## Inside this Issue

### Recent Developments in the NIS
- CIS Council of Border Guard Service Heads Meets in Turkmenistan
- CSTO Conducts Frontier-2005 Border Defense Exercises in Kyrgyzstan and Tajikistan
- Ukrainian Government Implements State Anti-Contraband Program
- Ukraine Opens Hotline to Combat Customs Corruption, Bribery
- Kyrgyz Customs Service Reorganized

### Changes in NIS Export Control Personnel
- Heads of Kyrgyz Borger Guard and Emergency Agencies Replaced; Border Guards Subordinated to National Security Service

### International Supplier Regimes
- Australia Group’s Plenary Meeting Marks the Organization’s 20th Anniversary; Dual-Use Biological Equipment Control List Expanded

### International Assistance Programs
- Latvia and United States Sign Nonproliferation Cooperation Agreement; Fresh Fuel Transferred to Russia
- United States to Install Radiation Detection Equipment on Ukrainian Borders; Ukraine-NATO Commission Adopts 2005 Target Plan

### International Assistance Programs (continued)
- U.S. Military Delegation Visits Tajikistan; U.S. Embassy Issues Fact Sheet on U.S. Border Security and Counternarcotics Assistance to Tajikistan
- United States and Russia Sign Agreement under Second Line of Defense Program
- DOE Organizes Export Control Seminars in Russia and Georgia

### Illicit Trafficking in the NIS
- IAEA Releases Illicit Trafficking Data for 1993-2004
- Kamchatka Customs Seizes Submarines Destined for China

### International Developments
- Chinese Port of Shanghai Joins U.S. Container Security Initiative; Argentina and Brazil to Follow Suit
- German Media Report Illegal Technology Transfers to Iran
- GAO Criticizes U.S. Export Control System
- UN Readies New Treaty to Curb Nuclear Terrorism
- Potential Restrictions on Chinese Re-Exporting Russian Engines to Pakistan

### Special Report

**The Globalization of Nuclear Smuggling: Methods Used by Two Pakistan-Based Networks**

by Stephanie Lieggi and Kenley Butler, Center for Nonproliferation Studies
Recent Developments in the NIS

CIS Council of Border Guard Service Heads Meets in Turkmenistan

In a March 18, 2005, interview with Nezavisimoye voyennoye obozreniye (Independent Military Review), the analytical supplement to the popular Russian newspaper Nezavisimaya gazeta, Colonel General Vitaliy Gritsian, the head of the coordinating office of the CIS Council of Border Guard Service Heads, discussed the agenda of the 53rd session of the council, which was held March 30-31, 2005, in Ashgabat, Turkmenistan.[1,2,3] The council meets every three months, and this was the fourth session held in Turkmenistan (prior council sessions in Turkmenistan included the 8th in 1994, 15th in 1995, and 24th in 1997). According to Gritsian, because of the fact that the Turkmen State Border Service was undergoing reforms in 2001-2003, the Turkmen representatives did not participate in the council’s proceedings in that period.[1]

The main topic of discussion at the council session in Ashgabat was the conduct of multilateral large-scale border defense operations. In particular, the participants reviewed plans to hold collective exercises on the Caspian Sea that will involve the naval border guard forces of the four Caspian Sea littoral states (Azerbaijan, Kazakhstan, Russia, and Turkmenistan) with Iran as an observer. While the exact dates are still not set, it is envisioned that Kazakhstan will be responsible for organizing these maneuvers. The main purpose of the exercises is to improve coordination of anti-poaching activities on the Caspian Sea. A similar operation led by Russia’s Federal Security Service (FSB) is planned for the Sea of Azov with Ukrainian participation. Finally, the purpose of the third planned operation is to improve coordination of participating parties in halting the import of drugs from Afghanistan. Kyrgyzstan will be responsible for making necessary preparations for this operation, which will include the other four Central Asian states.[1,2]

Another item on the agenda of the council was general discussion of the threats and challenges to the national security and territorial integrity of Central Asian states. There is growing concern that the impending departure of Russian border guards from the Tajik-Afghan border by the end of 2005 will cause a surge in drug trafficking from Afghanistan.[1] In the course of the 53rd session, council members also discussed the problems of illegal immigration as well as the draft of a joint action plan for 2006 and a program for cooperation in fighting terrorism and extremism for 2005-2007.[1,3]

On the sidelines of the council meeting, the heads of the Kazakh and Turkmen delegations—Lieutenant General Bolat Zakiyev, deputy chairman of the Committee for National Security of Kazakhstan and the commander of the Kazakh Border Guard Service, and Lieutenant General Orazberdy Soltanov, chairman of the State Border Guard Service of Turkmenistan—met to discuss cross-border cooperation between border guards of the two countries, including issues related to patrolling the maritime border on the Caspian Sea.[4]

Editor’s Note: The coordinating office of the CIS Council of Border Guard Service Heads prepares monthly bulletins for CIS border guard commanders. The monthly bulletins summarize the status of external borders of the CIS based on information provided by the border guard departments of each CIS country, with the exception of Turkmenistan and Uzbekistan. It is also expected that Azerbaijan, Moldova, and Ukraine will soon opt out of the information exchange as well. The council’s coordinating office has been functioning for 12 years; during this period of time it has been reformed six times, while its staff has been reduced from 120 to 47 employees, including the latest staff reduction in September 2004. Further cuts of approximately 10 percent are expected in the near future.[1]

CSTO Conducts Frontier-2005 Border Defense Exercises in Kyrgyzstan and Tajikistan

In accordance with a decision by the Council of Defense Ministers of the Collective Security Treaty Organization (CSTO) on November 25, 2004, Tajikistan and Kyrgyzstan hosted joint military exercises code-named Frontier-2005 on March 29-April 6, 2005.[1] [Editor’s Note: CSTO was founded in May 2002. CSTO members are Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia and Tajikistan. For more information, see Konul Gabulzade and Kenley Butler, “Inter-State Cooperation in the NIS,” NIS Export Control Observer, No. 9, September 2003, pp. 18-22, <http://cns.miis.edu/nis_excon>.] The press service of the CSTO Secretariat reported that the Frontier-2005 maneuvers comprised two stages. The first stage entailed command-and-control training led by the Kyrgyz minister of defense on the territory of Kyrgyzstan, whereas the second stage was held in Tajikistan, where troops used live munitions and overall guidance was provided by the Tajik minister of defense.[1]

Approximately 3,000 soldiers, including CSTO’s Collective Rapid Reaction Force in the Central Asian region, and more than 100 units of armored vehicles, as well as fighter jets and assault helicopters from Russia, Kazakhstan, Kyrgyzstan, and Tajikistan, participated in the Frontier-2005 military maneuvers.[1,2] The combat part of the exercises, which was held at the Eshokh-Maydon target range located 200 kilometers (km) south of Dushanbe (the capital of Tajikistan), consisted of a simulated cross-border incursion from Afghanistan into Tajikistan by a fictitious band of militants and its subsequent containment and annihilation by the CSTO forces.[2] The location of the exercises was chosen deliberately in close proximity to the Tajik-Afghan border, where incursions by drug smugglers are reported frequently and the situation remains tense. The main objective of the Frontier-2005 exercises was to improve interaction between the border guards of the CSTO member states to counteract the terrorist threat.[1,2]

Representatives from the Kyrgyz Ministry of Defense, CSTO’s Unified Headquarters and Secretariat, CIS Council of Border Guards Services Heads, CIS Anti-Terrorism Center (ATC), and the Shanghai Cooperation Organization’s (SCO) Regional Antiterrorist Structure (RATS) attended Frontier-2005 exercises.[1,2] Foreign guests included military observers from France and the United States.[2] After the exercises concluded, Russian Defense Minister Sergey Ivanov and CSTO Secretary General Nikolay Bordyuzha praised the performance of CSTO forces in the maneuvers.[2]

In the course of his visit to Tajikistan, Ivanov held meetings with Tajik President Emomali Rakhmonov and Defense Minister Sherali Khayrulloyev, which resulted in the transfer of the electronic optical orbital surveillance station Nurek to the Russian side.[2] The signing of the transfer agreement was a mere formal confirmation of the agreement that was reached during Russian President Putin’s visit to Tajikistan in October 2004.[3,4] [Editor’s Note: The construction of the Nurek station began in 1985. The Nurek station monitors military space satellites, which are used for navigation purposes, communications, and tracking of ballistic missile launches. The Nurek station is capable of monitoring space objects located at an altitude of up to 40,000 km. Until the transfer agreement was signed, the status of this high-tech facility was a subject of bilateral negotiations between Tajikistan and Russia for several years.][2,3]

In a related development, on April 5, 2005, the CIS Unified Air Defense System (CIS UADS), which formally incorporates 10 CIS states (Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan), held collective air defense exercises. Turkmenistan and Georgia did not participate in the exercises, while Ukraine and Uzbekistan participated in the maneuvers on a bilateral basis with Russia. Thus, only six countries, which are also CSTO members, were engaged in the maneuvers. In the course of the exercises, approximately 56 military aircraft and one helicopter made more than 60 sorties over the territories of CSTO member states.[5,6] The purpose of the CIS UADS exercise was to improve cooperation between the CIS member states in preventing airspace violations. Russia contributed two A-50 Airborne Early Warning (AEW) planes and eight long-range (strategic) aircraft Tu-22M3, Tu-95MC, and Tu-160 to this exercise.[6]

Ukrainian Government Implements State Anti-Contraband Program

On April 1, 2005, the Ukrainian Cabinet of Ministers adopted Decree No. 260 On Approval of the State Program “Stop Contraband” for 2005-2006, which entered into force the same day.[1,2] The state “Stop Contraband” program outlines the following measures aimed at eradicating illicit trade in contraband commodities in Ukraine:

