**VIEWPOINT:**
**ENSURING THE SECURITY OF RUSSIA’S CHEMICAL WEAPONS:**
**A LAB-TO-LAB PARTNERING PROGRAM**

by Kathleen Vogel

March 20, 1995, is a date etched in history. On that day, in a crowded Tokyo subway, the religious cult Aum Shinrikyo staged the first major terrorist use of chemical weapons (CW). The attack killed 12 and injured over 5,000 passengers. Only a fortunate bungling of the operation prevented thousands from being killed. Although nearly 400 cult members have been arrested for their involvement in the subway attack and other terrorist activities, many more of the cult’s criminals (some inevitably with CW expertise) are still at large.

Recent investigations of the attack have uncovered alarming information about Aum’s international efforts to procure high-tech equipment needed to produce weapons of mass destruction (WMD). This information reveals that a range of sensitive materials from the former Soviet Union (FSU) may be vulnerable to leakage. Aum leaders repeatedly visited the FSU to secure weapons and know-how. A Soviet-made MI-17 helicopter, gun models, and weapons blueprints were acquired by the Aum on several different occasions. Russian documents for gas-laser weapons, space-launch rockets, and nuclear weapons were also seized from cult members, although these weapons were never purchased. Russian officials have denied allegations that they helped Aum acquire armaments, but connections with Russian government and military figures have been reported by Russian and Japanese news sources. The combination of the cult’s extensive financial holdings (estimated at over $1 billion) and Russia’s desperate economic situation, with its rampant corruption and organized crime elements in the military and government, create an environment ripe for illegal transfer of WMD and related technologies from the former Soviet Union.

Prior to the 1995 subway attack, Aum’s activities and intentions were largely unknown. As one senior US law enforcement official has admitted, “they weren’t on our radar screen.” Although the cult continues to operate worldwide, its activities are now closely monitored. It is difficult to predict, however, whether Aum or other terrorist groups are plotting for another chemical attack—this time, perhaps, on US soil. As President Bill Clinton asserts, “In light of what happened in Japan, all advanced countries should be very, very concerned about the prospect of the merger of terrorism with weapons of mass destruction.”

Due to dire economic conditions in the former Soviet Union, security measures around Russian weapons facilities are poorly maintained, making insider theft or terrorist attack possible. The vulnerability of Russia’s CW has been made plain in recent news headlines. In 1996, through an undercover sting operation, the Istanbul Security Directorate seized Russian-made mustard gas and sarin. According to the Istanbul newspaper, Hurriyet, detectives agreed to buy 20 tubes of CW agents from seller Emin Ekinci for $1 million. Ekinci arrived at the exchange carrying the tubes of nerve and blister agents in a plastic bag and was promptly arrested after the transaction. In his subsequent interrogation by police, Ekinci disclosed that he had acquired the mustard gas from a former KGB officer in Russia. Ekinci’s deposition states that he was prepared to sell the containers to anyone who would pay for them. In 1997, Chechnyan terrorist leader Salman Raduyev declared his acquisition of Russian chemical weapons and made public threats to use them. More recently, the London Times has alleged that Hezbollah guerillas have attempted to purchase chemical and biological weapons from Eastern Europe. These purported cases of acquisition or diversion reinforce the chilling reality that terrorists have expressed a keen interest in securing chemical weaponry from the former Soviet Union, posing a real threat to US and international security.

With chemical terrorism now a frightening reality, it is in the US national interest to assist Russia in guarding

---

Kathleen Vogel is a post-doctoral fellow at the Center for Nonproliferation Studies at the Monterey Institute of International Studies in Monterey, California. She received a Ph.D. in Chemistry from Princeton University.
its chemical stockpile. The United States has committed assistance through the Department of Defense’s Cooperative Threat Reduction (CTR) Program, but less than ten percent of these funds have been directly appropriated for Russian CW problems. No funds have yet been allocated for security upgrades at CW storage facilities. An alternative means by which to address the Russian CW security problem would thus complement the existing CW-CTR program.

This viewpoint proposes a new partnering program between the United States and Russia to assist the Russian CW establishment with security concerns. Specifically, it suggests a Department-of-Energy (DOE)-coordinated “lab-to-lab” exchange between security experts from the US National Laboratories and Russian CW storage facilities. A precedent for such a lab-to-lab program has been launched with respect to the Russian nuclear weapons establishment and has been quite productive in dealing with security, inventory, and dismantlement problems. Establishing a comparable initiative with the Russian CW program would provide funding and assistance complementary to the CW-CTR effort.

This viewpoint will begin by describing the current status of the Russian CW stockpile and detailing the fragile security measures protecting these agents and weapons. Next, the CW agenda under the CTR project will be examined to highlight areas where DOE lab-to-lab efforts could be launched to complement existing work. Finally, based on the accomplishments of the Russian nuclear lab-to-lab model, practical and low-cost proposals will be offered for new lab-to-lab exchanges targeted at improving the security of Russian CW stockpiles.

THE RUSSIAN CW STOCKPILE: DELAYS IN DESTRUCTION

There are 40,000 metric tons of chemical weapons agents in the Russian stockpile (excluding munitions weight). These agents are located at seven sites, mainly concentrated in western Russia, along the Volga River basin (see Figure 1): Pochep (Bryansk oblast), Maradikovsky (Kirov oblast), Leonidovka (Penza oblast), Shuchye (Kurgan oblast), Kizner (Udmurtia Republic), Kambarka (Udmurtia Republic), and Gorny (Saratov oblast). Russian CW agents are distributed fairly uniformly across these stockpiles, with approximately 15 to 20 percent of the Russian total stored at each location, with the exception of Gorny, which holds only three percent (see Table 1). The composition of the stockpile consists primarily (80 percent of the total, or 32,300 metric tons) of organophosphorus nerve agents (VX, sarin, soman), with the remainder (20 percent, or 7,700 metric tons) composed of blister agents (mustard gas, lewisite, or a mustard/lewisite mixture) and phosgene. As shown in Table 1, most of the nerve agents are housed at five of the storage facilities. The bulk of lewisite and mustard gas, however, are stored in Kambarka, with lesser amounts in Kizner, Gorny, and Maradikovsky. The lewisite and mustard gas are primarily kept as bulk agents in storage tanks, whereas the nerve agents and phosgene are stored in munitions (see Table 2).

