Inside this Issue

Recent Developments in the NIS ............... 2
- Supreme Military Institute of Customs Established in Uzbekistan
- Russia Opens New Checkpoint on Border with Azerbaijan
- GUUAM, U.S. To Cooperate in Anti-Terrorism and Border Security Operations
- Kazakhstan’s Lower House of Parliament Approves Draft Amendments to Export Control Law
- Ukraine Introduces Internal Compliance Program Certification for Industrial Concerns

International Supplier Regimes .............. 5
- Australia Group Expands List of Controlled Pathogens
- Kazakhstan May Join MTCR
- Chairman of MTCR Ambassador Mariusz Handzlik makes his first official visit to Belarus

International Assistance Programs .......... 6
- U.S. Export Control Initiatives
- U.S. Government Provides More Assistance to Tajikistani Border Guards and Customs Officers under the Auspices of Export Control-Border Security (EXBS) Program
- Uzbekistan to Receive Aid to Restore Termez-Hayraton Checkpoint

Embargoes and Sanctions Regimes .......... 9
- U.S. Imposes Sanctions on Chinese Norinco Conglomerate over Exports to Iran

Illicit Trafficking in the NIS ............... 10
- Stolen Europium Found in Kyrgyzstan
- Two Incidents of Pathogen Smuggling Reported
- Two Radioactive Smuggling Cases Occur in Georgia within Weeks

Summaries from the NIS Press ............... 12
- Tensions Caused by Excessive Passport Stamping at Uzbek-Tajik Border
- Shanghai Cooperation Organization (SCO) to Endorse Anti-Drug Trafficking Agreement
- President Shevardnadze Denies Involvement of Georgian Specialists in Iranian Nuclear Project
- Russian Scientific Institute Acquires SARS Virus from Germany
- Heads of GAN, Minatom Acknowledge Nuclear Materials Leaks

International Developments ............... 17
- Cesium-137 Seized in Thailand
- Ingredients for the Deadly Gas Sarin Commercially Available in Britain
- Japanese Firm Attempts to Export Banned Goods to North Korea
- Chronology Details WMD Events of 2003

Workshops and Conferences ............... 20
- Kazakhstan Hosts Seminar on Export Control Lists
- IAEA Seminar on the Strengthened Safeguard System Held in Tashkent, Uzbekistan
- Export Control Meeting Held in Crimea
Recent Developments in the NIS

Supreme Military Institute of Customs Established in Uzbekistan

According to a May 27, 2003 report from UzA (Uzbekistan National News Agency), the Supreme Military Customs Institute of the State Customs Committee of the Republic of Uzbekistan has been established as part of the Customs Department of the Academy of Taxation and Customs Bodies. The Academy is subordinate to the State Committee for Taxation and the Customs College under the State Customs Committee.[1]

According to Decree No. 229 of the Uzbekistani Cabinet of Ministers of May 22, 2003 On Further Improvement of the Training System for Personnel of the State Customs Committee of the Republic of Uzbekistan, the Institute will provide professional training to customs officers. In addition, the Institute will conduct research in the field of customs, and develop recommendations on improving work methods and procedures. There are also plans to collaborate with similar educational institutions of foreign countries.[2]

The Institute will run a four-year Bachelor of Arts and a two-year Master of Arts program. The time students spend in the Supreme Military Institute of Customs will be counted towards their term of service in customs bodies. Colonel Sharakhmedov has been appointed as the first director of the Institute by the chairman of the State Customs Committee upon the agreement of the President of Uzbekistan.[3]

Approximately 125 students will be admitted to the Bachelor of Arts program of the Institute in the 2003-2004 academic year. Classes will start on September 1, 2003.

Editor’s Note: The Supreme Military Institute of Customs will provide students with higher education while the Customs College provides specialized secondary education.


Russia Opens New Checkpoint on Border with Azerbaijan

On May 17, 2003, Russia opened the Yarag-Kazmal checkpoint on its border between the Russian Republic of Dagestan and Azerbaijan. The checkpoint is an 11.5 hectare complex located near a bridge crossing the Samur River, and represents an investment of 250 million rubles ($8.24 million as of June 30, 2003) approved by the Russian State Duma in 1996.[1,2] In the past, the area was used by groups for criminal cross-border activities. The new checkpoint will permit a flow of 500 vehicles per day – 300 cargo trucks, 180 automobiles, and 20 buses, as well as 1,000 passengers and pedestrians. Officials expect that the new checkpoint will promote the development of trade relations between Russia and the Caucasian states while simultaneously facilitating the activities of customs officials, border guards, and other enforcement agencies.[1]


GUUAM, U.S. To Cooperate in Anti-Terrorism and Border Security Operations

On May 24, 2003, at the third meeting of the Council of Ministers of Foreign Affairs of GUUAM Countries in Tblisi, Georgia, the GUUAM members – Georgia, Ukraine, Uzbekistan, Azerbaijan, and Moldova – and their strategic partner, the United States, continued their third year of discussions regarding their common goals of fighting terrorism and transnational crime, enhancing border security and customs control, and encouraging trade.[1,2]
One of the programs aiming to facilitate these goals is the GUUAM-U.S. Framework Program, which seeks to create multilateral projects.[1] Under this program, the partners agreed to create a “Virtual Center,” intended to combat terrorism, drug trafficking, money laundering, and other cross-border crimes by sharing information on criminal activities and law enforcement through a database called the Interstate Information Processing System (IIPS).[1,3] The United States will provide funding for up to 90 days for a liaison officer from each of the five GUUAM states to collaboratively draft an implementation program for the Virtual Center and IIPS. In addition, funding will be provided for two representatives from each state to work with U.S. experts on facilitating trade and transport among the GUUAM states. An agreement establishing the Virtual Center and IIPS was signed by representatives from Azerbaijan, Georgia, Moldova, and Ukraine at the GUUAM Presidential Summit in Yalta on July 3-4, 2003. Uzbekistan, which has suspended its participation in GUUAM activities since June 2002, did not sign the agreement, and only signed two of the seven documents at the conference, on cooperation in trade and transportation, and customs affairs.[4,5] Creation of the Center will begin on September 1, 2003 in Kiev and Baku.[6]

**Kazakhstan’s Lower House of Parliament Approves Draft Amendments to Export Control Law**

On June 18, 2003, a plenary meeting of the Kazakhstani Majilis (lower house of parliament) approved a draft bill On Amendments to the Law of the Republic of Kazakhstan On Export Control.[1] The bill, which was introduced to parliament by the Ministry of Industry and Trade in May 2003, proposes the removal of Paragraph 9, Article 5, from the existing law On Export Control.[3] The explanatory note to the bill cited a number of inconsistencies in the licensing of exports. Paragraph 9, Article 5 of the export control law states that permits for export, import, and transit of goods subject to export control are issued by the government. At the same time, Paragraph 6, Article 5-1 of the same law delegates licensing of export and import operations on such goods to a specially designated export control authority. This means that exporters and importers of controlled goods must first obtain a permit from the government and then seek a license from the export control authority. Also, Paragraph 11 of Article 5-1 creates an overlap in functions between the designated export control authority and the government, as it tasks the export control authority with issuing transit permits for controlled goods in accordance with the existing government classification.[2]

In view of these deficiencies, the bill proposes the removal of Paragraph 9, Article 5, from the export control law. The designated export control authority will issue permits for export, import, and transit operations (Paragraphs 5 and 6, Article 5-1 and Paragraph 11, Article 5-1). Currently, the designated authority is the Ministry of Industry and Trade of Kazakhstan.