- improving the procedures for registering commodities by customs;
- finishing the demarcation of Ukraine’s borders with Belarus, Moldova, and Russia;
- improving the operations of border crossings and optimizing their number;
- creating an automated registration system for people and vehicles crossing the borders;
- creating an integrated computer registration system for vehicles entering Ukraine that will be linked with the system used by traffic police;
- improving information exchange between government agencies that monitor and oversee the international economic activities of Ukrainian business entities;
- creating mobile interagency groups to fight illicit trade in contraband commodities (these groups will perform random inspections of customs documents, customs offices, and warehouses);
- creating expert analytical groups to monitor foreign economic activities of Ukrainian business entities and commercial flows of goods (these groups will function within the structure of special law enforcement divisions, specializing in anti-corruption and anti-organized crime activities);
- performing quarterly analyses of the customs statistics of Ukraine and neighboring countries (Ukraine will sign relevant intergovernmental agreements, when required, to allow for the exchange of information);
- performing periodic qualification exams of management personnel of the Ukrainian customs service, as well as relevant divisions of the Security Service of Ukraine (SBU) and the State Border Guard Service that are responsible for combating illicit trade in contraband commodities;
- installing surveillance systems, electronic scales and vehicle number plate readers at border checkpoints;
- introducing electronic seals for controlling transit shipments; and
- creating an information exchange system between the State Customs Service of Ukraine (SCSU) and the Ministry of Transportation and Communication that will track the movement of containers and railway cars.[2,3]

In accordance with Decree No. 260, all relevant ministries are responsible for submitting to the Cabinet of Ministers quarterly reports about their progress in implementing the aforementioned list of anti-contraband measures.[1]

The Ukrainian Cabinet of Ministers has allocated 384,115 million hryvni ($75 million) for the implementation of the program for a two-year period (2005-2006).[4] Most of these funds will be used to equip border control and customs facilities: 240.5 million hryvni ($47 million) will be spent on technical upgrades alone, including the introduction of electronic customs declarations, improvement of transit shipment monitoring, installation of closed-circuit television cameras at border control and customs facilities, and installation of vehicle number plate readers and X-ray equipment. This year the Ukrainian government intends to spend 13.5 million hryvni ($2.5 million) to acquire border control equipment.[4]

In addition, on April 25, 2005, an analytical center was opened under the aegis of the Interagency Coordinating Council on the Fight against Contraband.[5,6] The analytical center operates on the premises of the Main Directorate of the Fight against Corruption and Organized Crime of the SBU. According to the SBU press center, the newly created analytical center will be responsible for aggregating information on contraband and individuals and organizations involved in illicit trade in contraband commodities. The center will also analyze the efficiency of anti-contraband measures and develop proposals for strengthening
control over illegal actions in the sphere of international economic activities of Ukrainian business entities.
The center is staffed by SBU operatives, SCSU specialists, and representatives from the State Taxation
Administration, State Border Guard Service, Ministries of Internal Affairs, Transportation and
Communication, Economy, Finances, Industrial Policy, and Justice. At the regional level, the center will be
represented by regional expert analytical groups.[5,6]

On May 19, 2005, during a meeting of the Interagency Coordinating Council for the Fight against
Contraband, Deputy Prime Minister Anatoliy Kinakh indicated that since the beginning of its
implementation in April 2005, the “Stop Contraband” program had already brought 1,730 million hryvnias
($342,574) into the state budget from the shadow economy. Mr. Kinakh noted that customs payments from
the Odessa, Lviv, and Donetsk customs offices increased by 90, 78, and 70 percent, respectively, above last
year’s figures.[7] According to Prime Minister Yulia Tymoshenko, since the beginning of this year, the
Ukrainian government took $1.6 billion from the shadow economy and returned it to state coffers. This
figure included the revenues received as a result of the implementation of the “Stop Contraband” program
by Ukrainian customs.[9]

Sources: [1] “Kabmin utverdil programmу ‘Kontrabande – STOP’” [Cabinet of Ministers adopted the ‘Stop Contraband’ program],
god’ (N 260 ot 01.04.2005 g.)” [Decree of the Cabinet of Ministers of Ukraine ‘On Approval of the State Program ‘Stop Contraband’
for 2005-2006 (No. 260 of April 1, 2005)], Dinay consulting company website (Kiev, Ukraine),
Agency – UNIAN, April 8, 2005, in “Ukraine Launches Program to Improve Border Posts, Fight Contraband,” FBIS Document
analiticheskiy tsentr” [The analytical center is created under the aegis of the Interagency Coordinating Council on Issues Concerning
Fight Against Contraband], Ukrainian Network of Business Information LigaBusinessInform, April 26, 2005,
kontrabandoy prinesla Ukrainye 1.7 mldr griven” [Fight against contraband brought Ukraine 1.7 billion hryvnias], Korrespondent.net
[Yulia Tymoshenko talked about the mistakes of the government], LigaBusinessInform, May 16, 2005,
– premier-ministre” [In 100 days the government of Ukraine took $1.6 billion out of the shadow economy – prime minister], Prime-

Ukraine Opens Hotline to Combat Customs Corruption, Bribery

On April 12, 2005, the Ukrainian Cabinet of Ministers opened a hotline phone number with the purpose of
stopping the practice of bribery in the customs service, according to the press service of the Kiev regional
customs office. The hotline operates from 9 am to 8 pm on weekdays and is staffed by officers from the
State Customs Service of Ukraine (SCSU), Security Service of Ukraine, and State Border Guard Service, as
well as representatives from the Council of Importers, which functions under the aegis of the Cabinet of
Ministers. The hotline was established to facilitate reporting of cases of bribery and extortion by Ukrainian
customs officials and to provide quick response of SCSU internal security detachments to complaints by
Ukrainian business entities engaged in international economic activities. The establishment of the phone
hotline represents another step toward rooting out misconduct by Ukrainian customs officers. Earlier, on
April 7, 2005, SCSU chairman Volodymyr Skomarovsky issued an order prohibiting customs officers from
having more than 100 hryvnias ($20) in domestic or foreign currency or cellular phones in their possession
while they are in the customs control areas.

Source: “Kabmin otkryl ‘goryachuyu liniyu’ dlya prekrashcheniya vyzyatotschinstva na tamozhne” [Cabinet of Ministers opened a
phone ‘hot line’ to stop bribery at customs], Ukrainski Novini news agency, April 12, 2005, <http://www.ukranews.com/cgi-bin
/openarticle.pl?lang=rus&id=612859&lenta=po>

Kyrgyz Customs Service Reorganized

On April 14, 2005, acting president and prime minister of the Kyrgyz Republic Kurmanbek Bakiyev signed
an edict On the Reorganization of Financial Regulatory Bodies of the Kyrgyz Republic, which entered into
force the same day. In accordance with the edict, the Committee for Revenues under the Ministry of
Finance of the Kyrgyz Republic was disbanded, while two agencies that had previously been subordinated
to that committee—the Department of Customs Service and the Tax Department—were transformed into
independent agencies and renamed the State Customs Inspectorate and the State Tax Inspectorate, respectively.\[1,2\]

In effect, this is a reversal of the October 1, 2002, reorganization when the Committee for Revenues was created by merging the State Tax Inspectorate and the State Customs Inspectorate.\[1\] Speaking at the Zhogorku Kenesh (Kyrgyz parliament), Bakiyev justified the new reorganization as a way both to make tax and duty collection transparent and effective, and to curb corruption.\[1,2\] Colonel Sarsen Omarkulov has been appointed director of the State Customs Inspectorate.\[3\] The customs agency will report directly to the Cabinet of Ministers.\[1,2\]

Editor’s Note: On March 25, 2005, following the overthrow of President Askar Akayev, the upper house of the Zhogorku Kenesh, the Council of People’s Representatives appointed Kurmanbek Bakiyev acting president and prime minister of the Kyrgyz Republic. All heads of state agencies appointed by Bakiyev are designated “acting” until a new president— to be elected in the presidential election scheduled for July 10, 2005—approves them or appoints new individuals to replace them.


Changes in NIS Export Control Personnel

Heads of Kyrgyz Border Guard and Emergency Agencies Replaced; Border Guards Subordinated to National Security Service

On April 27, 2005, acting president and prime minister of the Kyrgyz Republic Kurmanbek Bakiyev signed an edict dismissing Kalmurat Sadiyev and Temirbek Akmataliyev from their positions as chairman of the Border Guard Service and acting minister of ecology and emergency situations, respectively. Former minister of defense and Zhogorku Kenesh (Kyrgyz parliament) member Myrzakan Subanov was appointed new chairman of the Border Guard Service, and former Zhogorku Kenesh member Dzhanysh Rustembekov was appointed new acting minister of ecology and emergency situations.\[1,2,3\]

Following the dismissal of Sadiyev and Akmataliyev, the General Prosecutor’s Office initiated criminal investigations against them. According to acting prosecutor general Azimbek Beknazarov, Sadiyev was involved in the suppression of opposition protests in Osh, southwestern Kyrgyzstan, in March 2005, and both Sadiyev and Akmataliyev are believed to have orchestrated the shooting of peaceful protesters in Aksy, Jalal-Abad oblast, in March 2002, in which six civilians were killed as a result of clashes between police and protesters.\[3,4\] Akmataliyev was then minister of interior, and Sadiyev was his deputy.\[3\]

In a related development, on May 23, 2005, Kurmanbek Bakiyev signed an edict renaming the Border Guard Service as the Border Guard Troops and subordinating the agency to the National Security Service (NSS) of the Kyrgyz Republic. Due to this change, newly appointed chairman of the Border Guard Service Myrzakan Subanov is to be designated first NSS deputy chairman and commander of the Border Guard Troops.\[5,6\]

International Supplier Regimes

Australia Group’s Plenary Meeting Marks the Organization’s 20th Anniversary; Dual-Use Biological Equipment Control List Expanded

On April 18-21, 2005, the Australia Group (AG) met for its annual plenary, in Sydney, Australia. This year’s meeting marked the 20th anniversary of the AG, which was founded in 1985. The plenary—the first to be held in Australia—was opened by the Australian Minister for Foreign Affairs, Alexander Downer. Minister Downer praised the work of the AG over the previous 20 years noting that “the Group’s forward thinking, cohesive and pragmatic approach to preventing the spread of weapons of mass destruction ensures it achieves practical gains in the fight against proliferation.” Downer also noted the criticisms leveled by some countries “that the export controls [the AG] promotes restrict the access of developing countries to technology transfers.” The minister claimed that “these criticisms have become steadily less vocal in recent years.” Downer explained this development as reflecting the increasing recognition that “[w]hile many states parties to the Chemical Weapons Convention and the Biological Weapons Convention apply export controls in the implementation of their convention obligations, others do not. And many fail to enforce controls in a robust and effective manner. Moreover, in the absence of a verification body for the Biological Weapons Convention, the Australia Group’s development of control lists covering materials and technology relevant to the production of biological weapons represent the only harmonised form of control over these items… It has become increasingly apparent that the well-balanced and harmonised export controls implemented by Australia Group members have brought increased security to this trade [in the chemical and biotechnology sectors], without restricting legitimate trade… [M]any non-Australia Group members have recognised the real value of the Australia Group’s comprehensive control lists in preventing chemical and biological weapons-relevant items and technology falling into the hands of proliferators.”[1]

[Editor’s Note: Downer appears to be reiterating the view that international trade will be increased if there is confidence that exported materials will not be diverted to support prohibited activities. This statement is unlikely to assuage sufficiently the concerns of Iran and other members of the Non-Aligned Movement who regularly express displeasure with the AG in international forums such as the meetings of the Organization for the Prohibition of Chemical Weapons.]