On November 5, 1997, the Russian Federation ratified the Chemical Weapons Convention (CWC). Adherence requires destruction of all CW stocks by 2007. Although Russia was one of the first countries to sign the CWC, the treaty suffered numerous delays in the ratification process and was not approved by Russia’s parliament until after the treaty’s entry into force. Even now, support for the CWC is waning and there are increased calls within the Duma for Russia’s suspension of treaty implementation.14

One of the main Russian criticisms of the CWC is the requirement for total destruction of their CW stockpiles by 2007. This stipulation is not only a technical challenge, since Russia has yet to begin large-scale CW destruction, but an economic burden as well. The current official cost estimate for complete stockpile destruction is 34.4 billion “new” rubles in revalued 1998 currency (about $5.7 billion).15 The Russian government has repeatedly stated that there is no way that its ailing economy can bear this burden alone.

Although Russia’s chemical demilitarization program has begun, it is far behind schedule. A comprehensive chemical weapons destruction act was passed by the Russian State Duma and signed by President Yeltsin in 1997, but large-scale destruction operations have not started because of insufficient government funding. Current funds can barely cover routine maintenance costs and upkeep. As Colonel General Stanislav Petrov, commander of Russia’s chemical and biological defense forces, laments:

It must be said that the finance provision is poor. To give you an example, in 1996 we got 1 percent of the allocations requested and 5.5 percent of the budget allocations, the funds
Figure 1: Russian CW Storage Sites

Table 1: Chemical Weapon Distribution at the Russian Storage Sites*

<table>
<thead>
<tr>
<th>Storage Site</th>
<th>Percent of CW Stock</th>
<th>VX</th>
<th>Sarin</th>
<th>Soman</th>
<th>Mustard Gas</th>
<th>Lewisite</th>
<th>Mustard/Lewisite</th>
<th>Phosgene</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pochep Bryansk Oblast</td>
<td>18.8</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Maradikovsky Kirov Oblast</td>
<td>17.4</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Leonidovk Penza Oblast</td>
<td>17.2</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Shuchye Kurgan Oblast</td>
<td>13.6</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>Kizner Udmurtia Republic</td>
<td>14.2</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Kambarka Udmurtia Republic</td>
<td>15.9</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Gorny Saratov Oblast</td>
<td>2.9</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
</tbody>
</table>

+ present at site; - absent from site


Table 2: Russian CW Agents By Method of Storage*

<table>
<thead>
<tr>
<th>CW Agent</th>
<th>Percent Stored In Munitions</th>
<th>Percent Stored In Bulk</th>
</tr>
</thead>
<tbody>
<tr>
<td>V agent (viscous V agent)</td>
<td>100</td>
<td>-</td>
</tr>
<tr>
<td>Sari</td>
<td>100</td>
<td>-</td>
</tr>
<tr>
<td>Soman (viscous soman)</td>
<td>100</td>
<td>-</td>
</tr>
<tr>
<td>Mustard Gas</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td>Mustard Gas/Lewisitea</td>
<td>2</td>
<td>98</td>
</tr>
<tr>
<td>Lewisitea</td>
<td>10</td>
<td>90</td>
</tr>
<tr>
<td>Phosgene</td>
<td>100</td>
<td>-</td>
</tr>
</tbody>
</table>


*a Corrected figures (1998), John Hart, personal communication with author.
provided by the budget. Five or seven percent represents the sort of funding that enables us to hold our ground in the situation as it is without any sort of breakdown. There cannot be any substantive work being done.16

The Russian government promised to earmark 500 million rubles in 1998 for chemical disarmament; by August, only 84 million rubles had been distributed.17 These severe budget constraints have already caused a two-to-three year delay in the destruction process. Upon request, the Organization for the Prohibition of Chemical Weapons (OPCW) can approve a five-year extension to the CWC deadline. However, delaying the program beyond 2007 would involve additional storage and environmental monitoring costs, potentially increasing the total sum required by as much as 25 to 50 percent.18

Furthermore, the Russian government is currently plagued not only with massive financial and organizational problems, but also with social conflicts in carrying out the destruction plan. Previous proposals to build regional destruction facilities were rejected because of fears among local citizens of risks in the transportation of such toxic agents. Because of this negative public sentiment, a law was passed to build facilities at each of the seven storage sites. In addition, many local citizens are refusing to agree to construction and operation of the destruction plan. The absence of intruder alarms at the multiple entryways makes entrance easy.

RUSSIAN CW SECURITY: THEFT AND TERRORISM ARE LIKELY

Every day the CW destruction program is delayed increases the risk to not only Russian, but also US security. This stems from the inadequate protection of Russian CW stocks. Poor physical obstacles, the absence of electronic security devices, and rudimentary inventory practices make the Russian CW storage facilities susceptible to theft. Even Russia’s own military officers have described the security measures at these facilities as “inadequate,” pointing out that the chemical arsenal is “more vulnerable to theft” since the locations of Russia’s seven storage facilities have become a matter of public record.20

In 1995, Dr. Amy Smithson published a Stimson Center report, “Improving the Security of Russia’s Chemical Weapons Stockpile,” based on interviews with visitors to the CW facilities. The report offers disturbing insights into the condition and accessibility of the Russian CW storage facilities.21 To emphasize the current danger of CW theft, a potential terrorist scenario will be outlined in the following paragraphs. The conditions described at the sample facility reflect those depicted in Dr. Smithson’s report (See Table 3).