**Editor’s Note: Kazakhstan passed the law** On Export Control of Weapons, Military Technology, and Dual-Use Goods of the Republic of Kazakhstan on June 18, 1996. The law On Amendments and Additions to the Law on Export Control of the Republic of Kazakhstan came into effect on November 24, 2000.[3] The 2003 and earlier amendments suggest that there is a consistent effort to improve the legal framework underpinning the export control system in Kazakhstan.


---

**NIS Export Control Observer, July 2003**
Ukraine Introduces Internal Compliance Program Certification for Industrial Concerns

Article 14 of the newly adopted Law of Ukraine On State Control Over International Transfers of Military and Dual-Use Goods states that exporters of military goods or those who apply for general or open licenses must have internal compliance programs (ICP). The law also provides for establishing a mechanism for government certification of the ICPs.

To implement the law, the State Service on Export Control (SSEC) has developed the following definitions and mechanisms for certifying ICPs:

- An ICP is a set of organizational, legal, and informational measures carried out by exporters to comply with export control requirements;
- The purpose of ICP certification is to ensure an exporter’s ability to comply with export control requirements;
- To apply for ICP certification, exporters must submit the following documents to the SSEC:
  - a request for certification;
  - a copy of the certificate acknowledging that the company is registered at the SSEC as an exporter of controlled goods;
  - a copy of the special SSEC permit to export goods containing state secrets, or a statement regarding the absence of such permission;
  - a copy of the company order to establish an ICP department and assign a head of the department;
  - a copy of the company regulation specifying operation of the ICP department;
  - confirmation of the creation of databases on: a) regulations; b) commodity classification; c) contracts involving export or import of controlled goods; d) license applications; e) reports on used licenses;
  - a statement, signed by the company’s president, containing the following undertakings: a) to comply with export control requirements while carrying out transfers of controlled goods; b) not to carry out transfers of goods in violation of Ukraine’s domestic or international obligations; c) not to transfer goods, even if they are not on control lists, without SSEC license if there is credible information indicating the importer’s intention to use these goods for manufacturing weapons of mass destruction (WMD); d) not to sign trade contracts if there is credible information indicating the importer’s intention to use imported goods to manufacture WMD; e) to stop implementing the contract if there is credible information suggesting that the end-use or end-user of the exported goods will be other than those stated in the original contract; f) to report to the SSEC in a timely manner on actual use of issued licenses.

For the purpose of certifying ICPs, the SSEC will create a Commission on State Certification of ICPs that will consist of representatives from government agencies. The members of the Commission will be able to make on-site visits to inspect ICPs. The Commission must grant or deny certification within 45 days of receiving a complete set of application documents. Certification is valid for three years and can be renewed provided the renewal application is submitted to the SSEC no later than three months before the certificate expiration date, with the following documents:

- a statement, signed by the company’s president (see above);
- a report on how the ICP is functioning;
- a notification stating that the original application documents remain unchanged.

The SSEC may deny an ICP Certificate on the following grounds:

- inclusion of incorrect data in application materials;
- numerous violations of export control regulations;
- decision by the Commission on State Certification of ICPs after an on-site visit.

The ICP Certificate may be revoked on the following grounds:

- at the request of the exporter;
International Supplier Regimes

Australia Group Expands List of Controlled Pathogens

The Australia Group (AG) — an informal network of countries that coordinate their national export controls on dual-use items that could be used to create chemical or biological weapons (CBW) — agreed at its plenary meeting of June 2-5, 2003, held in Paris, to further strengthen export controls on CBW-relevant goods and technologies.[1]

First, the Group added 14 human pathogens to its Biological Control List. The human pathogens include two toxin-producing strains of bacteria, six highly lethal and incurable viruses requiring maximum biocontainment at Biosafety Level 4 (BSL-4), and six somewhat less dangerous viruses requiring high containment (BSL-3). The AG believes that all of the added pathogens could potentially be made into lethal biological weapons.[2]

The Group also agreed to a cooperative program of action to engage countries in the Asia-Pacific region on CBW-related export control issues. Under this program, participating AG members will provide information and practical assistance to non-members. The assistance will likely involve visits by small teams of experts from interested AG countries and will focus on technical discussions and exchanges on best practices.[3]

AG members also approved a new guide on best practices in the area of enforcement that is designed to assist government officials in detecting, identifying, and preventing illicit transfers of items controlled by the Australia Group.

Finally, AG members agreed to new measures designed to improve transparency and information-sharing. These new measures include mandatory sharing of information on the efforts of member countries to implement AG-related controls, including the implementation of changes in the chemical and biological control lists.[4]


Kazakhstan May Join MTCR

On June 3, 2003, Mariusz Handzlik, the Chairman of the Missile Technology Control Regime (MTCR), met with representatives of the Kazakhstani government in Almaty while visiting Kazakhstan for the 7th Regional Forum on Export Controls. In a report on Handzlik’s visit, Kazakh Television announced that Kazakhstan may join the Missile Technology Control Regime (MTCR) very soon, becoming the third CIS country after Russia and Ukraine to join the Regime.[1,2] According to Handzlik, the decision to include Kazakhstan in the MTCR must be agreed upon by all member states and will be considered at the next MTCR Plenary Meeting to be held September 22-26, 2003 in Buenos Aires, Argentina.[1,2]


MTCR Chairman Ambassador Mariusz Handzlik Makes His First Official Visit to Belarus

On May 15-16, 2003, Chairman of the Missile Technology Control Regime (MTCR) Ambassador Mariusz Handzlik of Poland visited the Republic of Belarus.[1,2,3] This was the first official visit of the head of the...
MTCR to Belarus. During his meeting with Belarusian government officials, Ambassador Handzlik invited the government of Belarus to consider the possibility of joining the MTCR.[2,3] In the course of the discussions the Belarusian side reaffirmed its commitment to the main goals and principles of nonproliferation of weapons of mass destruction, related technologies, and means of their delivery.[3] Both sides agreed to broaden the dialogue in the field of nonproliferation and export control of missiles and missile technologies.[3] Ambassador Handzlik emphasized that he held only preliminary discussions with the Belarusian side and that he did not expect to receive definite answers regarding the possible ascension of Belarus to the MTCR.[2,3]

Editor’s Note: In the late 1990s, Belarus allegedly exported to China vehicles for launching solid-fuel long-range missiles.[4] It has also participated with Russia in the modernization of the Pechora-2 anti-aircraft missile system.[5]


International Export Control and WMD Security Assistance Programs

United States Export Control Initiatives

The U.S. government has launched several programs to support Newly Independent States’ (NIS) efforts to develop and reinforce their export control systems. This article provides a brief description of a select list of U.S. sponsored programs in the NIS, listed by order of creation.