An important development at this year’s plenary was the acceptance of Ukraine as the 39th member of the AG. Ukraine possesses a large chemical manufacturing industry and, according to the AG press release, bringing it into the AG strengthened the credibility and effectiveness of the regime as a whole. Ukraine’s acceptance into the AG continued the process whereby the AG has worked to improve the coordination of the export control regulations of major chemical and biotechnology exporting nations. In this regard, the meeting also welcomed Israel’s recent announcement that it would adhere to the AG export control guidelines in administering its chemical and biotechnology exports.[2]

In order to encourage more states to adopt AG guidelines as the basis for their export control administration, the participants agreed to continue work on developing outreach strategies based on targeted regional approaches. The AG also recognized the need to improve its website by incorporating practical information on export control implementation and translating the site into all official UN languages.[2] [Editor’s Note: Currently the AG website is available only in English, French, German, and Spanish. The implementation of the aforementioned proposal would, therefore, create Arabic, Chinese, and Russian mirror versions of the website.]

Another important development at this year’s meeting, which will serve to increase the timeliness and effectiveness of information sharing among participants, was the establishment of the Australia Group Information System as a secure electronic communication tool between participants.[2] The effectiveness of the AG as a nonproliferation tool is highly dependent on all members having clear and up-to-date knowledge of denied applications in other member states. As a consequence of the new system, the time
and expense involved in processing export permit applications will hopefully be reduced, thus minimizing
the burden on exporters.

The activities of the nuclear proliferation network led by Pakistani nuclear scientist A.Q. Khan were also
noted and led to proposals for the examination of tighter controls on brokering and intermediary activities
in trade involving chemicals and biotechnology.

The AG meeting agreed on a number of important adjustments to the existing control lists. Existing
controls on pumps and genetically modified organisms were revised to improve enforcement and help
exporters better understand their obligations. As part of the AG’s ongoing efforts to keep its common
control lists up to date and scientifically relevant, participants also agreed to examine the addition of up to
25 more biological agents to the control lists.[2] These agents were not added at this meeting but may be
added to the control lists at the next plenary meeting in 2006.

Finally, an agreement was reached on adding a new category of items to the control list of dual-use
biological equipment.[3] The addition of certain types of spraying and fogging systems, which are capable
disseminating biological agents as infectious aerosols, to the control list was a significant enhancement
of international controls, but it is also likely to increase concerns that the AG is impeding the
modernization of developing countries. The AG added what it describes as “the most threatening aerosol
sprayers” to the control list in response to increasing concerns over indications of terrorist interest in
dispersal devices for biological agents.[2] The AG members have attempted to limit the range of items
incorporated in the control list so that the new regulations would not affect traditional crop-dusting type
activities. These activities generally rely on much larger droplet sizes than those suitable for the
dissemination of biological warfare agents.

The AG Control List of Dual-Use Biological Equipment and Related Technology now includes the
following new section:

8. Spraying or fogging systems and components therefore, as follows:
   a. Complete spraying or fogging systems, specially designed or modified for fitting to aircraft,
      lighter than air vehicles or UAVs [unmanned aerial vehicles], capable of delivering, from a liquid
      suspension, an initial droplet “VMD” of less than 50 microns at a flow rate of greater than two
      litres per minute.
   b. Spray booms or arrays of aerosol generating units, specially designed or modified for fitting to
      aircraft, lighter than air vehicles or UAVs, capable of delivering, from a liquid suspension, an
      initial droplet “VMD” of less than 50 microns at a flow rate of greater than two litres per minute.
   c. Aerosol generating units specially designed for fitting to systems that fulfil all the criteria
      specified in paragraphs 8.a and 8.b.[3]

Sources: [1] The Honorable Alexander Downer, Speech before the Twentieth Anniversary Plenary of the Australia Group, 18 April
      2005, Minister for Foreign Affairs of Australia, The Honorable Alexander Downer, MP, website,

International Export Control and WMD Security Assistance Programs

Latvia and United States Sign Nonproliferation Cooperation Agreement; Fresh Fuel
Transferred to Russia

On April 25, 2005, the governments of Latvia and the United States signed an agreement paving the way
for increased cooperation on nonproliferation and threat reduction issues. The agreement, signed by Latvian
Minister of Environment Raimonds Vejonis and U.S. Secretary of Energy Samuel Bodman, provides “for
repatriation to Russia of Soviet-/Russian-origin nuclear fuel from Latvia’s shut-down research reactors at
Salaspils; security enhancement of the reactor site and storage of the nuclear materials at the site; and safe
and secure storage of Latvia’s nuclear materials, including improved methods of protection, control, and
accountability of nuclear materials to reduce the risk of theft or possible diversion of nuclear materials
stored at the premises.”[1]
The Latvian Institute of Nuclear Physics at Salaspils, located 20 miles from Riga, houses a 5 megawatt (MW) research reactor, a zero power reactor—a reactor designed to operate at such a low power level that essentially no heat is produced—as well as spent (used) and fresh nuclear fuel, the last shipment of which was received from Russia in 1986.[2,3,4,5] One of the first research reactors in the Soviet Union, the 5-MW reactor was built in 1959 and went critical in 1961.[6] It was permanently shut down in July 1998 owing to the lack of government funding and concerns for environmental safety in the event of an accident.[2,3]

The April 25 agreement allowed the U.S. Department of Energy’s National Nuclear Security Administration (NNSA) to remove the highly enriched uranium (HEU) fuel stored at Salaspils.[1] [Editor’s Note: HEU is potentially usable as the core of a nuclear weapon and could be an attractive target for terrorist organizations.] The task of repatriating Soviet-/Russian-origin nuclear fuel falls under the jurisdiction of NNSA’s Global Threat Reduction Initiative (GTRI). On May 25, 2005, 2.5 kilograms (kg) of fresh HEU fuel were removed from the Salaspils reactor and returned to Russia. According to the Russian Federal Atomic Energy Agency, the fuel will be downblended at Russia’s Luch Institute into low-enriched nuclear fuel for power plants.[7] [Editor’s Note: Low-enriched uranium is not usable for nuclear weapons.]

Under GTRI’s Russian Research Reactor Fuel Return Program, which is also supported by the International Atomic Energy Agency (IAEA), Russia has accepted to date 107.5 kg of fresh Soviet-/Russian-origin HEU from seven countries—Bulgaria, Czech Republic, Latvia, Libya, Romania, Serbia, and Uzbekistan.[1,2,7] In addition to the Latvian fresh fuel, Russia, the United States, and the IAEA hope to repatriate Russian-origin fresh HEU fuel from two other locations in 2005—the Czech Technical University, in Prague, and a critical assembly in Libya.[1,8]

The timeline for removing the spent fuel stored at Salaspils is less certain, however. In the past, Riga indicated that it was willing to pay Moscow for the transport and repatriation of the spent fuel to Russia, but to date, Russia has not agreed to accept any shipments of Russian-origin spent research fuel.[8,9] [Editor’s Note: Spent fuel is considered less a proliferation threat than fresh fuel because of its highly radioactive nature. Nonetheless, spent fuel that has been only lightly irradiated in a reactor might not pose a major risk to human health and consequently might present a significant risk for theft or diversion.]

Editor’s Note: The United States and other members of the international community have long been involved in working to improve the security of HEU fuel and other materials stored at Salaspils. In the 1990s, the IAEA and a number of countries, including Finland, Sweden, and the United States, provided technical assistance and funding to Latvia to improve material control and accounting regulations and physical protection systems at Salaspils. The latter included the installation of electronic personal identification number (PIN) access controls, a hand-geometry biometric identification system, video surveillance, improved radio communications, motion detectors, and a central alarm system.[10,11]


United States to Install Radiation Detection Equipment on Ukrainian Borders; Ukraine-NATO Commission Adopts 2005 Target Plan

On April 22, 2005, Linton Brooks, administrator of the U.S. Department of Energy’s NNSA, and Colonel-General Mykola Lytvyn, chairman of the State Border Guard Service of Ukraine, signed an agreement to
install radiation detection equipment at key land border posts, airports, and seaports in Ukraine. The special equipment designed to detect, deter, and interdict illicit transfers of nuclear and other radioactive materials will be provided under the NNSA Second Line of Defense (SLD) program. “The United States and Ukraine recognize the need to work cooperatively to stem the threat posed by the trafficking of nuclear and other radioactive materials,” said Brooks. “This agreement will enable our countries to further international nonproliferation efforts and better protect the citizens of Ukraine, the United States and other countries against nuclear terrorism.”[1] The available open sources do not specify which Ukrainian border posts, airports, and seaports will be equipped with radiation detection equipment.