Under the cover of night, a terrorist unit makes its move. Upon entering the storage compound, the unit encounters chain-link or barbed wire fences surrounding the perimeter of the facility (some either rusted or with holes). The terrorists pass directly through the worn fences or perhaps through one of the poorly secured side entrances. Only the main gates are consistently guarded; side entrances provide several alternative routes for entry and escape. Perimeter lights are scant and in poor condition, providing camouflage for potential theft. The absence of intruder alarms at the multiple entryways makes entrance easy.

Once inside the compound, the terrorist team moves easily to the individual CW storage buildings. There they find run-down buildings constructed of cement or wood, with either steel or wooden doors. Entry can be obtained by slipping through holes in the roofing, or by picking the single-key padlocks on the doors. No guards are present outside the storage units to deter the assailants. The absence of tamper-detection seals, electronic intruder sensors, or video cameras at the individual storage buildings allows the terrorist unit to enter undetected.

Inside the storage buildings, the terrorists find munitions and missile warheads stacked in “wine-rack” type storage units, with only production lot numbers (not serial numbers) tracking their existence. Containers for the missile warheads and bulk CW storage drums are typically unsealed. The terrorists need simply remove a few munitions or warheads and place them into a backpack before escaping into the night. It might take days for the missing CW weapons to be noticed, leaving ample time for the terrorists to threaten a civilian target. The frightening potential for CW theft by terrorists is summarized by one of Smithson’s interviewees, who warned, “You could really walk into that place without any problem.”22
### PERIMETER SECURITY

<table>
<thead>
<tr>
<th></th>
<th>United States</th>
<th>Russia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear Zones</td>
<td>• Clear zones maintained 30 feet outside of the outer fence</td>
<td>• In some cases, clear zone and patrol path evident around the perimeter; in others, outer fence adjacent to a forest or village</td>
</tr>
<tr>
<td></td>
<td>• Reinforced with steel cables to prohibit vehicle penetration of the outer fence, and, terrain permitting, speed bumps, highway barriers, or steel posts partially embedded in the ground prevent high-speed vehicle approaches</td>
<td>• Clear zones reasonably well-maintained between fences, except at one site</td>
</tr>
<tr>
<td>Fencing</td>
<td>• Two concentric perimeter fences, seven feet high, with barbed or razor wire outriggers</td>
<td>• Sites have two to four concentric rings of fencing, either chain link, barbed wire, or electrified</td>
</tr>
<tr>
<td></td>
<td>• Clear zones maintained between fences as well as inside inner fence</td>
<td>• At one site, restricted area surrounded by a wall</td>
</tr>
<tr>
<td></td>
<td>• In some cases, clear zone and patrol path evident around the fences, between the fences, and the clear zone outside the outermost fence</td>
<td>• Fences in disrepair at some sites</td>
</tr>
<tr>
<td>Lights</td>
<td>• Perimeter lights illuminate entire area inside the fences, between the fences, and the clear zone outside the outermost fence</td>
<td>• At two sites, perimeter lights observed, but the are few in number or appear to be poorly maintained</td>
</tr>
<tr>
<td></td>
<td>• Sites have two to four concentric rings of fencing, either chain link, barbed wire, or electrified</td>
<td>• No lights observed at the other sites</td>
</tr>
<tr>
<td>Gates</td>
<td>• A two-gate entrapment system for vehicles</td>
<td>• Separate gates exist for railroads, pedestrians, and road vehicles</td>
</tr>
<tr>
<td></td>
<td>• Armed guards check and/or inspect all personnel and vehicles entering or exiting main gate</td>
<td>• Only main gates appear to be guarded</td>
</tr>
<tr>
<td></td>
<td>• Crash barriers installed when appropriate</td>
<td>• Guards check identification and issue badges</td>
</tr>
<tr>
<td></td>
<td>• Personnel use a secured separate gate; other emergency gates secured with locks and a variety of sensors to detect intrusion</td>
<td>• A two-gate entrapment system is used at two sites, while another, inside a larger military compound, has a turnstile for pedestrian entry</td>
</tr>
<tr>
<td>Intrusion</td>
<td>• Two continuous intrusion detection system lines, each with different sensing methods, installed to detect entry into the perimeter area</td>
<td>• Railroad gates closed with a padlock</td>
</tr>
<tr>
<td>Detection</td>
<td>• Sensors monitored 24 hours a day from central security control facility</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>• None observed</td>
<td></td>
</tr>
<tr>
<td>Closed-</td>
<td>• Closed-circuit TV with tamper-proof barriers allows for real-time identification of intruders</td>
<td>• None observed</td>
</tr>
<tr>
<td>Circuit TV</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### STORAGE BUILDINGS