Nonproliferation and Disarmament Fund (NDF): The NDF entered into operation on April 1, 1994. The program is designed to provide a rapid response to unanticipated or unusually difficult proliferation challenges and opportunities to prevent the spread of and to destroy existing weapons of mass destruction (WMD), delivery systems, and materials, as well as limiting the spread of advanced conventional weapons and delivery systems. NDF has a 2003 budget of $15 million, and has requested funding of $35 million in the 2004 budget. Part of the proposed increase in funding is to establish a Dangerous Materials Initiative (DMI) to assist other countries in establishing control and accounting systems to secure radioactive materials, pathogens, and precursor materials.[1] The NDF homepage can be accessed at http://www.ndf.org.

International Counterproliferation Program (ICP): Part of the Defense Threat Reduction Agency (DTRA) in the U.S. Department of Defense, the ICP was created in 1997 and works in collaboration with the U.S. Bureau of Customs and Border Protection and Federal Bureau of Investigation to train and equip law enforcement and border control authorities in order to counter the threat of proliferation of WMD materials and technologies across borders.[2] With an annual budget of approximately $9 million, ICP has trained over 2,200 individuals in 19 countries in the former Soviet Union and Eastern Europe.[2,3] The ICP homepage can be accessed at http://www.dtra.mil/os/icp/os_icp.html.

Second Line of Defense: The Second Line of Defense (SLD) program, which began in 1998, is part of the National Nuclear Security Administration at the Department of Energy. SLD focuses on preventing illicit trafficking of nuclear and other radioactive materials through major railways, airports, seaports, and other state entry and exit points in Russia. In 2002, SLD began expanding its operations into Kazakhstan and Ukraine. Discussions have also taken place with the Baltic States over possible expansion of the program into that region. SLD installs and maintains radiation detection equipment, including hand held portal
monitors, and provides training to officials in the use of the equipment. SLD is also responsible for the worldwide maintenance of portal monitors and X-ray vans provided through assistance programs by the U.S. Department of State.[4] SLD is also closely working with the Bureau of Customs and Border Protection on the Container Security Initiative (CSI) Program. More information on the SLD Program can be found at http://www.nti.org/e_research/cnwm/interdicting/second.asp.

The Export Control and Related Border Security Assistance Program (EXBS): Originally known as the Export Control Assistance program when it first received funding from Congress in 1998, the program was renamed the Export Control and Related Border Security Assistance Program in the fall of 2000.[5] EXBS is directed and funded by the Office of Export Control Cooperation of the Bureau of Nonproliferation in the State Department (NP/ECC), and draws on the expertise of other U.S. agencies, including the U.S. Bureau of Customs and Border Protection, Department of Commerce, Department of Energy, and the U.S. Coast Guard.[7]

EXBS operates in over 30 countries, and submitted a budget proposal of $40 million for 2004.[6,1] While EXBS activities were originally focused on countries that were considered possible sources of WMD technologies in the former Soviet Union, these activities have expanded to countries that are considered possible smuggling routes in Eastern and Central Europe, the Balkans, Central Asia, the Caucasus, as well as countries in South Asia and major shipment centers in the Mediterranean, Middle East, and Southeast Asia.[7]

EXBS helps countries improve their ability to prevent and interdict shipments of dangerous items and technologies by providing practical assistance to individual countries. This assistance includes helping to create new export control laws for countries in the Former Soviet Union, providing Central Asian customs and border guard agencies with hands-on training and equipment, providing Malta with X-ray equipment for screening cargo at ports, and providing software and training to Russian industry to help it comply with Russia’s export control regime.[6,7] The program also organizes the International Conference on Export Controls, a series of annual international conferences and forums on export controls and enforcement, and sponsors a website (http://www.exportcontrol.org) providing information on proceedings and measures adopted at the conferences.

Container Security Initiative (CSI): Launched in January 2002, the CSI is a new effort under the Department of Homeland Security, Bureau of Customs and Border Protection (CBP), developed in the aftermath of the September 11, 2001 terrorist attacks. CSI operations consist of four core elements: identifying and targeting high-risk shipping containers, pre-screening high-risk containers before they depart for U.S. ports, using detection technology to pre-screen high-risk containers quickly, and implementing smarter, tamper-evident containers. Under CSI, CBP personnel work with host nation counterparts in ports to secure containerized shipping from terrorists. Eighteen of the top 20 international ports – which are responsible for two-thirds of the containers shipped to the United States – have signed onto CSI. These ports are Hong Kong, Shanghai, Singapore, Rotterdam, Pusan, Bremerhaven, Tokyo, Genoa, Yantian, Antwerp, Nagoya, Le Havre, Hamburg, La Spezia, Felixtowe, Algeciras, Kobe, and Yokohama. The program is also being expanded to include additional important ports that are not among the top 20, such as Gothenburg, Sweden, as well as Klang and Tanjung Pelepas in Malaysia.[8] The CSI homepage can be accessed at http://www.customs.ustreas.gov/xp/cgov/import/cargo_control/csi/.

Transshipment Country Export Control Initiative (TECI): Operating under the Bureau of Industry and Security, TECI was launched by the Department of Commerce in fall 2002 in order to strengthen trade controls and export control systems of countries or territories that contain global transshipment hubs, such as Taiwan, Singapore, and the United Arab Emirates. As part of a two-pronged approach, TECI works with both governments and private industries to prevent illicit shipments of goods and technologies. TECI also coordinates with other U.S. government programs, such as EXBS and the CSI initiative.[9] The TECI homepage can be viewed at http://www.bis.doc.gov/ComplianceAndEnforcement/ExecutiveSummary.html.
**WMD Proliferation Prevention Initiative (PPI):** A new program established in 2003 by the Department of Defense, the WMD PPI aims to enhance NIS countries’ abilities to prevent illicit trafficking in WMD and related materials.[10] The program has a budget of $40 million for FY 2003 and will concentrate on providing support to secure land, sea, and air borders, increase domestic security, enhance legal and regulatory systems, personnel training, and boost interagency and international communication.[11] More information on the WMD PPI program can be found at http://www.nti.org/e_research/cnwm/interdicting/wmd.asp.


**U.S. EXBS Program Provides More Assistance to Tajikistani Border Guards and Customs Officers under the Auspices of Export Control-Border Security (EXBS) Program**

On May 12-14, 2003, the U.S. Embassy in Tajikistan provided $670,000 worth of new equipment to the State Border Protection Committee and the Customs Department of the Ministry of State Revenues and Tax Collection of Tajikistan.[1,2,3] U.S. assistance to the State Border Protection Committee included 2,500 sets of military uniforms, eight short wave (SW) repeater stations, 79 high frequency (HF) antennae masts, and two Customs Interdiction Tool Kits (CIT Kits).[1] The Tajikistani Customs Department received 28 HF antennae masts and five CIT Kits.[1] The U.S. Customs Service will dispatch three customs experts to Tajikistan to train Tajikistani border guards and customs officials on the use of the CIT Kits.[1] According to a press release issued by the U.S. Embassy in Tajikistan, the U.S. government has provided a total of $1,700,000 of EXBS assistance to Tajikistan since June 2002.[1,2,3]