The agreement follows the April 4, 2005, joint statement of U.S. President George W. Bush and Ukrainian President Viktor Yushchenko issued during Yushchenko’s visit to the United States, in which they pledged to “begin a new chapter in the fight against the proliferation of weapons of mass destruction and their means of delivery,” and deepen “cooperation on nonproliferation, export controls, border security, and law enforcement to deter, detect, interdict, investigate and prosecute illicit trafficking of these weapons and related materials; enhance the security of nuclear and radiological sources; and dispose of spent nuclear fuel.”[2]

In a separate development, on April 21, 2005, a meeting of the Ukraine-NATO Commission at the level of foreign ministers was held in Vilnius (where NATO ministerial meetings were taking place). The meeting approved a Ukraine-NATO Target Plan for 2005, which aims to deepen cooperation between Ukraine and the alliance. The document provides for a series of concrete and immediate measures to strengthen democratic institutions, reinforce political dialogue, and reinvigorate cooperation in reforming defense and security sectors. A package of measures also involves enhancing public diplomacy efforts in order to improve understanding of NATO in Ukraine. NATO countries expressed their readiness to offer Ukraine consultative assistance in promoting the integration of its defense industry in the Euro-Atlantic environment, including through the application of NATO standards in arms export controls. To achieve this, the plan envisages intensifying consultations on arms control, export controls, and nonproliferation, among other subjects.[3,4,5,6]

Ukrainian Foreign Minister Borys Tarasiuk stated at the meeting that integration with the Euro-Atlantic community is Ukraine’s strategic objective and priority, and that Kiev could complete the necessary military and political reforms within three years. However, NATO distanced itself from any timeframe and, instead, invited Ukraine to begin an “intensified dialogue” on Ukraine’s aspirations to membership and relevant reforms “without prejudice to any eventual Alliance decision.” NATO Secretary General Jaap de Hoop Scheffer told reporters, “The pace at which any partner comes closer to NATO is based on performance in respecting NATO standards and values. NATO and its member states stand ready to do what we can to help Ukraine achieve them.”[4,6]


U.S. Military Delegation Visits Tajikistan; U.S. Embassy Issues Fact Sheet on U.S. Border Security and Counternarcotics Assistance to Tajikistan

On April 15, 2005, a U.S. military delegation led by Lieutenant General David W. Barno, commander of Combined Forces Command-Afghanistan Anti-terrorist Coalition Forces in Afghanistan, visited the capital of Tajikistan, Dushanbe, where he met with President Emomali Rakhmonov, Minister of Defense Colonel General Sherali Khairulloev, Chairman of the Committee for State Border Protection Colonel General Saidamir Zuhurov, and Director of Drug Control Agency Lieutenant General Rustam Nazarov. In the course of the meeting, Lieutenant General Barno and Tajik officials discussed the current military situation
in Afghanistan, the state of U.S.-Tajik military cooperation, and U.S. assistance to Tajikistan in the areas of border security and counternarcotics.[1,2]

On the same day, the U.S. Embassy in Dushanbe issued an official fact sheet presenting a summary of U.S. assistance to Tajikistan in the areas of border security and counternarcotics.[2] Selected sections of this fact sheet are presented below:

- Since 2002, the U.S. government has provided more than $13 million in border security and counternarcotics assistance to Tajikistan, most of it to the Committee for State Border Protection of Tajikistan. Of the $13 million, $9 million in transportation, uniforms, communications equipment, generators, and training was provided to Tajik border guards.
- The U.S. Department of State fully funds two major projects run by the UN Office of Drug Control (UNODC), including the following:
  - Border Management Assistance. To date the U.S. government has allocated $2.5 million for the UNODC E24 border control project, which aims to assist Tajik law enforcement agencies to upgrade their capacities to identify and intercept drug traffickers, to facilitate the storage and destruction of seized drugs, to promote more effective analysis of seized narcotic substances, and to promote effective use of drug-scenting dogs.
  - Drug Control Agency Assistance. To date, the U.S. government has allocated $3.2 million for the UNODC H03 project to assist the Drug Control Agency of Tajikistan. In 2005, the United States will allocate an additional $3.4 million to help the Drug Control Agency become capable of coordinating national efforts and working with international law enforcement agencies.
- In the framework of the Export Control and Related Border Security Assistance (EXBS) program, to date the U.S. government has provided $4.2 million in uniforms, trucks, and communications and power equipment (see the itemized list below) to Tajikistan. In 2005, the EXBS program will provide $1.2 million in assistance to Tajikistan, and $1.5 million is proposed for 2006.

### Table 1. Equipment Supplied to Tajik Border Guards Through the EXBS Program

<table>
<thead>
<tr>
<th>Type of Equipment</th>
<th>Number of Units</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TRANSPORTATION</strong></td>
<td></td>
</tr>
<tr>
<td>GAZ Passenger Vans</td>
<td>6</td>
</tr>
<tr>
<td>UAZ All-Terrain Vehicles</td>
<td>45</td>
</tr>
<tr>
<td>NIVA All-Terrain Vehicles</td>
<td>10</td>
</tr>
<tr>
<td>KAMAZ Trucks</td>
<td>24</td>
</tr>
<tr>
<td><strong>COMMUNICATION</strong></td>
<td></td>
</tr>
<tr>
<td>Global Positioning Satellite Systems (GPS)</td>
<td>300</td>
</tr>
<tr>
<td>Lap Top Computers (Pentium III)</td>
<td>3</td>
</tr>
<tr>
<td>Barrett High-Frequency (HF) Radios, including:</td>
<td>107 (each unit with spare batteries, chargers and antenna masts)</td>
</tr>
<tr>
<td>- 950L Base Stations</td>
<td>40</td>
</tr>
<tr>
<td>- 950R Mobile Radios</td>
<td>35</td>
</tr>
<tr>
<td>- 940 Man Pack Radios</td>
<td>32</td>
</tr>
<tr>
<td>Motorola Short Wave (SW) Radios, including:</td>
<td></td>
</tr>
<tr>
<td>- GP 140 SW (handheld)</td>
<td>786</td>
</tr>
<tr>
<td>- GP 140 SW (mobile)</td>
<td>350</td>
</tr>
<tr>
<td>- GP 140 SW (base station)</td>
<td>26</td>
</tr>
<tr>
<td>- GP 160 SW (base station)</td>
<td>160</td>
</tr>
<tr>
<td>- GP 160 (handheld)</td>
<td>20</td>
</tr>
<tr>
<td>- Motorola 2000 Repeater Systems</td>
<td>230</td>
</tr>
<tr>
<td>Bushnell Binoculars</td>
<td>8</td>
</tr>
<tr>
<td><strong>POWER EQUIPMENT AND UNIFORMS</strong></td>
<td></td>
</tr>
<tr>
<td>Diesel Generators</td>
<td>9</td>
</tr>
<tr>
<td>Gas Generators</td>
<td>33</td>
</tr>
</tbody>
</table>
### WMD Detection Equipment

<table>
<thead>
<tr>
<th>Item</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radiation Pagers (handheld)</td>
<td>70</td>
</tr>
<tr>
<td>Customs Interdiction Tool Kits (CITKs), each unit includes the following:</td>
<td>2</td>
</tr>
<tr>
<td>• Fiber Optic Scope</td>
<td></td>
</tr>
<tr>
<td>• Light Source</td>
<td></td>
</tr>
<tr>
<td>• Radiation Pager</td>
<td></td>
</tr>
<tr>
<td>• Density Meter (Buster)</td>
<td></td>
</tr>
<tr>
<td>• Basic Tools (1/2, 2/8, j, inch drive socket sets, screwdrivers, wrenches, hammers, crowbar, mirrors, and flashlights)</td>
<td></td>
</tr>
</tbody>
</table>

- In 2004, the U.S. Department of State provided $600,000 through the International Organization for Migration for a pilot project to train Tajik border guards to detect passport and visa fraud. This is part of a regional project aimed at reducing illegal migration and narcotics trafficking through better management of land border crossings.

- In April 2005, the Combined Forces Command-Afghanistan organized the first bilateral meeting between Afghan and Tajik border officials in Kabul, where participants shared intelligence and began establishing working relations necessary for day-to-day border management.

- In May 2005, the U.S. Army Corps of Engineers began construction of a bridge that will connect Tajikistan and Afghanistan. The estimated cost of this construction project is $30 million. It is envisioned that the bridge will serve as a focal point of future bilateral Tajik-Afghan border cooperation.

### United States and Russia Sign Agreement under Second Line of Defense Program

On April 27, 2005, Jerald Paul, principal deputy administrator of the NNSA, and Tatyana Golendeyeva, deputy director of Russia’s Federal Customs Service (FCS), signed the SLD Sustainability Plan. This document commits both sides to ensuring successful long-term sustainability of bilateral efforts under the SLD program to prevent illicit trafficking of nuclear and other radioactive materials across Russian borders. Measures to ensure sustainability include proper maintenance, effective use, upgrade, and replacement of radiation detection equipment; training of local officials in its use; and training of new officials if personnel turnover occurs to ensure the continued and proper use of equipment. In addition, the document acknowledges that the sides are moving closer to a time when sustainability of all systems will be the sole responsibility of the FCS rather than a joint NNSA/FCS responsibility. [1,2]

In a related development, on April 26, 2005, a U.S. delegation led by U.S. Ambassador to the Russian Federation Alexander Vershbow visited a branch of the Russian Customs Academy in Vladivostok, Russian Far East. U.S. officials were familiarized with activities of the local Training Resource Center for Customs Control of Fissile and Radioactive Materials. [3] The center was established in 1999 by FCS's predecessor, the State Customs Committee, to train or retrain customs officials engaged in radiation control.[4] Since its establishment, the center has received more than $200,000 worth of advanced radiation detection and other training equipment under the SLD program. According to the FCS, more than 600 Russian and CIS customs officials have received radiation control training at this center. [3]
DOE Organizes Export Control Seminars in Russia and Georgia

Russia
On April 19-21, 2005, the NNSA’s International Nonproliferation Export Control Program (INECP) held an export control training seminar for Russia’s Federal Atomic Energy Agency (Rosatom) enterprises. Representatives from approximately 20 Rosatom institutes and enterprises located in western Russia attended the seminar. The seminar participants were from facilities that had experienced significant turnover in their internal compliance programs staff or had not received export control training for several years. Presentation topics included profiles of proliferant countries, internal compliance and high-risk property management systems at the U.S. Oak Ridge National Laboratory, the international nuclear export control regime, the Russian export control system, end-use risk, nuclear fuel cycle and control lists, dual-use goods and technology, technology control and identification, internal compliance programs, and legal responsibilities of institute personnel. Lecturers included representatives from Rosatom, the Federal Technical and Export Control Service, the Federal Customs Service, and technical experts from the Institute of Physics and Power Engineering (IPPE, Obninsk, Kaluga Oblast, Russia) and the All-Russia Research Institute of Technical Physics (VNIITF, Snezhinsk, Chelyabinsk Oblast, Russia).