<table>
<thead>
<tr>
<th></th>
<th>United States</th>
<th>Russia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building</td>
<td>• Walls either eight-inch-thick reinforced concrete or reinforced cement blocks</td>
<td>• Some buildings constructed of cement blocks, while others made of wood</td>
</tr>
<tr>
<td>Construction</td>
<td>• Windows, ceilings, and roof provide resistance to penetration equal to the walls</td>
<td>• Cement-block buildings have wooden or steel doors; wooden buildings have wooden doors</td>
</tr>
<tr>
<td></td>
<td>• Some storage bunkers bermed</td>
<td>• Some buildings have bars on windows, some have large mesh grilles</td>
</tr>
<tr>
<td></td>
<td>• Steel-reinforced wood or steel-reinforced metal doors constructed to prevent prying or jacking</td>
<td>• At one site, holes observed in the roof; at another, buildings had just been re-roofed</td>
</tr>
<tr>
<td>Doors:</td>
<td>• King Tut blocks, or similar concrete barriers, placed in front of doors whenever feasible</td>
<td>• Storage building doors secured with single-ke padlocks</td>
</tr>
<tr>
<td>Physical</td>
<td>• Doors have two high-security padlocks</td>
<td>• Doors at one site have a bar requiring a separate key or tool to open, as well as unsecured, lift-up “dog doors” to facilitate first-entry monitoring</td>
</tr>
<tr>
<td>Barriers and</td>
<td>• No one person possesses keys to both locks</td>
<td>• Intrusion detection devices (circuit-breakers) observed on doors at one site, and possibly at another</td>
</tr>
<tr>
<td>Locks</td>
<td>• Keys secured when not in use</td>
<td>• At other sites, no confirmed observation of electronic or other intruder detection sensors on entrances or other openings to storage buildings</td>
</tr>
<tr>
<td>Intrusion</td>
<td>• Intrusion detection systems such as motion sensors with tamper detection devices on all openings in all storage buildings</td>
<td></td>
</tr>
<tr>
<td>Detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

An even more disturbing theft scenario could involve an inside operation. The risk of this type of CW theft is even greater, given the lack of inventory and accountability at the CW storage facilities. Current security practices follow the former Soviet style of personal accountability, rather than the US practice of inspection and computerized inventory. In the Russian system, individual officers are personally responsible for keeping track of hundreds of chemical weapons, typically stored throughout several buildings. Although written records are kept, no computers have been installed to log and inventory the massive quantities of munitions. It is also unclear whether inventory records are updated to reflect the periodic removal of leaking munitions. Further, although the officers are held personally responsible for CW whereabouts, it is actually enlisted soldiers who conduct the inventory. At present, there is no established method for cross-checking inventories on a routine basis. Since tamper-detection seals on the weapons are rare, this could result in one or more soldiers and/or officers removing small quantities of CW munitions over time without detection.

Inside operations are a great threat, given the pervasive criminal environment now plaguing the Russian military establishment. The collapse of the former Soviet government has resulted in a significant increase in corruption and organized crime in military society. Illegal arms sales have found a flourishing market both inside and outside of Russia. The lack of government funding for the military, and the military’s subsequent downsizing, have depleted not only resources and manpower, but also the desire to combat these crimes. Furthermore, the sporadic and meager financial support of soldiers in these hard economic times creates a tempting environment for illegal arms activity. Criminal elements, whether the mafia, corrupt government officials, or independent/foreign operators, can provide substantial compensation for underpaid military personnel and their families. According to one analyst, “Russian military and security forces are the principal source of arms becoming available to organized crime groups, participants in regional conflicts, and corrupt state officials engaged in black, gray, and legal arms markets in their various dimensions.” An underground trade in ammunition, weapons, and heavy equipment ranging from armored vehicles to MIG aircraft has been widely reported.

Although the illegal sale of conventional arms is well documented, the extent of WMD sales is unclear. Given the criminal element present in conventional arms sales, there is strong reason to suspect an emerging, lucrative market for WMD. Several cases of smuggling involving Russian fissile materials emphasize the potential for such a market. A notable example was the theft of nuclear material from the Murmansk naval storage facility. Three Russian Navy officers stole approximately 4.5 kilograms of enriched uranium. The officers planned to sell the material, but were arrested before a transaction occurred. Only a matter of timing prevented this nuclear material from entering the black market.

The naval nuclear smuggling incident highlighted the lack of security at the nuclear storage facility. There existed only minimal fences (some with extensive holes), no alarm systems, simple locks, poor seals on the nuclear materials, and a lack of trained guards—a situation not unlike that plaguing current Russian CW storage facilities. Dr. Graham Turbiville, senior analyst with the Foreign Military Studies Office, Office of the US Undersecretary of the Army for International Affairs, concludes, “The protection of Russian military chemical agents and the potential vectors for their diversion constitute a problem at least as large as the nuclear proliferation issue.”

The potential for criminal diversion of Russian chemical agents has already been documented from recent incidents. As noted, the horrific 1995 Tokyo attack led to the discovery of personnel and hardware links between the Russian CW establishment and the Aum Shinrikyo cult. A substantial number of Aum members have been found in Russia, with ties to the Russian Radiation, Chemical, and Biological Defense Troops, the Russian Academy of Sciences, and Russian Intelligence. It has been documented that the cult was able to procure various Russian weapons and design systems. Although the cult manufactured its own sarin (allegedly from a Russian military recipe), it is not unlikely that Russian CW could have been (or will be) diverted in the future. The poor quality of the sarin and delivery system used in the Tokyo attack could tempt current cult members or other terrorist groups to acquire proven and reliable Russian chemical agents and weapons.

Another case of potential CW theft also came to light in 1995. Former Chemical Troops General Anatoliy Kuntsevich was charged by the Russian Federal Security Service with delivering 800 kilograms of CW precursors to Syrian buyers in 1993 and attempting to
smuggle an additional 5.5 tons in 1994. Although these charges were eventually dropped, Kuntsevich was also judged negligent for the poor conditions at the Shikhany CW production facility, which he once commanded (an accusation that could be true of many CW officers). Finally, the aforementioned Turkish sting operation leading to the arrest of Emin Ekinici indicates the potential involvement of Russian security and military personnel and the vulnerability of CW stocks to insider theft.

