

[31] Ron Southwick, "Elite Panel of Academics Wins Fight to Continue Advising Military," *The Chronicle of Higher Education* (June 7, 2002). Today, the JASONs include experts from other scientific specialties as well. *Id.*

[32] CIA, Title Classified (OTI SF 2003-108) (Nov. 3, 2003)

[33] The legislation designates the Joint Intelligence Community Council as responsible for advising the DNI on "establishing requirements…and monitoring and evaluating the performance of the Intelligence Community." Intelligence Reform and Terrorism Prevention Act of 2004 at § 1031, Pub. L. No. 108-458.

[34] Classified examples concerning the Intelligence Community's collection efforts are contained in our classified report, but could not be included in an unclassified discussion.

[35] Interview with CIA senior scientist (Jan. 25, 2005).

[36] *See, e.g.*, International Atomic Energy Agency, Staff Report, *UN General Assembly Backs IAEA's "Indispensable Role"* (Nov. 2, 2004) (noting the IAEA's role in conducting inspections of nuclear programs in Iraq, Iran, and North Korea).

[37] Executive Order 12938 (amended July 28, 1998).

[38]*Id.* at § 4(a).

[39]For current purposes, we define a "dirty bomb" as a radiological dispersal device that uses the force of conventional explosives, such as TNT, to scatter radioactive material.

[40] Interview with Department of Energy intelligence analysts (Jan. 10, 2005).

[41] Interview with DIA analyst (Jan. 18, 2005).

[42] George Tenet, Remarks as prepared for delivery at Georgetown University (Feb. 5, 2004). We discuss the specifics of the A.Q. Khan story in greater detail in our classified report.

[43] *Id.*

[44] *Id.*

[45] Interview with CIA DO official (Sept. 14, 2004).

[46] Satinder Bindra, Bhopal marks chemical tragedy: 20 years since gas leak killed thousands in Indian city (Dec. 3, 2004), *available at* http://edition.cnn.com/2004/WORLD/asiapcf/12/02 /india.bhopal.mark (accessed Feb. 7, 2005).

[47] CIA, Title Classified (CTC 2003-30079H) (Aug. 7, 2003) at p. 4.

[48] *Id.*; Senate Government Affairs Permanent Subcommittee on Investigations Staff Statement, *Global Proliferation of Weapons of Mass Destruction: A Case Study on the Aum Shinrikyo* (Oct. 31, 1995), *available at* www.fas.org/irp/congress/1995_rpt/aum/part05.htm (accessed Feb. 7, 2005).

[49] National Security Presidential Directive-17 (also designated Homeland Security Presidential Directive-4) presents a broad national strategy for countering chemical, biological, and nuclear weapons proliferation that emphasizes interdiction of illicit proliferation transfers. In addition, the Proliferation Security Initiative provides a framework under which the United States and its allies have created agreements to authorize the tracking and interdicting of weapons-related shipments.

[50] Interview with senior administration official (Dec. 17, 2004).

[51] Collection Concepts Development Center, Title Classified (Nov. 21, 2003) at p. 4.

[52] *Id.* at pp. ii-iii.

[53] *Id.* at p. 46.

[54] *Id.* at p. 5.

[55] In particular, the Maritime Security Policy emphasizes the importance of a "robust and coordinated intelligence effort [that] serves as the foundation for effective security efforts in the Maritime Domain." NSC, *NSPD-41/HSPD-13: Maritime Security Policy* (Dec. 21, 2004) at pp. 5-6.

[56] A short classified section concerning how best to coordinate the government's interdiction efforts is omitted from this version of the report.

[57] The Department of Defense has recently named U.S. Strategic Command the lead Unified Command for the interdiction and elimination of weapons of mass destruction. Interview with senior Department of Defense official (Jan. 13, 2005).

[58]Officials from Special Operations Command and the Office of the Secretary of Defense for Policy have faulted the Intelligence Community for not gearing collection requirements toward sufficient levels of operational specificity, and for not quickly sharing the intelligence that is collected. Covert platforms must find an appropriate means to share ("push") information quickly to users, and users must have the capability to "pull" intelligence from the infor-

mation sharing environment with appropriate permissions and standards established by the DNI. OSD/SOLIC, *Nuclear Terrorism Intelligence: A Special Operations Perspective* (briefed on Oct. 26, 2004).

[59]Interview with former administration official (Feb. 7, 2005).

[60] Presidential Directive-27 was designed to enable expeditious decisionmaking, consider views of "concerned Departments and agencies," coordinate public statements, and "keep the White House fully informed throughout." *PD-27: Procedures for Dealing with Non-Military Incidents* (Jan. 19, 1978).

[61] The Proliferation Security Initiative is a framework under which the United States and its allies have created agreements to authorize the tracking and interdicting of weapons and materials of proliferation concern.

[62] Each of the three—Liberia, Panama, and the Marshall Islands—is significant because of the large number of vessels that are flagged there.

[63] Office of Naval Intelligence analysts confirm that this would indeed be helpful. Interview with National Maritime Intelligence Center officials (Feb. 14, 2005).

[64] Interview with Department of Homeland Security official (Oct. 7, 2004).

[65] Interview with Customs and Border Protection officials (Feb. 18, 2004). Interview with Customs and Border Protection officials (Jan. 21, 2005).

[66] Executive Order 13224 at § 1(d).

[67] 50 U.S.C. § 5318A.