Georgia
A team of INECP and Georgian technical export control specialists conducted a Nuclear Commodity Identification Training workshop in Tbilisi, Georgia, on April 20-22, 2005, and a second workshop at the Red Bridge border guard and customs facility on the Georgian-Azerbaijani border on April 25-27, 2005. The workshops aimed to familiarize customs and border guard officers with items subject to export control regulations and included in the Nuclear Suppliers Group’s trigger and dual-use lists.

Illicit Trafficking in the Newly Independent States (NIS)

IAEA Releases Illicit Trafficking Data for 1993-2004
The IAEA Illicit Trafficking Database (ITDB), established in 1995, contains information confirmed by participating IAEA member states about incidents of illicit trafficking in nuclear and other radioactive materials that have occurred since January 1, 1993. Several hundred additional incidents—reported in open sources but not confirmed by the states—are also tracked in the database but not included in the confirmed statistics. The ITDB includes incidents of unauthorized acquisition, provision, possession, use, transfer, or disposal of nuclear material and other radioactive material, whether intentional or unintentional and with or without crossing international borders. It also includes unsuccessful or thwarted events and incidents involving the inadvertent loss of control of nuclear and other radioactive materials and the discovery of such uncontrolled materials.[1]

The IAEA recently released an ITDB fact sheet for 1993-2004. As of December 31, 2004, more than 650 incidents were confirmed by IAEA member states. The fact sheet does not specify locations of these incidents or the number of incidents that took place in the NIS. Of the 650 episodes, about 30 percent involved nuclear materials, about 60 percent involved other radioactive materials, and the remaining incidents involved both nuclear and other radioactive materials or radioactively contaminated material. About half of the confirmed incidents involved criminal activities—for example, theft, illegal possession, smuggling, or attempted illegal sale of material.[1]

The nuclear material involved in most of the confirmed cases for 1993-2004 was natural uranium, depleted uranium, or low-enriched uranium fuel, none of which can be used directly for nuclear weapons. Only 18 of the confirmed incidents involved trafficking in highly enriched uranium or plutonium—both of which can be used for this purpose—with only a few of the cases involving kilogram quantities of weapons-usable nuclear material. In some cases, the material involved appeared to be a sample of larger quantities allegedly available for illegal sale or at risk of theft. In addition, the majority of the confirmed incidents involving nuclear materials were criminal in nature.[1]
As for the radioactive materials listed in the confirmed incidents, they were in the form of sealed radioactive sources with various activity levels and applications. The majority of these sources used the radioisotopes cesium-137, strontium-90, americium-241, cobalt-60, and iridium-192. These materials cannot be used for nuclear weapons, but they could be used in a radiological dispersal device, or “dirty bomb.” A large portion of the incidents involving radioactive sources were not criminal in nature. Numerous recorded cases involve discoveries of uncontrolled, or orphan, radioactive sources.[1]

The IAEA’s previous release of information from its illicit trafficking database, covering incidents from January 1993 through December 2003, listed only 17 cases as involving highly enriched uranium or plutonium.[2] Although the IAEA released a detailed list of the 17 incidents at the time, no similar list was provided with its 2005 overview of database cases.[1,2] Thus it is not possible to determine whether a new case arose during the intervening year or whether a case that occurred at an earlier time was added to the database.


**Kamchatka Customs Seizes Submarines Destined for China**

In late April 2005, customs authorities in Kamchatka, Russian Far East, seized two diesel submarines that an unnamed Russian federal state unitary enterprise (an official exporter of decommissioned military equipment) was in the process of exporting to China where the vessels were to be broken up as scrap metal. According to the declaration submitted to customs control, all armaments had been removed from the submarines, which are owned by a commercial firm in Kamchatka (also unnamed). However, according to the Far Eastern Customs Directorate, an examination of the vessels resulted in the discovery of equipment on board that had not been declared, including six torpedo tubes. The exporters did not have permission to export this equipment.[1,2,3]

An investigation has been launched under Article 16 Paragraph 2 of the Russian Code of Administrative Violations, “Undeclared or falsely declared goods and (or) means of transport.”[1,2,3] The submarines were towed to the Petropavlovsk-Kamchatskiy Commercial Port for further examination, which includes a determination of whether the torpedo tubes are in operating condition. If so, they will be confiscated.[1] The violation of the customs code may also result in a fine of 50-200 percent of the value of the goods.[3] However, one Far Eastern Customs Directorate source reportedly said that the submarines’ owner would likely pay a fine, fill out a new customs declaration in accordance with requirements, and re-export the submarines to China.[1]


**International Developments**

**Chinese Port of Shanghai Joins U.S. Container Security Initiative; Argentina and Brazil to Follow Suit**

On April 28, 2005, Robert C. Bonner, Commissioner of U.S. Customs and Border Protection (CBP) and Mou Xinsheng, Director of the General Administration of Customs of the People’s Republic of China (PRC), announced that the Chinese port of Shanghai became the 36th operational port under the Container Security Initiative (CSI).[1]
CSI cooperation between the United States and China began on October 25, 2002, when U.S. President George W. Bush and former PRC President Jiang Zemin reached a consensus on the issue in Crawford, Texas. On July 29, 2003, Commissioner Bonner and Director Mou signed the Declaration of Principles on CSI to target and pre-screen cargo containers from the ports of Shanghai and Shenzhen destined for U.S. ports. According to a written statement by Mou Xinsheng, “the Chinese government firmly opposes and condemns terrorism in all its forms and manifestations, and actively takes actions to prevent and combat all terrorist activities. China and the U.S. have great prospects for anti-terrorism cooperation and both sides’ efforts in strengthening cooperation in container security are a good example.” U.S. Ambassador to the PRC Clark T. Randt, Jr., said, “I am pleased that CSI is now extended to the port of Shanghai, China’s busiest port and one of the world’s most important ports. I look forward, also, to the opening of CSI in Shenzhen in the coming months.”[1] (For more detail on the negotiations between China and United States on CSI, see Shi-Chin Lin, “The U.S. Container Security Initiative in Asia,” Asian Export Control Observer, No. 2, June/July 2004, pp. 18-21.)

In a related development, on May 9, 2005, U.S. Ambassador to Argentina Lino Gutierrez and Dr. Alberto R. Abad, federal administrator of National Revenue of the Argentine Republic, signed the Declaration of Principles on CSI. Argentina is the first South American country to participate in the CSI. It is expected that Buenos Aires will become the first Argentine port to join the initiative.[2] On May 24, 2005, U.S. Ambassador to Brazil John Danilovich and Antonio Deher Rachid, Brazil’s secretary of the Federal Revenue Secretariat, signed the Declaration of Principles on CSI. In accordance with the declaration, the port of Santos, a major export center in southeastern Brazil and the largest port in South America, will become the second port in this part of the world to be included in the CSI.[3]

The CSI is a U.S. initiative launched in January 2002, with the aim of securing maritime containerized cargo shipped to the United States against terrorist threats, by inspecting such cargo at the port of embarkation. As of May 2005, the 36 operational ports collaborating in the CSI effort and representing the world’s major seaports are: Antwerp and Zeebrugge, Belgium; Halifax, Montreal, and Vancouver, Canada; Shanghai, China; Le Havre and Marseilles, France; Bremerhaven and Hamburg, Germany; Piraeus, Greece; Rotterdam, The Netherlands; Hong Kong; Genoa, Gioia Tauro, La Spezia, Livorno, and Naples, Italy; Kobe, Nagoya, Tokyo, and Yokohama, Japan; Port Klang and Tanjung Pelepas, Malaysia; Singapore; Durban, South Africa; Busan, South Korea; Algeciras, Spain; Göteborg, Sweden; Laem Chabang, Thailand; Dubai, UAE; and Felixstowe, Liverpool, Southampton, Thamesport, and Tilbury, United Kingdom.[1]


German Media Report Illegal Technology Transfers to Iran

The German press recently reported two cases of illegal technology transfers from Germany to Iran, the first involving a high-tech crane and the second involving vibration test machines.

The April 25, 2005, issue of the German news magazine Der Spiegel reported that a state-of-the-art crane built by the German firm Liebherr was shipped to Tehran-based Mizan Machine, a firm believed to be a front for Iran’s weapons program and blacklisted by German customs. The crane was loaded aboard the Bahamas-flagged freighter Hual Africa in Hamburg on April 7, 2005. For reasons that are unclear, German customs officials became aware of the shipment only after the ship had already left the port of Hamburg. According to Der Spiegel, the crane should not have received clearance for export to Iran at all. A further investigation by German authorities concluded that the crane is probably intended for use in Iran’s Shahab missile program. Iranian Foreign Ministry Spokesperson Hamid Reza Assefi rejected allegations that the crane was to be used in association with Tehran’s Shahab missile program. “This is a baseless claim and theory. It is unclear how crane equipment can be used in Shahab missiles,” said Assefi.[1,2,3] [Editor’s Note: Iran’s Shahab-3 missile has a range of 1,200 miles (1,931 km) and can reach most points in the Middle East, including Israel. Cranes can be used to support Shahab-3 missiles in the field or at storage

NIS Export Control Observer, May 2005 15
facilities. The missile is launched from a transporter-erector-launcher (TEL). A large truck-mounted crane would be standard equipment in any logistical support unit. Its purpose would be to transfer the Shahab-3 missile body from a support vehicle to the TEL. It is not clear from the available information whether or not the German crane is a truck-mounted or fixed crane, however.