Although Dr. Smithson’s report states that the soldiers interviewed at the CW facilities did not appear to be discontented, these soldiers probably suffer from erratic and paltry pay, as has been reported for soldiers at nuclear weapons facilities. Massive Russian CW stockpiles, lack of inventory practices, poor security measures at storage facilities, depressed economic conditions, and widespread military and government corruption create a climate ripe for CW theft from within. One of Dr. Smithson’s sources offers a sobering prediction: “Sooner or later, someone will make the soldiers at these sites a better offer than Moscow does. If something was missing, it is likely to be an inside job.”

Once chemical weapons are in the hands of a terrorist group, carrying out a CW attack on an unsuspecting civilian population could prove to be simple. There are a variety of chemical munitions that are relatively small in size, making them easy to conceal and transport. Protective clothing and gas masks are commercially available. Compared to nuclear weapons, chemical weapons would be much more straightforward to employ. Chemical weapons are not protected by the Permissive Action Links (PALS) that are often placed on individual nuclear weapons. Stolen chemical munitions could be delivered using many existing conventional systems, or in homemade reconfigured designs. Although such use would require some effort and coordination, the Aum example suggests that it would be possible for an organization with sufficient resources and technological infrastructure. Terrorist groups such as Aum need only show their capability and willingness to acquire and use WMD to threaten US national security, since “backpack-sized chemical or biological weapons, too small, improvised, and fragile to have an impact on a battlefield or against soldiers equipped for chemical and biological defense, could nonetheless be devastating against some civilian targets.”

When asked to assess the relative threats of Russian nuclear weapons theft versus chemical weapons theft, some experts viewed them as “very much the same.” Others disagreed, arguing that Russia’s chemical arsenal presents a far more exposed and appealing target for potential thieves or attackers. The threat of terrorism is not limited to within Russia’s borders. Once a chemical weapon is in the hands of a terrorist group, there is a very real possibility that it could be used against the United States.

LIMITATIONS OF THE CTR CHEMICAL WEAPONS PROGRAM

In light of these emerging proliferation risks, Congress responded by initiating financial assistance through the passage of the Soviet Nuclear Threat Reduction Act (Public Law 102-228), more commonly known as the Cooperative Threat Reduction Program. In November of 1991, under the CTR, Congress approved $400 million of Department of Defense (DOD) funds in fiscal years (FY) 1992-1993 to help Belarus, Kazakhstan, Russia, and Ukraine: (1) destroy their weapons of mass destruction, (2) safely store and transport the weapons in connection with their destruction, and (3) reduce the risk of weapons proliferation. This assistance consists of goods and services such as materials, equipment, and training, rather than direct cash payments. Through FY 1998, Congress approved $1.1 billion in assistance to address these concerns, leaving prioritization of these objectives to DOD’s discretion.

With regard to CW allocations, the main thrust of the CTR program has been to “jump start” Russia’s chemical weapons destruction efforts. This commitment involves providing Russia with technological assistance to get its destruction plan off the drawing board and to facilitate its implementation. In no way is the CTR program committed to financing the entire Russian CW dismantlement program. So far, Congress has increased total support to $136.5 million for FY 1998, with an additional $88.4 million recently approved in the FY99 budget. However, all monies approved so far are earmarked for activities directly related to destruction, such as the pilot destruction facility at Shuchye. This CW storage site holds only 14 percent of the Russian CW stockpile. The CW-CTR program has yet to address the need, either technologically or financially, for destruction facilities at the six other CW agent storage sites in Russia. Moreover, funds have yet to be allocated to address the dire security problems at the CW storage facilities.

The effectiveness and future of CTR support in the
Russian CW program have been topics of heated debate. An unexpected loss of support was experienced in FY 1996. Of the $73 million in the FY96 budget, $60 million was reallocated to strategic delivery vehicle dismantlement work in Ukraine, Belarus, and Kazakhstan. This loss of funding occurred because the president could not certify to Congress that Russia was complying with the Biological Weapons Convention (BWC). US assistance has been disbursed only when Russia has shown that it is “committed to complying with all relevant arms control agreements” and “observing internationally recognized human rights, including the protection of minorities.” This stipulation has cost Russia precious CW-CTR funding, given doubts about Russian compliance with the BWC, delayed ratification of the CWC, and difficulties with the Treaty on Conventional Forces in Europe.

Other problems plaguing CTR funding to Russian nuclear and CW efforts can be traced back to certain provisions in the CTR legislation. Since contracting must go through DOD, all goods and services are subject to Federal Acquisition Regulations, imposing various constraints and creating a potentially tedious, bureaucratic process. This can result in an inefficient procedure to take care of CW security concerns. As Graham Allison et al. have noted, “The Department of Defense acquisition process may be appropriate for procuring weapons that take years or decades to develop and manufacture, but it hardly allows for quick and agile reactions necessary to respond to an immediate policy challenge.”

Furthermore, the acquisition guidelines impose strict auditing procedures. This is problematic since such operations must occur at top-secret military facilities in Russia. These were previously closed to outsiders, and a wariness of inspectors remains. As one DOD official explains, “The Russian concept for an audit was that of an arms control inspection. Russia was concerned about extending unimpeded access to sensitive Russian facilities without arms control inspection type procedures agreed to in advance.” This distrust of foreign WMD accounting has even resulted in restricted access to CW storage facilities. In light of Russia’s ratification of the CWC, it is hoped the convention’s mandates for inspection and accounting will minimize such access restrictions. However, many details and diplomatic issues remain to be resolved for a workable US/Russian auditing protocol.