Editor’s Note: A repeater station listens for a signal on one frequency (the input frequency) and retransmits, or “repeats” it on another frequency known as the output. Repeater stations are located on top of tall buildings or mountains where the "radio horizon" is much greater than from the ground. CIT Kits consist of tools including fiber optic scopes and density meters that will enable Tajikistani border guards and customs officials to significantly increase the quality of inspection of vehicles, trucks, and cargo that cross the borders of Tajikistan.[1]

Uzbekistan to Receive Aid to Restore Termez-Hayraton Checkpoint

In response to the capture of Mazar-i-Sharif, Afghanistan, by the Taliban in 1997, Uzbekistan closed the Druzhba (Friendship) Bridge over the Amu Darya River, which forms the border between Uzbekistan and Afghanistan. The border and the Termez-Hayraton checkpoint, named after the nearest cities in Uzbekistan and Afghanistan, respectively, remained closed until November 2001, when humanitarian aid began to flow across the bridge into Afghanistan following the fall of the Taliban. Soon after, in February 2002, Druzhba Bridge was reopened to commercial traffic.[1] With increasing cross-border traffic, it has become apparent that current border facilities are inadequate. Last year alone, over 72 tons of drugs were seized by customs officials; meanwhile total opium production in Afghanistan has been estimated at 3,400 tons.[2]

Recognizing the need for improvements in security along the Afghan-Uzbek border, the UN Office on Drugs and Crime (UNODC) initiated a training program in 2002 for border personnel, called the “Friendship Across Borders” initiative. Through this program, Uzbekistani border guards and customs officials received training on humanitarian aid, migration management, human rights, and prevention of drug, arms, and valuable item smuggling.[1] The training program for the officers was completed during the week of November 14, 2002, exactly one year after the reopening of the border to humanitarian aid shipments.[1]

During a meeting of the Uzbekistani State Customs Committee on April 30, 2003, UNODC and Uzbekistani officials signed documents approving a project called “Immediate Assistance to Uzbekistan for the Resumption of Activities at the Termez-Hayraton Checkpoint.”[1,3] Under the project, sponsored by several regional and international donors with a budget of $2 million, Uzbekistani officials will receive equipment, such as vehicle scales, endoscopes, computers, and communications equipment, as well as training in the use of the equipment and on coordinating activities with other law enforcement officials.[1,3]


Embargoes and Sanctions Regimes

U.S. Imposes Sanctions on Chinese Norinco Conglomerate over Exports to Iran

On May 23, 2003, the U.S. State Department announced the imposition of sanctions on China’s state-owned North China Industries Corporation (Norinco) conglomerate and its subsidiaries, for supplying missile-related technology to Shahid Hemmat Industrial Group. The sanctions were imposed under Executive Order 12938 of November 14, 1994, as amended by Executive Order 13094 of July 28, 1998.[1] Shahid Hemmat Industrial Group is an Iranian missile manufacturer believed to be involved in the development of Iran’s Shahab-3 intermediate-range missile.[2,3] The sanctions, which took effect on May 9, 2003 and will be maintained for two years, ban procurement of Norinco products by U.S. government agencies, prohibit any form of assistance by the U.S. government, such as services or funds, and also prevent any imports of the company’s goods into the United States.[3] Norinco has over 300 subsidiaries, including factories, research institutes, and trading companies in China and abroad. The company exports a multitude of goods to the United States, including toys, weapons, chemicals, construction materials, and optical goods, worth over $100 million in 2002 alone.[4,5,6] The State Department has not specified what materials Norinco supplied to the Iranian company, only that it had engaged in “missile technology proliferation activities.”[3] It has been suggested that there was a series of transfers of dual-use materials, such as high-strength maraging steel (a very durable form of steel, which has a low carbon and high nickel content, used in construction of gas centrifuge rotors), between Norinco and Shahid Hemmat.[7,8]

China is not a formal signatory to the 33-nation Missile Technology Control Regime (MTCR). However, China agreed in 1991 to abide by the MTCR’s original 1987 Guidelines and Parameters. In 1994, 1997, and 2000 China further clarified the nature of its adherence to the MTCR and subsequently published, in August 2002, new export control regulations and an expanded control list of missile technologies similar to...
the MTCR’s list of controlled items. Nevertheless, discrepancies still remain between China’s view of missile export controls and those of key MTCR signatories, most notably, the United States. While the United States has applied sanctions before on Chinese companies and individuals, Norinco is the largest to have sanctions levied against it. In addition, the announcement of sanctions was accompanied by a warning to the Chinese government, accusing China of negligence in its enforcement and implementation of export controls.[9] This is the first time that sanctions against a Chinese entity have been accompanied by such an accusation.


Illicit Trafficking

Stolen Europium Found in Kyrgyzstan

As reported in the February issue of the NIS Export Control Observer, 23 boxes containing europium oxide and 43 boxes of silicon wafers were stolen from a warehouse of the Kyrgyz Chemical Metallurgical Plant in Kyrgyzstan in January 2003.[1] In the second half of May 2003, Kyrgyzstani law enforcement authorities arrested three individuals suspected of carrying out the theft: Zh. Chokchonov, a 37-year old resident of the village of Orlovka; M. Tynaliyev, a 41-year old resident of the village of Kyzyl-Suu; and K. Abdakhanmanov, a 38-year old resident of the village of Progress.[2] The three are members of an organized group that has allegedly engaged in thefts of rare-earth metals.[3] They are charged with violating Article 168 of the Criminal Code of the Kyrgyz Republic, which provides for imprisonment from six to twelve years and confiscation of property.[2,4] In the course of their investigation, Kyrgyzstani authorities established that the perpetrators divided the stolen silicon wafers and europium oxide into several parts, which were then stored in different locations.[3] At present, all stolen silicon is accounted for. However, only about 100 kg of more than 400 kg of stolen europium oxide has been recovered.[2]

Editor’s note: Europium metal for commercial use is not radioactive and cannot be used as an explosive. It is used as a neutron absorber in the production of nuclear equipment, such as control rods for nuclear reactors.[6] It is also used in steel production, optics, X-ray equipment, and color television screens. Although all but two of the more than a dozen isotopes of europium are radioactive, most of the radioactive europium isotopes have relatively short half-lives – less than a few months; therefore, they would not be useful in a radiological dispersal device or “dirty bomb.” Some of these radioactive europium isotopes are typically used as tracer material in chemical reactions, as well as for medical diagnoses and treatment of some forms of cancer. The four europium radioactive isotopes that are long-lived, with half-lives ranging from 5 to 34 years, pose external and internal health hazards; however, these isotopes are rare in occurrence and mainly present a health concern at nuclear waste storage locations, such as the Hanford site in the United States.