The German Economics Ministry coordinated its efforts to halt the shipment with other German government authorities and foreign governments, including the United States, which issued a statement on April 28 that it was concerned about the shipment. As of April 23, 2005, Hual Africa and its cargo were at Port Said, Egypt, on the Suez Canal. German government officials have suggested that the country’s foreign trade law could be invoked to halt the shipment. At the writing of this issue of the NIS Export Control Observer, no additional information on the status of the shipment to Iran has appeared in open sources.[1,2,3]

A second case of illegal technology transfer to Iran was reported by two German magazines—Der Spiegel and Focus. According to the reports, the export chief of Tria, a defense company located in the eastern German state of Thuringia, was arrested on April 28, 2005, on suspicion of espionage. The suspect, identified as 64-year-old Peter K. (full name not revealed), and other employees of Tria have reportedly provided Iran with about 15 vibration machines since 2001 that can be used to test missile turbines.[4,5] The arrest of Tria’s export chief was followed by the May 2005 arrest of Tria’s manager, identified as Volker St., who is suspected of working for a foreign intelligence service and breaching export regulations.[6] German authorities began to investigate Tria after an unnamed intelligence service in the Gulf region discovered a high-tech shipment from Thuringia to Dubai, ultimately destined for Iran. The intelligence service provided the German government with information on the suspicious transaction. No further open source information on the status of the Tria case was available at the time of this writing.[4,5]

Germany and its European Union partners, the United Kingdom and France, have been at the forefront of negotiations to persuade Tehran to abandon civil nuclear activities some believe are a cover for a nuclear weapons program. These recent allegations about the possible transfer of German technology to Iran’s missile program are likely an embarrassment to Berlin and serve as a reminder that even countries with advanced export control systems are not immune to illegal technology leakage.


GAO Criticizes U.S. Export Control System

On April 7, 2005, the U.S. Government Accountability Office (GAO), the federal agency in the United States charged with assessing federal programs and expenditures, issued a report highlighting weaknesses and inefficiencies in the country’s arms export control system and criticizing the U.S. Department of State for failing to implement significant changes to the system since the September 11, 2001, terrorist attacks. (The report, entitled “Defense Trade: Arms Export Control Vulnerabilities and Inefficiencies in the Post-9/11 Security Environment,” may be accessed at <http://www.gao.gov/new.items/d05456r.pdf>.)

The U.S. arms export control system is directed by the State Department’s Directorate of Defense Trade Controls under the authority of the 1976 Arms Export Control Act. In this capacity, the department seeks to ensure that exports of arms are consistent with U.S. national security and foreign policy objectives. Other parts of the U.S. export control system—including the export control system directed by the U.S. Department of Commerce’s Bureau of Industry and Security covering dual-use strategic commodities—were not assessed in this GAO report.

The GAO has issued numerous reports over the last several years that identify weaknesses in the U.S. arms export control system and inefficiencies in the current administration’s management of that system. The weaknesses identified by the GAO in the current and past reports “relate to the most basic aspects of the
arms export control system—which items should be controlled and when those items should be subject to government review prior to export.” Specifically, the report notes that the current system lacks clarity as to whether an item is controlled by the State or Commerce Department. The jurisdictional disagreements involve sensitive defense items, such as those related to missiles and night vision. The GAO report also highlighted limits on the government’s ability to ensure that exports exempt from licensing requirements comply with laws and regulations. For example, the report states, some arms exports to Canada do not require licenses. When exemptions are used, the burden for ensuring the exports’ legitimacy shifts from the State Department to exporters. To help ensure that exemptions are properly used and items are safeguarded, the report stresses, exporters need sufficient guidance to minimize the possibility of incorrect interpretations of the regulations and improper exports. The April 7, 2005, report summarizes recommendations from past GAO reports and indicates which of these have not yet been implemented. According to the report, however, State Department officials maintain that significant changes to the arms export control system are not needed.

The GAO concludes that it is time to step back and rethink whether the current system adequately protects U.S. interests in a post-September 11 environment.


UN Readies New Treaty to Curb Nuclear Terrorism

On April 13, 2005, the UN General Assembly unanimously adopted the International Convention for the Suppression of Acts of Nuclear Terrorism. The convention will provide a legal basis for international cooperation in the investigation, prosecution, and extradition of those who commit terrorist acts involving radioactive material or a nuclear device.

The convention will open for signature on September 14, 2005, at the high-level plenary meeting, scheduled for the General Assembly’s 60th session. It will enter into force after 22 states ratify it.[1,2]

Under the convention, it is an offense for a person to possess or use radioactive material, damage a nuclear facility (such as a nuclear power plant) with the intent to cause death or serious bodily injury or substantial damage to property or the environment, or to compel a natural person, a legal person, an international organization, or a state to take or refrain from taking a specific action. Radioactive material is defined to include both materials that might contribute to the manufacture of a nuclear explosive and materials that (because of their inherent radioactivity) could be used in a radiological dispersion device, or “dirty bomb.”

The convention calls for states to develop appropriate legal frameworks to criminalize nuclear terrorism–related offenses and requires that alleged offenders be either extradited or prosecuted. It also encourages states to cooperate in preventing terrorist attacks by sharing information and assisting each other in connection with criminal investigations and extradition proceedings.[3]

In addition, parties are called upon to provide technical assistance in the aftermath of nuclear terrorism incidents. The convention also requires states to make every effort to adopt appropriate measures to ensure the protection of materials usable for the development of nuclear weapons or dirty bombs, taking into account relevant recommendations and functions of the IAEA. The text of the International Convention for the Suppression of Acts of Nuclear Terrorism may be viewed at <http://www.un.int/usa/a-59-766.pdf>.

The convention is based on a draft instrument submitted by Russia in 1998 and is the first treaty adopted at the UN at the initiative of that country.[3,4] U.S. President Bush and Russian President Putin called for early adoption of this convention in their February 24, 2005, joint statement on Nuclear Security Cooperation.[5]

The convention deals only with offenses committed by persons. Article 4 of the treaty makes clear that the convention does not cover the use of nuclear arms by states, declaring, “This Convention does not address, nor can it be interpreted as addressing, in any way, the issue of the legality of the use or threat of use of nuclear weapons by States.”
Potential Restrictions on Chinese Re-Exporting of Russian Engines to Pakistan

On May 13, 2005, the state-owned Russian arms-trading firm Rosoboroneksport signed a contract with a Chinese aerospace firm to supply 100 RD-93 engines, spare parts, and technical services to be used in Chinese FC-1 fighter aircraft. Under the $267 million agreement, the contract may be extended to provide an additional 500 engines. The Russian Aircraft Corporation “MiG” (RAC “MiG”) will produce the engines at its Chernyshev Machine-Building Enterprise in Moscow and at its V. Ya. Klimov Plant in St. Petersburg. [Editor’s Note: The RAC “MiG” was formed in 1999 from a merger of the major manufacturers and developers of the Russian MiG aircraft. The Federal State Unitary Enterprise RAC “MiG” is the first fully integrated aircraft company in Russia and is a full-cycle enterprise combining all aspects of production, sales, support, and overhaul. RAC “MiG” is an official main contractor to the Russian Ministry of Defense and has long-standing marketing agreements with Rosoboroneksport. The Klimov Plant specializes in development of aircraft engines, while Chernyshev carries out the production of the engines.] [2] The delivery contract between the Russian and Chinese companies does not currently allow for the production of the RD-93 engines at Chinese plants. [Editor’s Note: While Russia up to now has not allowed Chinese companies to be involved in aero-engine production, there have been technology transfers in other aerospace areas, such as avionics and fire control.]

After the deal was announced, questions arose about whether Russia would allow re-export of these engines. The Chinese and Pakistani aerospace industries have cooperated in the development of the FC-1 fighters—also known as the JF-17 Thunder—since the early 1990s. Of the 400 fighters expected to be produced under this cooperation, the Pakistani military will receive 150 aircraft and China will retain the remaining 250 fighters, most likely for the export market. [Editor’s Note: The JF-17 Thunder is being jointly developed by China’s Chengdu Aircraft Group Corporation, in cooperation with the China Aero Technology Import and Export Corporation (CATIC) and the Pakistan Aeronautical Complex at Kamra. The United States imposed sanctions against CATIC in December 2004, reportedly for assisting Iran with its missile development program.] The JF-17 prototype made its maiden flight on September 3, 2003, and is currently undergoing trials for its fourth prototype. Pakistan plans to receive the first four aircraft by the end of 2006 for trial flights and then begin domestic serial production of the JF-17 at Kamra by 2007. [6]

The use of the Russian engines in the JF-17s may cause problems for this plan, however, as Russia has committed itself not to supply arms to Pakistan. On December 1, 2004, at a press conference in New Delhi, Russian Defense Minister Sergey Ivanov stated, “At the request of the Indian side, we have virtually no military-technical cooperation with Pakistan.” [7] Owing to objections from India over the supply of Russian engines to Pakistan, a source in Russia’s Federal Service for Military Technical Cooperation told the Russian newspaper Kommersant, China is not being given the right to re-export the engines either separately or installed in the FC-1 aircraft. However, according to one expert on China’s defense industry, the use of Chinese-made engines would not be feasible since China has not developed a power plant “sufficiently suitable for the FC-1. The aircraft has to be powered by the RD-93.” [4] Russian reluctance to allow re-export of the engine could also prove a problem for China’s marketing of the aircraft to other customers. A number of other countries, including Iran [8] and Zimbabwe [4], have reportedly already made orders for this aircraft.

Pakistani officials appeared unconcerned about the Russian statements about the engines’ re-export. The Pakistani head of the joint JF-17 project, Air Vice Marshal Shahid Latif, responded to the Russian reports in early May 2005, stating that there would be no hurdles to acquiring the Russian-produced engines, as China has already provided written assurances to Pakistan that the Russian engines would be supplied.