New CW-CTR budget battles emerged in the FY 1999 House bill. Of the administration’s $88.4 million CW funding request, the House National Security Committee recommended a reallocation of $53.4 million to the Strategic Arms Elimination Project. This recommendation stemmed from doubts as to whether Russia was able to meet its own financial obligations in construction of the Shuchye CW destruction facility. In the end, the entire $88.4 million request was approved in the final FY99 budget, albeit with a number of conditions. However, such battles in Congress reveal the legislature’s tenuous political support for additional CW-CTR funding, particularly in areas that are not directly related to destruction efforts.

Such unstable CW-CTR funding can be linked to a failure by Congress to appreciate the role of such assistance in serving US interests. Many legislators continue to view aspects of the program as foreign aid, instead of as an investment in US security. Since many legislators (and their constituents) are averse to committing additional US funds to foreign assistance programs, the CW-CTR funding is vulnerable to cuts. This view is quite inappropriate given that the primary financial beneficiaries are US contractors. This point, however, remains to be emphasized on the legislative floor.

Finally, the CW-CTR program has experienced difficulties in the working relationships between the Russian Ministry of Defense (MOD) and US Department of Defense. The MOD and DOD are both responsible for the development and operation of their respective destruction facilities, along with maintaining the safe storage of their respective weapons as they await destruction. This, along with CTR, has made DOD the primary agent in dealing with the Russian CW establishment. Since both Russia and the United States have eliminated CW as a component of national defense, it was originally believed that there would be more favorable interactions between the CW branches of MOD and DOD (in contrast to their nuclear branches), facilitating cooperation and agreement on CW-CTR activity. However, this has not necessarily proven to be the case.

According to Russian CW expert Igor Khripunov, “in order to understand some of the ineffectiveness of CW funding under CTR, one must understand the personalities of Russian individuals controlling the CW program.” Professor Khripunov relates that some military officers who lead the MOD’s CW program are members of the “old guard” and are highly suspicious of US...
intentions. Many are hesitant to provide full transparency into the once-secret CW program, and they resent US auditing requirements on the CTR funds spent on the Russian CW establishment. Chemical weapons General Stanislav Petrov’s attitude towards CTR funding can be observed in his following remarks:

The Americans attached all sort of strings to this aid, which essentially boils down to extracting the maximum information about Russia’s military-chemical potential in exchange for American money. It is very difficult to work with them. Much easier to work with the Germans, for instance. They do not attach any conditions. They make money available and only ask us to provide precise reports on where the money is going...this is all real, with no strings attached—political or otherwise.48

In addition, many Russian military officials are embarrassed to reveal the desperate condition of their CW installations to US military personnel. The Russian CW establishment suffers from a position of diminished power and prestige (with both US and Russian officials), which has outwardly manifested itself through an attitude of resentment and hostility towards DOD officials. Such an atmosphere of distrust and insecurity has created an additional source of frustration in implementing objectives of the CTR program, and it is likely to continue.

The CW-CTR program has been crucial in moving the Russian CW stockpile towards destruction. Continued availability of CTR funds for destruction is necessary to ultimately eliminate the threat of CW diversion. However, many non-destruction-related projects under the CW-CTR program have suffered from competition for funds. More attention and support are needed to address areas, such as CW security concerns, to which the CTR program has not attached priority consideration.

A NEW PARTNERSHIP: A PROPOSED LAB-TO-LAB PROGRAM

As stated above, although CW-CTR funding has provided important monies for the destruction effort, the program still has problems and limitations. A relatively small, scientist-led effort at the Department of Energy, however, has been able to successfully address similar difficulties that once troubled CTR assistance to the Russian nuclear establishment. In 1992, the directors of the Los Alamos National Laboratory (LANL) and Lawrence Livermore National Laboratory (LLNL) initiated discussions with the directors of the Arzamas-16 and Chelyabinsk-70 nuclear facilities in Russia.49 This meeting spawned an arrangement whereby US and Russian scientists from the weapons labs would collaborate on a variety of scientific research endeavors. These collaborative projects provided assistance for the financially strapped Russian nuclear weapons laboratories. Although DOE was informed about the various lab-to-lab projects, it was not the main player. As the name suggests, the program was established so that technical contacts were made directly by the scientists, and it involved only the US and Russian laboratories and institutes.

Two years later, in the spring of 1994, Undersecretary of Energy Charles Curtis directed US government labs to extend their collaborations with Russia to include projects involving accounting of and safeguards on nuclear materials.50 In light of the emerging risks of nuclear theft and terrorism, a new lab-to-lab initiative was launched. It was hoped that the collaboration would reduce these risks through practical, concrete solutions, while providing employment opportunities to prevent potential “brain-drain” of Russian weapons specialists to terrorist groups or proliferant states. This directive proved to be the start of a very fruitful and efficient exchange. Within six weeks of Curtis’s request, contracts had been signed for a joint project to develop an indigenous Russian system of fissile material protection, control, and accounting (MPC&A) and to improve physical security at two Russian nuclear facilities.51 This fast turnaround provides a contrast to some of the difficulties experienced in the MPC&A effort under the CTR program. Two million dollars in financial assistance were initially supplied to the DOE lab-to-lab program in FY 1994, increasing to $31 million in FY 1996 and $137 million in FY 1998, for security enhancements at Russian nuclear facilities.52

Under the lab-to-lab program, a collaboration between Sandia National Laboratory and the Kurchatov Institute focused on upgrading the security system at the Kurchatov facility.53 Additions and improvements launched under this project included systematic inventories of fissile materials and the installation of new fences, sensors, and alarms. The initiative at Arzamas-16 mainly involved developing a model MPC&A system, to be shared with other nuclear weapons
establishments in Russia. Both of these collaborations have been praised by Russian scientists and the Russian Ministry of Atomic Energy, garnering much interest and cooperation within the nuclear establishment.