Two Incidents of Pathogen Smuggling Reported

Evidence of the growing risks of pathogen smuggling was highlighted at two recent international conferences. During a presentation at the Seventh Regional Forum on Export Control and Nonproliferation for Central Asian Countries and the Caucasus, held in Almaty, Kazakhstan, June 2-4, 2003, a representative of a U.S. government agency disclosed that a case of illegal export of pathogens took place recently in the United States. According to the official, in 2000, at the U.S.-Canadian border, U.S. Customs officers stopped a shipment that contained a pathogenic strain of *E. coli*, equipment to grow the bacteria, and a manual on how to operate the equipment. The shipment was intended to transit the United States en route to a foreign destination (not disclosed by the speaker). U.S. customs officers identified several irregularities in the shipping documents, and further investigation revealed that the recipient company did not exist. After consultations with a scientist from the U.S. Centers for Disease Control and Prevention, customs officials determined that the shipment could be used for malevolent purposes. [Editor’s note: A few liters of *E. coli* bacteria put into a chlorinated, urban water supply would be extensively diluted and probably killed by the chlorine. However, large-scale food contamination might be possible under certain scenarios, like the contamination of meat or bottled drinks at a processing plant.] U.S. Customs seized the shipment and launched a full investigation. The investigation has been completed, but the only details the official chose to disclose were those related to the originating company and the fate of the strains. The shipment, which originated in Canada, was made by a Canadian company, which has a U.S. affiliate, to an undisclosed country. The *E. coli* strains were seized and later died, due to improper storage at the border.

A second incident was disclosed during a Biological Weapons Nonproliferation Training seminar organized by the Monterey Institute’s Center for Nonproliferation Studies and held on May 12-14, 2003, in Almaty, Kazakhstan. According to the speaker, who wished to remain anonymous, in 2002, an individual transporting biological materials in a package specially labeled for that purpose was stopped at the border in Crimea, Ukraine. The package’s special label attracted the attention of customs officials, who decided to inspect it. When they opened it, they discovered that the package contained several ampoules marked “Ebola,” one of which was damaged. This discovery generated a panic at the border, as no procedure was in place at that time to manage a bio-hazardous event. The officials eventually alerted Ukraine’s Special Services, who seized the package and launched an investigation. The materials were sent to a Crimean institute for analysis, where it was discovered that they were non-infectious and non-virulent.[1] Details regarding the source of the material and the intended destination were not revealed.

Although the second incident turned out to be a false alarm, these two events demonstrate that the interdiction of BW trafficking relies on the professional instinct of customs officials. The two incidents also underscore the importance of training customs officials to recognize and intercept biological material crossing borders, and to develop appropriate alert and response mechanisms.


Two Radioactive Smuggling Cases Occur in Georgia within Weeks

In the past two months, Georgian authorities have foiled two attempts to smuggle radioactive materials into and out of the country. The first episode occurred in late May. On May 31, 2003, while conducting patrols in downtown Tbilisi after the escape of inmates from a local prison, officers of the Georgian Ministry of Internal Affairs criminal investigation department found three metal boxes containing dangerous material in the trunk of a taxicab en route to Tbilisi’s central railway station. Two of the boxes contained Cesium-137 and Strontium-90, two potent radioactive substances.[1,2] The third container held a dark brown liquid that was later identified as mustard agent.[3,4]

The seized materials were transported to the former nuclear reactor facility at Mtskheta, near Tbilisi.[1] Analysis revealed that the radioactivity level of the Strontium-90 was about 500 microroentgens per hour, which exceeds the legal maximum of 30 microroentgens per hour.[1] However, according to Georgian Environment Minister, Nino Chkhobadze, no environmental contamination resulted from this incident.[4] Strontium-90 and Cesium-137 are byproducts of nuclear fission and are the most likely ingredients for a radiological dispersal device (RDD), or a “dirty bomb,” which combines conventional explosives with radioactive materials with the purpose of spreading radioactivity across populated areas to cause panic and
infect economic damage. Mustard agent, often referred to as a “gas,” is in fact a persistent liquid with a strong odor of garlic. Skin exposure results in painful chemical burns and fluid-filled blisters after a delay of one to six hours. Mustard gas can also cause temporary or permanent blindness and, if inhaled, severe and sometimes fatal lung damage. In the great majority of cases, however, mustard exposure results in injury (including a number of chronic illnesses) rather than death.

Even though the seizure of the containers from the Tbilisi taxi and the first arrest occurred on May 31, 2003, the details of the investigation were made public only during a press conference held on June 16, 2003. During the press conference, the deputy head of the criminal investigation division of the Georgian Ministry of Internal Affairs, Givi Mgebrishvili, indicated that the taxi driver, Tamaz Tsatsunashvili, was unaware of the danger posed by his cargo and was released after being questioned.[1,3,6] The investigation revealed that the three boxes belonged to Tedo Mokeriya, a resident of Kobuleti, a town located in the Autonomous Republic of Adjaria, on the border with Turkey.[1,5] After his arrest, Mokeriya stated that he was en route to Kobuleti to deliver the boxes to his father-in-law, Amiran Khakhtueishvili, but he did not know what the boxes contained.[1,5] Georgian police later arrested Khakhtueishvili, who admitted that he intended to sell the radioactive material in Turkey.[1,5] Both Tedo Mokeriya and Amiran Khakhtueishvili were released on condition that they do not leave their places of residence.[1] A full criminal investigation is under way and the suspects were charged with illegal storage and transportation of radioactive substances.[1,7]

In a similar case, on June 27, 2003, an Armenian citizen was detained at the Armenian-Georgian border, while trying to smuggle containers of radioactive powder in the trunk of his car.[8,9] According to the Armenian news agency Arminfo, the powder was purchased in Vladikavkaz, the capital of North Ossetia-Alania, Russia. [8] Although as of late July, the material had not been identified, Georgian Environment Minister Nino Chkhobadze speculated that it might be uranium.[8,9] It is not known why the Armenian citizen was bringing the material into Georgia, or what the ultimate destination of the material was.


Summaries from the NIS Press

Tensions Caused by Excessive Passport Stamping at Uzbekistani-Tajikistani Border

A May 23, 2003 article published in The Messenger, an English-language newspaper published in Tashkent, reports that Uzbekistani customs officers have been excessively stamping passports at the border with Tajikistan, thus causing tensions with border residents and shuttle traders.[1] For various reasons that analysts consider to be both political and economic, Uzbekistan has attempted to limit border crossing from neighboring countries.[1,2,3,4] Lately, in Tajikistan, this has taken the form of increased passport stamping, requiring Tajikistani nationals to renew their passports as they quickly run out of pages. Passport renewal in Tajikistan costs about six dollars, approximately the equivalent of the average monthly salary in Tajikistan ($8.30 in 2001) [5], thus leaving border residents with the dilemma of putting an end to their border trade activities, or saving their meager earnings to pay for a new passport.[1] To attract the attention of Uzbekistani authorities to the problem, customs officials of the Patar checkpoint in Tajikistan adopted similar practices vis-à-vis Uzbekistani nationals crossing the border.[1]
Border demarcation has been a bone of contention between the two countries since the Soviet period, when boundaries established between the republics placed large areas populated by ethnic Tajiks under Uzbekistani authority and vice versa.\[2,3\] The border conflict with Tajikistan took a dramatic turn in 1998, when the Uzbekistani government closed the border after a failed coup in Tajikistan by Tajikistani Colonel Makhmud Khudoiberdiyev and his rebel forces, who invaded Tajikistan's Leninabad province from the territory of Uzbekistan in November 1998. Tajikistani authorities suspected the rebels of receiving support from Uzbekistan.\[1,6\] In 2000, Uzbekistani authorities began placing landmines along the border with Tajikistan and established a visa regime (except for border residents).\[1,2,7,8\] These decisions were triggered by a series of explosions in Tashkent in February 1999, attributed to the Islamic Movement of Uzbekistan (IMU), whose members used Tajikistan as a transit country to launch their attacks on Uzbekistan.\[1,9\]

In 2002, both countries appeared to make progress in resolving their border disputes. At the third summit of the Central Asian Cooperation Organization (CACO), the presidents of Uzbekistan and Tajikistan signed an agreement finalizing the demarcation of 86% of their common border.\[4\]

**Editor’s Note:** The IMU, also known as the Islamic Party of Turkestan, is a group of Islamic militants from Uzbekistan and other Central Asian states, whose primary goal is to overthrow President Islam Karimov and establish an Islamic state in Uzbekistan.\[9,10\] For more information on this group, see the CNS terrorism database, [http://cns.miis.edu/research/wtc01/imi.htm](http://cns.miis.edu/research/wtc01/imi.htm).