According to Latif, the statement by the Russian Defense Minister in India had been motivated by political reasons and was not a concern for Pakistan.[9]


Special Report

The Globalization of Nuclear Smuggling: Methods Used by Two Pakistan-Based Networks

As nuclear smuggling networks are becoming global, it is important to understand how proliferators manage to bypass existing export control systems and exploit the weaknesses of multilateral regimes. This article describes the methods used by two Pakistan-based networks—the little-publicized Karni-Khan network and the better-known A.Q. Khan network. Apart from being both based in Pakistan, these two networks have many other similarities: they both extended to various countries of the world, they involved people knowledgeable in the nuclear area, they capitalized on an unexpected flaw in the Nuclear Suppliers Group (NSG) regime, and they exploited the weaknesses of national export control systems.

The Case of Asher Karni and Humayun Khan

by Stephanie Lieggi, Center for Nonproliferation Studies, Monterey Institute of International Studies

In April 2005, a Washington, DC, federal grand jury unsealed an indictment handed down against Pakistani businessman Humayun Khan for violating U.S. export control laws, conspiring to violate federal laws, and aiding and abetting the violation of federal laws. If convicted, Khan, who lives in Islamabad and is not in U.S. custody, could face a maximum penalty of 35 years in prison, although, based on federal sentencing guidelines, a period of incarceration ranging from 78 to 97 months is more likely.[1,2]

The federal indictment followed earlier action taken by U.S. authorities against Humayun Khan. On January 31, 2005, the U.S. Department of Commerce’s Bureau of Industry and Security (BIS) issued a temporary order denying exports to Khan and his Islamabad-based company Pakland PME for at least six months. According the BIS, a “Temporary Denial Order (TDO) is needed to give notice to persons and companies in the United States and abroad that they should cease dealing with [Khan and Pakland] in export transactions involving items subject to the EAR [the U.S. Export Administration Regulations].”[3]

Both the denial order and indictment were based on evidence implicating Khan, his company, and “others, known and unknown” in the illegal export from the United States to Pakistan of items controlled by EAR. According to BIS, the accused “caused and attempted to cause exports of items controlled for nuclear non-proliferation reasons to Pakistan with knowledge that violations of the EAR would occur, and that [the accused] took actions intended to evade the EAR.”[3]

According to U.S. authorities, Khan conspired to purchase an unspecified number of oscilloscopes and 200 triggered spark gaps from U.S. companies.[3] Khan allegedly arranged for the transfers of the spark gaps and oscilloscopes to Pakistan with the assistance of Asher Karni, an Israeli citizen based in South Africa. Karni’s company, Top-Cape Technology, specializes in acquiring military and aviation equipment for customers. According to media reports, Top-Cape appeared to be working as a middleman for individuals in a number of countries interested in buying sensitive military and dual-use items.[4,5]

U.S. federal prosecutors first convened the grand jury that issued the 2005 indictment in October 2003 in order to examine the activities of Karni and Khan. Karni was arrested by U.S. authorities in January 2004.[4] He pled guilty in U.S. federal court to conspiracy and to violating U.S. export control regulations.
His plea was announced shortly before the Khan indictment was released.[2] The case against Khan appears to have been strengthened by information provided by Karni after his arrest.[6]

Khan and his family business have worked closely with the Pakistani military for decades, according to press reports, and investigators suspect that the items in question were meant for Pakistan’s nuclear program. These reports indicate that the Khan family business has been helping supply the Pakistani nuclear program for a number of years, with one source noting that its work began as early as 1975.[7,8] After the issuing of the BIS denial order, Khan gave an interview to the New York Times, in which he claimed that his company supplied civilian companies and laboratories, and that it only rarely worked with the Pakistani military. However, according to the same New York Times report, evidence produced by Khan to show the non-military purpose of his dealings, such as letters from civilian companies requesting items such as oscilloscopes, appeared to have been fabricated when the newspaper checked them further.[8]

Bypassing U.S. Export Controls: Use of Brokers and False End-User Information

According to the federal indictment, Khan, with full knowledge that the items would require export licenses, engaged the services of Karni to procure nuclear dual-use items from U.S. companies.[1] U.S. prosecutors claim that in August 2002, Khan contracted with Karni to have him to acquire oscilloscopes, and, in an email presented to the court, Khan warned Karni to “approach these cases carefully as all items are controlled.”[2] [Editor’s Note. Although U.S. export controls for most oscilloscopes were liberalized in 1997, sophisticated oscilloscopes—such as those that were the subject of the Khan indictment—that can be used to measure nuclear weapons yields and assist with improving warhead designs remain under export controls, particularly to countries where concerns about diversion to nuclear weapons facilities are present—such as Pakistan. Such oscilloscopes can also be used for testing telecommunications equipment, computers, and consumer electronic equipment repair and maintenance.] In December 2002, Khan sent Top-Cape a purchase order for a Model TDS 3054B oscilloscope, produced by the Oregon-based firm Tektronix. [Editor’s Note: Pakland Corporation is the official distributor of Tektronix products in Pakistan. Tektronix’s website lists oscilloscopes as one of the products in which Pakland specializes. However, according to the Tektronix’s spokesperson, shipments to the company are on hold pending the outcome of Khan’s criminal investigation.][8,9] A month later, Khan arranged for Karni to receive payment for the single oscilloscope, and in February 2003, Karni had “a broker in Israel with an affiliate in Plainview, New York,” order the item. Karni’s broker shipped the oscilloscope “and related items” to Top-Cape in Cape Town, which Karni, in turn, forwarded on to Pakistan.[1]

South Africa is a member of the NSG, and therefore many dual-use items, such as those Karni procured for Khan, do not require licenses from the U.S. government—if South Africa is the end destination. In regard to the oscilloscope transfers—and similarly with the spark gap transfers discussed below—since the U.S.-based broker that Karni used exported the items to South Africa, and there was no indication given by Top-Cape that the final destination was Pakistan, the transfers of the oscilloscopes did not require an export license. Therefore the initial part of these transactions—the shipment of the oscilloscopes from the United States to South Africa—did not violate U.S. export control regulations. The regulations were violated, however, once Karni and Khan conspired to re-export of these items to Pakistan

With this first transaction completed, Karni and Khan repeated the subterfuge of routing controlled goods bound for Pakistan through South Africa. In May 2003, Khan, U.S. investigators claim, contacted Karni to arrange for the transfer of additional oscilloscopes manufactured by Tektronix. According to the federal indictment, Khan asked Karni to procure “22 Model TDS 7154 oscilloscopes, 14 Model TDS 784D oscilloscopes, and related components, purportedly on behalf of a Pakistani company known as M/S Matrix Telecom Technologies.”[1] Karni directly contacted Tektronix’s Austrian representative about acquiring some of the oscilloscopes, noting that the end user would be Matrix in Pakistan. Tektronix appeared to be suspicious of Karni’s request. According to U.S. government accounts, Khan was contacted via email by a representative of Tektronix asking him if he knew of the company Karni was purchasing for—Matrix—and if he was aware of any attempt by this company to purchase oscilloscopes. [Editor’s Note: As noted above, Pakland is a certified distributor of Tektronix products in Pakistan.] Khan replied that he was unaware of the deal, and that he “would know if there is any telecom business in the air, but again there is no such demand that we
Tektronix reportedly sent Karni an export license application and an end-user certificate, noting that Karni had to guarantee that the equipment would not “be used in nuclear explosive activities; unsafeguarded nuclear activities; safeguarded or unsafeguarded nuclear fuel cycle activities or be directly employed in the design, development, production, stockpiling, or use of missiles or chemical and biological weapons.”[4] Karni did not reply to Tektronix correspondence and, on May 30, 2003, Khan sent Karni an email stating: “You’re (sic) friends exposed our country, pls see that this does not get further, like our name, customer name, etc. Appreciate it if you can play it ‘safe’ or we may lose this great opportunity.”[1,4] Karni then contacted Giza Technologies in New Jersey to obtain assistance with acquiring the requested equipment. [Editor’s Note: The indictment against Khan does not specifically list Giza but does mention that Karni worked with a broker in Secaucus, New Jersey. However, earlier media reports and recently released emails, which are available at <http://www.pbs.org/frontlineworld/stories/nuclear/conversation.html>, point to Giza as the broker Karni worked through in New Jersey.] In late August 2003, the oscilloscopes were sent to Top-Cape, then forwarded to Khan’s customer in Pakistan.[1]

Thanks to information provided by a still-unknown individual in South Africa, authorities at the BIS Office of Export Enforcement (OEE) and U.S. Immigration and Customs Enforcement (ICE), under the Department of Homeland Security, became aware of Karni’s activities in July 2003. OEE and ICE agents, reportedly with the assistance of South African authorities, were able to track his dealings with Khan, including their email correspondence.[3] Many familiar with the case agree that without this tipster the transactions between Karni and Khan would not likely have been detected by authorities.

While Top-Cape was still working on acquiring various oscilloscopes for Pakland and its customers, Khan asked Karni to purchase another nuclear dual-use item. In June 2003, according to U.S. government charges, Khan contacted Karni regarding the proposed purchase of a large number of triggered spark gaps (Model GP-20B) from the Massachusetts-based PerkinElmer Optoelectronics, noting that Karni should “not disclose the end destination.” After an initial inquiry by Karni to its affiliate in France, PerkinElmer representatives informed Karni that the items would require export licenses, an end-user certificate, and assurances that the triggers would not be re-exported.[11] Karni emailed Khan that he would not proceed with the purchase under these circumstances. [Editor’s Note: Triggered spark gaps are used in medical equipment for the treatment of kidney stones and gallstones, but can also be used as triggers for nuclear weapons. Triggered spark gaps that have an anode delay time of 15 microseconds or less and are rated for a peak current of 500 amperes or more are controlled under the guidelines of the Nuclear Suppliers Group (NSG) and also under the E.A.R. Spark gaps with capacity below these guidelines—which include Model GP-20B—may also require an export license if the exporter has reason to suspect the item could be diverted for use in a nuclear weapons program. This "catch-all" provision seems to have been the reasoning for PerkinElmer to have informed Karni of the requirement for an export license in the initial stages of this transaction.]