Part of the favorable response from the Russian side has resulted from the greater involvement of Russian goods and services. Since the funds for the lab-to-lab effort come from the DOE, they are not subject to the acquisition regulations of the DOD or the CTR stipulations to use American contractors whenever possible. Because of these exemptions, most of the equipment and services used in the projects have been Russian-made, increasing the incentives for Russian cooperation. In addition, since the US security experts under the lab-to-lab program are civilian personnel, the Russians have been more receptive to collaborations involving sensitive nuclear facilities.

Currently, the lab-to-lab program is focused on improving security and accounting procedures at nuclear weapons facilities, with surprisingly little attention to the CW establishment. In light of the lab-to-lab successes on nuclear MPC&A, similar initiatives should be launched with the Russian chemical weapons establishment to complement the CW-CTR program. Since the majority of nuclear MPC&A upgrades are readily transferable to the protection of chemical weapons, and physical security is mostly independent of the type of weapons stored at the site, there should be little technical difficulty extending the lab-to-lab effort into the Russian CW establishment. Such a partnership could alleviate some of the competition within the CW-CTR program for limited funds and some of the problems arising from difficulties in US-Russian military interactions, as well as tap into the expertise and resources of the firmly established DOE lab-to-lab program.

As stated previously, the chemical weapons storage facilities in Russia are severely underprotected and poorly inventoried. Physical security measures at the CW facilities are limited and vary from site to site. Moreover, there is no good MPC&A program for tracking and securing weapons and agents. The potential risks for theft and/or terrorism remain high at Russian CW storage installations. A comparison of physical security at US and Russian chemical weapons facilities is presented in Table 3. In contrast to current Russian conditions, US storage facilities are characterized by layers of physical and electronic security, both inside and outside the complex. Amy Smithson summarizes the stark contrast: “By US standards, Russian chemical weapon storage facilities unquestionably appear to be vulnerable to attack from outside and theft from within.”

Just as US national labs have successfully implemented new security measures at Russian nuclear facilities, they could collaborate with CW storage facilities to develop security plans that would be unique and effective for the particular agents at each facility, whether these agents are housed in bulk storage tanks or in munitions. On the lab side, Sandia has taken the lead in addressing physical security upgrades, while material control and accounting projects have involved Los Alamos and Lawrence Livermore.

With respect to Russian CW sites, priority should be given to the nerve agent storage facilities at Pochep, Maradikovsky, Leonidovka, and Kizner. No destruction plans have been crafted for these sites in spite of the fact that dangerous air- and artillery-delivered nerve agent munitions are housed at these facilities. Such munitions pose the greatest threat to US national security, because they are already in a form in which they could be employed effectively if stolen. Initial work would involve establishing an assessment of facility needs and deficiencies, followed by a specific workplan tailored to each CW storage facility, and then a timetable for completion of upgrades.

At first, collaborations need to pursue improvements in physical protection, which need not be expensive or complicated. Access to the compounds should be restricted: multiple gates and entryways must be closed, equipped with high-security locks and sensors, and patrolled regularly by military personnel. Infrared and microwave sensors can be added onto existing intact fences. Clear zones, new light fixtures, and video surveillance equipment should be installed around all the compounds and storage buildings to monitor personnel and intruder access. Large-vehicle barriers, speed bumps, and posts should be erected outside of the storage compounds to protect against terrorist attacks. At compound entrances, portal monitoring systems consisting of metal detectors should be constructed to deter theft of small CW munitions.

Enhanced physical security of individual storage facilities should start with repair of dilapidated roofs and building structures. Current entrances should be replaced by steel-reinforced doors with high-security
padlocks. All doors, windows, and other openings in the buildings should have tamper-proof seals and intruder sensors, linked to a central security control center. Closed-circuit video cameras should also be installed both outside and inside the storage facilities to monitor movement and weapons security. Sensing tags and seals should be installed on all munitions and bulk-agent storage containers to secure contents.

Although more high-tech physical security measures are available, these would not be the most desirable for the Russian stockpile, for reasons of expense and long-term sustainability. Even without advanced technology, upgrades involving full-scale physical protection with several layers of defense can provide excellent security. Redundant and diverse layers of protection increase the difficulty of penetration and guarantee that security is not dependent on any single defensive layer. Adding high-tech equipment is not likely to significantly enhance security and may, in the long term, actually increase security risks. These risks tie in with the problem of sustainability. High-tech security measures are far more difficult and expensive to maintain. The Russians need security items that they can reliably control and replace with Russian parts throughout the extended lifetime of the CW destruction process. In these tough economic times, Russia needs security measures that do not depend on advanced technical know-how or a large budget to sustain. For these reasons, it is important to use indigenous equipment and resources as much as possible.

Once the physical security upgrades have been completed, other collaborative projects could involve the development of a more stringent MPC&A protocol for the chemical munitions and bulk agents while they await destruction. In order to prevent diversion of weapons, it is critical to install good accounting practices before the multi-year destruction effort begins. As with its nuclear inventory, the FSU never developed a rigorous materials control system for its chemical weapons; rather, a personalized control system was used. While this system worked well under the strict, totalitarian control of the Soviet state, it is unreliable under the current decentralized government and pervasive military corruption. As former US Deputy Secretary of Energy Charles Curtis commented, “After the breakup of the Soviet Union, they [weapons establishments] lost both the restrictions on movement and the surveillance system of the Communist Party, an estimated (by some) 50 to 60 percent loss in their security system.”

What is urgently needed is a detailed accounting system like that present in US chemical weapons facilities. This system is characterized by a computerized command center that tracks inventory practices at the individual storage facilities. Munitions are assigned serial and production-lot numbers. Physical inventories of the munitions and bulk agents are taken by soldiers at each CW storage building and then crosschecked by officers. The information is entered into a computerized database that is monitored by the central command post. The command post then periodically (and randomly) dispatches inspection teams to check records at all CW storage facilities. In this way, a detailed log of all weapons is maintained, minimizing the risk of internal theft.