**Shanghai Cooperation Organization (SCO) to Endorse Anti-Drug Trafficking Agreement**

During the third summit of the Shanghai Cooperation Organization (SCO), held in Moscow on May 28-29, 2003, the presidents of the six member-states reaffirmed their collective intention to strengthen cooperation in the fight against “illegal trafficking of drugs and narcotics and easy-to-make poisonous and chemical materials.”[1]

The SCO is a regional organization established in Shanghai on June 15, 2001 by the Russian Federation, the Republic of Kazakhstan, the Republic of Tajikistan, the Republic of Uzbekistan, the Kyrgyz Republic, and the People’s Republic of China.[2] The SCO is a successor organization to the Shanghai Five, a multilateral forum, founded in Shanghai in April 1996 by Russia, Kazakhstan, Tajikistan, Kyrgyzstan, and China to discuss and solve border issues through confidence-building measures and mutual reduction of armed forces in the border areas.[2] At the sixth summit of the Shanghai Five forum, held in Shanghai in June 2001, membership was extended to Uzbekistan and the member-states decided to transform the Shanghai Five into the Shanghai Cooperation Organization. The main purpose of the new organization is “to develop all-round partnership of the six nations through concerted efforts to carry out cooperation in the political, economic and trade, humanities and other fields to deal with new threats and challenges.”[1]

During the May 2003 meeting, presided over by current SCO Chairman Kazakhstan’s President Nursultan Nazarbayev, Tajikistani President Emomali Rahmonov emphasized that the increasing flow of drugs originating from Afghanistan necessitates the creation of a broad anti-drug coalition by the SCO member-states.[3,4,5] President Rahmonov also tied the problem of drug trafficking to the anti-terrorist struggle.[4]
The initiative was supported by the other participants, including Russian President Vladimir Putin, and was incorporated into the SCO declaration, the final document summarizing the results of the summit.[6,7] According to the declaration, “the SCO member states maintain that it is necessary, under the UN leadership, to develop a comprehensive international strategy to deal with the threat of drugs from Afghanistan.”[1] The SCO member-states are planning to contribute to this objective by signing a “relevant multilateral cooperation agreement before the end of this year.”[1]

In addition, member states agreed to facilitate efforts geared towards opening a regional anti-terrorist center in Bishkek, Kyrgyzstan, under the auspices of the SCO. The creation of the center is based on the Agreement on a Regional Anti-Terrorist Organization, adopted on June 7, 2002 at the second SCO summit in St. Petersburg.[1,3,4,5] According to President Rakhmonov, the first organizational meeting of the regional anti-terrorist center will be held in Bishkek in the fall of 2003.[5] Member states also plan to organize their first joint military exercises in Kyrgyzstan and Kazakhstan in August 2003.[3]

Member states devoted the rest of the meeting to analyzing the activities of the SCO in 2002, and addressing organizational matters. For example, the participants elected China’s Ambassador to Russia Zhang Deguang to be the first Executive Secretary of the SCO and agreed to establish the SCO Secretariat in Beijing as a permanent organization.[4,5,6,8] The member states also agreed on the procedures for drafting and executing the organization’s budget, which will be approved at the next SCO heads of states meeting, due to take place in Shanghai in the fall of 2003.[1,4,5,6] Finally, the six presidents adopted the emblem and flag of the SCO.[6] According to a senior official of the Russian Ministry of Foreign Affairs, the SCO summit in Moscow marked “the completion of the organizational stage in the building of the new regional organization.”[5] According to the final declaration of the summit, all of the permanent organizations of the SCO should become operational by January 1, 2004.[1,4]


President Shevardnadze Denies Involvement of Georgian Specialists in Iranian Nuclear Project

At a news briefing held at the State Chancellery in Tbilisi on June 2, 2003, Georgian President Eduard Shevardnadze denied that Georgian nuclear physicists are involved in the Iranian nuclear weapons program.[1,2] In a previous declaration made on January 13, 2003, President Shevardnadze stated that a group of former employees of the Sukhumi Institute of Physics and Technology (SIPT) [3] were working in Iran, raising suspicions that they might be involved in the Iranian nuclear program.[2,4,5] However, information obtained by the Georgian government through various channels, including reports provided by “Western special services,” [2] clearly indicated that the Georgian nuclear physicists are involved in “innocent work” in Iran that has nothing to do with the development of Iranian nuclear capabilities.[5,6]

With regards to the sale of SU-25 fighter planes assembled at the Tbilaviamsheni 31st Aircraft Assembly Plant to Iran, President Shevardnadze confirmed that Tbilaviamsheni sold SU-25s to Iran in the past and described those business deals as “ordinary commercial transactions.”[1,5] However, President Shevardnadze noted, “As far as I know, the factory has recently found a more profitable partner to whom it will sell SU-25 fighter aircraft, and contracts with Iran have been suspended.”[2]


NIS Export Control Observer, July 2003 14
Russian Scientific Institute Acquires SARS Virus from Germany

Russian health officials have confirmed that the Vector State Scientific Center for Virology and Biotechnology, located in Koltsovo, a small town near Novosibirsk, now possesses a control sample and live strain of the severe acute respiratory syndrome (SARS) coronavirus. Vector, best known for its role in the former Soviet biological weapons program, received the live strain of SARS on June 4, 2003, from the Institute of Medical Virology in Frankfurt, Germany, an affiliate of Johann Wolfgang Goethe University.[1,2] In addition, Hamburg’s Bernhard Nocht Institute of Tropical Medicine supplied Vector with a synthetically made, non-infectious control sample of DNA from the SARS virus containing a segment of the virus’s genetic code. The control sample will serve as a standard to check the domestic RT-PCR diagnostic test-systems developed at Vector. (PCR, or the pymerase chain reaction, is a genetic technique used to amplify the number of copies of a specific DNA segment, producing enough DNA to test for and identify a virus with very high probability.[5]) Vector also plans to send the non-infectious sample to other Russian research centers in order to establish a diagnostic routine.[3] Vector scientists will use the live strain of the SARS virus to examine the effectiveness of current antiviral medications in combating the atypical pneumonia, and to test their own diagnostic kits and, possibly, vaccines. Vector also plans to conduct fundamental research on the SARS virus, exploring its mutability and mechanism of spread.[4]