In response to Karni’s email, Khan pressed him to proceed with procuring the triggered spark gaps. In an email to Karni, Khan asked him “to re-negotiate [the purchase] from any other source, we can give you an end user information [sic] as it is genuinely medical requirement [sic].”[11] Karni agreed to acquire the spark gaps for Khan, and, in July 2003, he contacted Giza Technologies to arrange for Giza to broker the deal.[1] In August 2003, a representative of Giza wrote Karni that no export license would be required since the items were heading for South Africa. However, a few weeks later the representative wrote back that PerkinElmer would require some end-user information before completing the sale. Since South Africa was the given end destination for the items, the request for extra end-user information appeared to be an attempt by PerkinElmer to assure that they had carried out due diligence in assuring the item would not be diverted for illegal activities.[11] In response, an associate of Karni’s from Top-Cape identified the end-user as “Baragwath Hospital, Soweto, South Africa.” [Editor’s Note: In an interview with U.S. news program Frontline, administrators of Baragwath—South Africa’s largest hospital—stated that the hospital never ordered this equipment.][12]
In September 2003, Karni’s broker in New Jersey sent 66 triggered spark gaps to Cape Town. Since U.S. authorities had been tracking Karni’s actions for a number of months, they were aware of this transaction and convinced PerkinElmer to render the spark gaps in this shipment unusable. After arrival in Cape Town, the shipment of spark gaps was then sent to Pakistan, via the United Arab Emirates.[2]

Armed with the information provided by the still unnamed tipster, U.S. and South African authorities, who had been working together in this investigation, searched Asher Karni’s house in December 2003, removing electronic records and files. Despite the search, Karni flew to Denver, Colorado, less than a month later for a family ski vacation, where he was arrested by U.S. authorities as he disembarked.[13]

In September 2004, investigators from the IAEA visited South Africa to investigate the nuclear smuggling revelations. According to Abdul Samad Minty, head of the South African Council for the Nonproliferation of Weapons of Mass Destruction, the South African government was cooperating fully with the IAEA in its investigation. South African investigators have also worked closely with U.S. authorities in building a case against Karni and Khan.[14]

Karni/ Khan Investigation Continues

Shortly after the release of the indictment against Khan by U.S. authorities, the deputy chief of mission in Pakistan’s Washington embassy, Mohammed Sadiq, stated that Khan “was not involved in procuring triggers or other equipment for Pakistan’s nuclear program.” Sadiq continued that the case was being exploited by “the dirty tricks department of certain lobbies who look for excuses to malign Pakistan.”[15] He also pointed to the fact that, although Karni is reported to have also had dealings with elements in India, no Indian had yet to be indicted.[16, 17]

With the recent indictment of Khan, U.S. authorities are currently trying to obtain his extradition from Pakistan. This process is likely to be long and difficult, as Pakistani authorities do not appear anxious to admit to another nuclear smuggling ring within its borders after the revelations of the network headed by Pakistani scientist A.Q. Khan. Conflict within the U.S. government also appears to have slowed the earlier investigation. With Pakistan an important partner in the war on terrorism, some officials in Washington are hesitant to antagonize Pakistan.[5]

Since his arrest, Karni has assisted investigators by providing further information about individuals in a number of countries he has assisted with illicitly procuring nuclear-related items. While the most prominent “co-conspirator” appears to be Humayan Khan, U.S. authorities are also investigating several other individuals.[13]

How the Abdul Qadeer Khan Network Circumvented Export Controls

by Kenley Butler, Center for Nonproliferation Studies, Monterey Institute of International Studies

Ongoing investigations by the United States, other governments, and the IAEA into the nuclear smuggling network led by Pakistani nuclear scientist Abdul Qadeer Khan have revealed a complicated and seemingly ever-expanding web of manufacturers, middlemen, and customers that extends to more than 30 countries. The A.Q. Khan network supported the nuclear weapons program of Libya, which that country renounced in December 2003, and clandestinely supplied sensitive nuclear technology to Iran and North Korea.

One of the striking aspects that the ongoing investigations have revealed is the ability of the A.Q. Khan network to evade national export control systems and exploit weaknesses in international export control regimes, regimes designed to stem the flow of illicit nuclear technology. A key technique used by Khan to avoid detection was to spread out production and distribution of nuclear equipment among many countries with no history of seeking nuclear weapons themselves or of actively supporting proliferation by others. According to IAEA General Director Mohamed ElBaradei, “Nuclear components designed in one country could be manufactured in another, shipped through a third (which may have appeared to be a legitimate user), assembled in a fourth, and designated for eventual turnkey use in a fifth.”[18]
Turkey was one of the numerous countries exploited by the network. A May 2004 IAEA report revealed that components for uranium enrichment centrifuges shipped to Libya via Dubai (United Arab Emirates) in March 2004 were assembled in Khan network workshops based in Turkey. The centrifuges can be used to improve natural uranium to highly enriched uranium, suitable for use in nuclear weapons. The Turkish workshops imported subcomponents from Europe and elsewhere, and, after assembly, shipped assembled components to Dubai under false end-user certificates for repackaging and shipment to Libya.[19] [Editor’s Note: During the 1970s and 1980s, the United States was aware of shipments of electrical components—many of them manufactured in the United States—from Turkey to Pakistan, at a time when the A.Q. Khan network was illicitly importing nuclear goods into Pakistan to support that country’s nuclear weapons program. According to a March 2005 article in Arms Control Today, the United States issued dozens of demarches to Ankara during this period, but Turkish officials claimed their country’s export control laws were too weak to allow the government to interfere with such trade. Although Turkey subsequently adopted more stringent controls, Turkish authorities have not enforced them effectively, according to the Arms Control Today article. ][20]

Malaysia was also involved in a string of transactions orchestrated by the A.Q. Khan nuclear supply network intended to provide Libya with centrifuges. A Malaysia-based engineering company, Scomi Precision Engineering (SCOPE), manufactured centrifuge components that were shipped to a Khan middleman in Dubai for later shipment to Libya. According to the Malaysian investigation, SCOPE staff was under the impression that the components were intended for the petroleum and gas industry. When shown photographs of the components, experts from the Malaysian Institute of Nuclear Technology Research and the Malaysian Energy Licensing Board noted that the “parts could easily be fitted into many industrial or home components” and suggested one would have to know the existence of a secret nuclear network before concluding the parts were intended for a nuclear centrifuge. The 14 different types of components manufactured by SCOMI could not have been assembled into a complete centrifuge; rotors, for one, were missing, according to the Malaysian police report. SCOPE produced the following components: casings, molecular pumps, top spacers, positioners, top ends, crash rings, stationary tubes, clamp holders, and flanges. A Swiss engineer, Urs Tinner, was brought in at the suggestion of Khan network operative Buhari Sayed Abu Tahir, to oversee production of the components and manage the project. The Malaysian police report into SCOPE concluded that the company and Malaysian authorities did not violate any national laws or Malaysia’s obligations under the nuclear Nonproliferation Treaty, which requires parties, such as Malaysia, to control exports of highly specialized nuclear equipment.[21] Tinner, currently being held by German authorities, is awaiting extradition to Switzerland, where he will be charged for his role in the endeavor. According to the German newsmagazine Der Spiegel, Tinner will face reduced charges because of his agreement to provide information to U.S. intelligence services about the network.[22]

South Africa was also used by the Khan network. An investigation led by South African authorities in cooperation with the IAEA and a number of other countries uncovered at least two companies—Trade Fin Engineering and Krisch Engineering—with alleged connections to the Khan network. As a result of the investigation, 11 containers filled with uranium enrichment components intended for Tripoli’s nuclear weapons program were seized by South African authorities outside Johannesburg in September 2004.

Even advanced Western countries were not immune to exploitation by the Khan network, as revealed in a March 2005 article in the trade newsletter NuclearFuel discussing an episode in the Netherlands.[23] In 1999, according to the report, the Dutch firm Slebos Research shipped six U.S.-produced absolute capacitance manometers to Pakistan. Officials cited in the article suggest that the manometers—dual-use equipment used to monitor the uranium hexafluoride (UF6) gas flow in uranium enrichment plants—may have been reverse engineered and sold by the recipient, Khan Research Laboratories, to other parties, including Iran, Libya, and North Korea. Although manometers are featured on the NSG dual-use list and Dutch customs intelligence had been tracking Slebos since 1985 and had warned the company about exporting dual-use items to Pakistan, Dutch customs authorities did not question the shipment, labeled as transducers, when it left Amsterdam’s Schiphol Airport in 1999. The U.S. manufacturer, MKS Instruments of Wilmington, Massachusetts, did not know that its German subsidiary had sold the equipment to Slebos until two years later.
In spite of President George W. Bush’s February 2004 assessment that the Khan network “is being dismantled,”[24] there is evidence to suggest parts of it or other networks like it continue to circumvent export controls and operate as before. One IAEA official quoted by the New York Times in December 2004 said, “It may be more like Al Qaeda, where you cut off the leadership but new elements emerge.”[25] The IAEA is still looking for additional suppliers and customers and a separate U.S. investigation has so far failed to unravel Khan’s web of suppliers.[26]

Moreover, while the Pakistani government may be cooperating in closing down elements of the A.Q. Khan network involved in supporting nuclear programs in other states, Islamabad continues to rely on elements of the network to support its own nuclear weapons program. Press accounts from the March 2005 report, for example, that Pakistani agents had been recently caught trying to make illicit purchases of specialized steel and nuclear triggers.[5] “General procurement efforts (by Pakistan) are going on. It is a determined effort,” said a diplomat from a member of the NSG. Nuclear experts say these channels involve new middlemen not involved in previous transactions.[27] And a source close to Khan Research Laboratories in Islamabad told Time magazine earlier this year that “nothing has changed”—the network has not stopped.[28]