In addition, a strict measure of access control should be implemented. This would include restricting personnel access to the actual CW material in storage buildings by requiring identification cards with personal identification numbers (PINs) to enter the storage buildings. Also, upgraded communications systems for security personnel would keep all units informed and speed up mobilization of guards in case of unauthorized entry. It would also be desirable to train an on-site rapid-response team at CW storage facilities to deal with a terrorist attack.

Finally, it is important to provide guard training as a crucial component of security assistance. A “safeguards culture” must be established and adopted by Russian security personnel to provide a continuous environment of protection. Training and refresher courses on MPC&A, as well as periodic safety and terrorism drills, would instill and reinforce a safeguards mentality among the guards. CW security personnel could take part in the ongoing DOE-sponsored MPC&A training sessions held at the Russian Methodological Training Center and the Engineering Physics Institute, both located in Moscow, and the Kuzmycz Training Center in the Ukraine. Under 1998-1999 DOE funding, two additional training centers are scheduled to be developed: a Urals/Siberian Training Center and a graduate-level training program at Tomsk Polytechnic University.

The cost of such security and accounting upgrades would be negligible compared with the costs of CW terrorism. Similar security and inventory arrangements were installed at the Kurchatov Institute for about $1 million. This cost was shared among the Institute, the
Russian Ministry of Atomic Energy, and Sandia National Laboratory. And all of the upgrades were completed in a matter of five months! A lab-to-lab program is a quick and cost-effective means by which the DOE can lend a helping hand to reduce Russian CW security dangers and complement the larger DOD CTR effort.

CONCLUSIONS

The Russian CW destruction effort is far from completion, and unstable political conditions throughout the globe, coupled with a troubled Russian military, make the Russian CW stockpile an attractive target for theft. Although some estimates project total elimination of Russia’s CW in the next 10 years, newer estimates suggest a more realistic completion time is 15 to 30 years. The destruction effort continues to suffer numerous delays related to mounting financial, social, and organizational problems. These delays create a real risk of CW theft and terrorism in the days and years to come.

The United States is not immune to acts of terrorism. The longer Washington fails to address the Russian CW security problem, the more the United States places itself at risk. Although the United States has provided needed assistance in the form of CTR funds, the program has not addressed security concerns at Russian CW facilities. A CW lab-to-lab initiative would be a new approach to this long-standing problem.

The idea of launching such a new initiative, however, is not beyond criticism. The CTR program under the DOD has served as the lead government program to assist the Russian CW community. Historically, the DOE has not formed relationships with the MOD on CW issues, and this may prove to be a challenge. However, as stated earlier, there may also be less hostility and more opportunity for confidence-building between MOD and DOE officials. But there is always the nagging possibility of “turf wars” among US government agencies, which would complicate a DOE/DOD partnership. Since the CTR program has always managed US assistance in Russian CW issues, there may be reluctance to see involvement of DOE workers in a perceived DOD program. However, the Russian CW security situation is a national security problem, necessitating full cooperation among and assistance from various US governmental agencies. The problems plaguing the Russian CW program are larger than the stated scope of the CTR program—from the beginning the CTR’s only commitment has been to “jump start” the Russian CW destruction effort. The need to reduce security problems at the CW sites may thus be better served through a DOE lab-to-lab effort.

The DOE lab-to-lab program, first initiated with the Russian nuclear weapons storage facilities, offers a unique opportunity for a new partnership with the DOD community on the Russian CW situation. The CW-CTR program has made significant strides in dealing with destruction of the Russian stockpile, and should continue as the lead agent in that role. Room exists, however, for further involvement by US agencies, such as the DOE, to complement and expand US assistance to the troubled Russian CW destruction effort. Political support for such assistance, however, is on shaky ground. Members of the DOD, DOE, Congress, and the Office of the President need to see a new CW partnership program as an integral component of US national security policy. A new lab-to-lab effort could also serve to catalyze other US government agencies, such as the Environmental Protection Agency and the US Agency for International Development, to provide assistance to the Russian CW establishment and local communities in areas such as environmental and social infrastructure that fall outside the scope of CW-CTR assistance. Providing targeted assistance to Russia through a combination of US partnering programs would be an effective and timely way to protect US national security interests against the risks of CW terrorism.

---

1 The author wishes to thank Frank von Hippel, Ken Luongo, Jonathan Tucker, Eric Croddy, John Hart, and Gavin Cameron for providing valuable comments on this viewpoint.
3 Ibid., pp. 71-72.
4 Ibid.
5 Ibid., pp. 73-74.
6 Ibid., p. 57.
7 Ibid., p. 49.
27, 1996).


3 Ibid., pp. 4-21.

3 Ibid., p. 12.

3 Ibid., pp. 16-12.


3 Ibid., p. 9.


3 US Senate, Permanent Subcommittee on Investigations, Staff Statement, pp. 69-79.


3 Ersenmiz, “Twenty Containers Seized.”

3 Smithson, “Improving the Security,” p. 16.

3 Ibid., p. 17.


3 Ibid.


3 U.S.C. Title 22 Sec. 5902(d), <http://www.law.cornell.edu/uscode/22/5902.html>.


3 Igor Khrispunov, telephone interview with the author, October 26, 1998.


3 Monterey Institute, Nuclear Successor States of the Soviet Union, p. 79.

3 Allison et. al., Avoiding Nuclear Anarchy, pp. 84-85.


3 Allison et. al., Avoiding Nuclear Anarchy, p. 84.


Kathleen Vogel