Considerable international cooperation between German scientific institutes and Vector, facilitated by the World Health Organization (WHO), expedited the pathogen transfers. On April 17, 2003, the WHO announced that the Bernhard Nocht Institute of Tropical Medicine had developed a series of primers, or short segments of the SARS virus’s DNA, enabling the use of PCR to quickly diagnose suspected SARS-positive specimens. In an agreement with the WHO, the Hamburg institute agreed to freely provide control, non-infectious components of the SARS virus to any laboratory in the world on request[3,6], or the virus itself with national governmental approval.[7] It also appears that Russian health officials took steps to accelerate Vector’s obtaining the requisite import license. In accordance with Decree of the President of the Russian Federation No. 1004 of August 8, 2001, new diseases such as SARS are automatically placed on the Russian government’s List of Human, Animal, and Plant Pathogens, Genetically Modified Microorganisms, Toxins, Equipment, and Technologies for Export Control.[8] Cross-border operations involving items appearing on the List are regulated by Resolution of the Government of the Russian Federation No. 634 of August 29, 2001, which requires the Russian importer or exporter to obtain a license from the Department of Export Control at the Ministry of Economic Development and Trade.[9] However, in the special case of an epidemiological outbreak, the Russian Minister of Health can procure an item on the List without a license. Although the process of acquiring a license reportedly takes at least a month[10], Vector received the non-infectious control sample of SARS from Hamburg on May 15, 2003, only a few days after Russia’s first reported case of atypical pneumonia. Denis Soynikov, a 25-year old man, was admitted to a hospital in Blagoveschensk on the Russian-Chinese border, in early May 2003. Soynikov was officially diagnosed with SARS on May 28, 2003 after his diagnosis was twice postponed pending additional tests.[1,11]

Non-infectious control samples pose no danger to laboratory personnel, and are usually sent through the regular mail[3], provided they are clearly labeled and sealed in packaging consisting of three layers.[12] The live strain of the SARS virus from Frankfurt qualifies as an “Infectious Substance, Affecting Humans” under UN Resolution 2814, and requires the same labeling and triple-packaging as a control sample.[12] However, according to the latest addition of the International Air Transport Association’s (IATA) Dangerous Goods Regulations, infectious substances can only be transported through the air via cargo aircraft.[13] While the details surrounding these pathogen transfers are not perfectly clear, it appears that stringent security measures were taken in transporting the virus. The Hamburg sample was securely packaged in a test-tube and special container, and shipped via commercial plane from Hamburg to
Novosibirsk. There it was placed in a briefcase and delivered to Vector from Novosibirsk’s Tolmachevo Airport in an armored truck.[1,7] According to Professor Lev Sandakhchiev, Director General of Vector, the WHO assisted Frankfurt’s Institute of Medical Virology in transporting the virus.[3] Although Vector representatives declined to provide more details on the transfer, they stated that all procedures taken on the way from the airport to Vector, and at Vector, were in compliance with international and domestic regulations.[7]

In order to develop an express diagnostic routine for SARS throughout Russia and Central Asia, Vector and the Sanitary and Epidemiology Service under the Ministry of Health of the Republic of Kazakhstan have agreed to undertake collaborative research at Vector beginning in September 2003. The Kazakhstan Sanitary and Epidemiology Service has expressed interest in having a United States delegation also participate in the SARS research, but it is not clear that Vector will agree to such a proposal.[2] Both Russia and Kazakhstan closed their borders with China in early May to prevent importations of the SARS virus. Russia reopened its major border crossing with China’s northeastern Heilongjiang Province on June 10, 2003, while Kazakhstan reopened its entire western border with China on June 26, 2003. The reopening of borders demonstrates the success of international scientific cooperation in stemming the spread of SARS in the former Soviet Union.[14]


Heads of GAN, Minatom Acknowledge Nuclear Materials Leaks

Last year, Yuriy Vishnevskiy, then head of Russia’s Nuclear Regulation Agency Gosatomnадзор (GAN), made several statements regarding theft of nuclear materials in Russia over the past decade. At a press conference on October 14, 2002, Vishnevskiy confirmed that there had been some “leakage” of nuclear materials from the country’s nuclear facilities in the past 10 years. He said there had been thefts of both weapons-grade material and low-enriched uranium used in fuel elements. He underlined, however, that the amount of weapons-grade material stolen measured in grams, while the low-enriched uranium used for fuel amounted to kilograms. Vishnevskiy noted that most of the material was taken from nuclear-fuel production facilities, and he specifically named the Machine-Building Plant in Elektrostal and the Novosibirsk Chemical Concentrate Plant as facilities from which the majority of stolen material originated. He did not, however, provide any details about particular cases or say what types of materials – highly enriched uranium (which can be used directly for nuclear weapons) or low-enriched (which is not suitable for nuclear weapons) – went missing from these two facilities.[1]

In a February 2003 press conference, Vishnevskiy noted that there had been two or three attempts to steal nuclear materials in 2002, but these involved small amounts of less than one kilogram of low-enriched

NIS Export Control Observer, July 2003 16
uranium. Vishnevsky denied that any nuclear materials in Russia “are still not accounted for.”[2] At the same time, he admitted that “it is not possible to objectively conclude that the nuclear material on hand corresponds to accounting records.” He said an initial physical inventory of nuclear materials had begun at only a limited number of facilities.[3] While speaking before the State Duma on March 5, 2003, Vishnevskiy said that Russia records no more than 10 cases of unsanctioned transfer of nuclear materials per year. At the same time, he noted that the number of safety and security violations has decreased from year to year.[4]

Aleksandr Rumyantsev, the head of Russia’s Ministry of Atomic Energy (Minatom), in an interview with the Russian newspaper *Vremya novostey* in February 2003, also acknowledged that over the past decade there had been thefts of tens of kilograms of natural uranium and tens of grams of weapons-grade material.[5] He stated that almost all of the stolen material had been recovered, including all of the weapons-grade material. While speaking before a meeting of International Physicians for the Prevention of Nuclear War in May 2003, Rumyantsev elaborated on the amount of stolen uranium and said that about 100 kilograms of non-weapons usable uranium had been stolen throughout the history of Russia’s nuclear program, about half of which has been recovered.[6]

Though Vishnevskiy and Rumyantsev generally agree on the type of thefts that have occurred over the past decade, their views on the overall security of Russia’s nuclear facilities differ significantly. Speaking before the Russian State Duma on March 5, 2003, Vishnevskiy said physical protection of Russia’s nuclear facilities was not at the level it needed to be. He said that this was largely due to the fact that a government program to secure radioactive and nuclear materials had received only 10-15% of promised funding. He said the program is to be implemented over six years, but that Russia cannot wait that long. Some 7,000 Russian enterprises and facilities involved in the management and handling of nuclear and radioactive materials are guarded by facilities’ or agencies’ own security services. Many of these guard units are made up of pensioners, most of whom are unarmed.[7] Rumyantsev, in contrast, declared that Russia’s nuclear security is “satisfactory.” He recalled that throughout the history of the country’s nuclear weapons program there had never been any “irregularities” in the handling of nuclear munitions, including during transport. He underscored that Minatom applies the same safety and security principles to nuclear energy production, as well as the transport of spent nuclear fuel.[8]


**International Developments**

**Cesium-137 Seized in Thailand**

An eight-month old U.S. – Thailand operation culminated on June 13, 2003, with the arrest of an individual in possession of radioactive cesium-137 – a substance that could fuel a radiological dispersal device, more commonly known as a “dirty bomb.”[1] Royal Thai Police arrested Narong Penanam, a 44 year-old elementary school principal from Thailand’s Surin province, in the parking lot of the Royal Pacific Hotel in Bangkok while allegedly in the act of selling the cesium.[2] The sale was a set-up, jointly organized by the Royal Thai Police and the U.S. Bureau of Immigration and Customs Enforcement, the investigative arm of the U.S. Department of Homeland Security.[3]

Although both U.S. and Thai authorities have confirmed that Narong Penanam thought he was meeting with a potential client in what appears to be the last of a series of orchestrated contacts, a few other major details remain unclear. For instance, the exact quantity of seized cesium involved in the transaction has yet
to be confirmed by the authorities. Initially, press reports indicated that a total of 30 kilograms of cesium had been seized.[2] More recent reporting speculates that the actual amount is probably less than one gram with a radioactivity content of about 75 milllicuries [4], which is below the threshold of security concern now being considered by the International Atomic Energy Agency and the U.S. Nuclear Regulatory Commission.[5] Thirty kilograms of cesium-137 would contain some 2.5 million curies – a level comparable to that of all the radioactive cesium released during the 1986 Chernobyl nuclear power plant accident. A person standing one meter away from 2.5 million curies of unshielded cesium would receive a lethal dose of ionizing radiation in less than a minute. Safely shielding this much radioactivity would require more than 30 kilograms of lead. The lack of any reported deaths from radiation exposure further casts doubt that 30 kilograms of radioactive cesium were seized. However, as reported by The Wall Street Journal, Thai officials also believe that the cesium seized in Bangkok is part of a larger quantity. In their opinion, there are two additional larger stashes hidden with one or more of Narong Penanam’s accomplices somewhere in Laos.[6]

Other uncertainties still riddle this case. It is not clear whether Narong Penanam was acting as a middleman on behalf of some criminal organization and if any accomplices were backing him up during the sale in Bangkok.[2,7] It also remains uncertain how Narong Penanam acquired the cesium in the first place. Narong Penanam denies any terrorist involvement and both Thai and American authorities recognize no known ties to terrorist groups.[2] His involvement appears to be financially driven and Thai police officials said the man was expecting to earn $240,000 from the cesium sale.[2] Narong Penanam declared that he received the radioactive material from a “friend” – the aide of an Air Force Marshal now deceased – and also claimed that the metal box containing the seized cesium was brought to Thailand from Russia and that it was stored for a period of time in Laos.[2,6]

In a June 18, 2003, article published in the Bangkok Post, Praphai Charensuk, the 60-year-old widow of a Thai Air Force Marshal, told Thai authorities that her late husband might have been holding the cesium at some point in early 1997. According to her, around that time the Air Force Marshal had been contacted to help examine a substance suspected of being uranium from Russia. After the Air Force Marshal’s death in 2001, Charensuk had received a call from an unknown man claiming to be in possession of the material. The individual also claimed to be planning to hand over the radioactive source to the Office of Atomic Energy for Peace (OAEP), Thailand’s nuclear regulatory agency. [8]

As for the possible intended recipients of the material, Homeland Security agents based in Bangkok believe in the possibility that terrorist organizations operating in Southeast Asia might be the most interested in acquiring a substance like cesium-137.[2]

The cesium-137 seizure in Thailand confirms that this isotope has increasingly become the object of illicit trafficking. Commonly found in medical and industrial equipment, cesium-137 has long been high on the list of security-critical isotopes. Both the IAEA and UN have recently included highly radioactive cesium-137 sources in their list of potent materials that could be used for building radiological dispersal devices.[9] The interest of smugglers in radioactive cesium is also confirmed by other recent illicit trafficking incidents. For example, a few weeks prior to the cesium seizure in Thailand, police in the Republic of Georgia discovered two metal containers filled with strontium-90 and cesium-137.[10]

Ingredients for the Deadly Gas Sarin Commercially Available in Britain

In order to demonstrate the lack of laws restricting the domestic sale of chemical weapons precursors in Great Britain, a BBC reporter – Angus Stickler – decided to acquire commercially-available ingredients to make twice the amount of sarin gas as was used in the deadly 1995 attack on Tokyo’s subway system.[1] The 1995 terrorist attack killed 12 and injured more than a thousand.

On May 30, 2003, Stickler declared that it took him three weeks to obtain the four chemicals required to produce sarin, a colorless, odorless, and highly lethal nerve agent, using information found on a website linked to Bristol University, United Kingdom. The information has since been removed from the website.[3] Stickler purchased the chemicals from two British firms – Dorset-based Molekula and Derbyshire-based Fluorochem – allegedly to do research on chemicals used in pesticide manufacture.[1,3]

Commenting on the event, the Chemical Industry Association of Britain declared that the issue is difficult to legislate because many chemical weapons precursor chemicals have legitimate industrial, commercial, or household uses.[2] British Home Office Secretary David Blunkett also stated: “It would be impractical and ineffective to ban the production and sale of substances which are used safely and legitimately in daily life.”[4]

Sources:

Japanese Firm Attempts to Export Banned Goods to North Korea

A May 8, 2003 police search of the offices of Meishin, a Tokyo-based trading company owned by a North Korean national, revealed that the company had attempted to export an oscilloscope to North Korea. The export of oscilloscopes is controlled in Japan due to their possible use in radar and submarines. Certain models can also be used in the development of high-speed centrifuges for enriching uranium for potential use in nuclear weapons. Earlier, the Japanese Ministry of Economy, Trade, and Industry (METI) had denied Meishin’s license request to export the item to Korea Daesong General Trading Corp., a North Korean company that has been identified by U.S. intelligence as being involved in weapons development.[1,2]

This is not the first time Meishin has come under scrutiny for attempted illegal exports. In April 2003, Meishin violated the Foreign Exchange and Trade Control Law for attempting to export three power supply devices to North Korea using a Thai telecommunications equipment maker as an intermediary.[3] The devices, worth a total of two million yen ($17,170 as of May 13, 2003), were transformers used to control the flow of direct electrical current and could be used either in the uranium enrichment process or to stabilize missile trajectories.[2,3,4] After an investigation by METI officials of Meishin’s offices and inquiries to the Thai firm, the devices were seized from a freighter at port in Hong Kong.[3] According to the Tokyo Police Department, the company has attempted to export three different types of controlled devices on four separate occasions since 2000.[1]

Japan’s export control system came under international criticism in 2001 after it was discovered that a DPRK spy ship that had been sunk in an exchange of fire with a Japanese Coast Guard vessel contained Japanese-made radar and other high-tech equipment.[3] Between April 2002 and April 2003, ten Japanese companies have attempted to export high-tech dual-use items to North Korea.[5] One such company, Seishin Enterprise Co., was accused of illegally selling jet mill grinding machines, which can be used to produce solid missile propellant and for milling dried biological warfare agents; the illicit sales were made to China in 1992, Iran in 1999 and 2000, and North Korea in 1994.[6,7] Seishin has also reportedly conducted deals involving jet mills and other related equipment several times in the early nineties to companies connected with the Indian military and in 1992 to an atomic energy research institute in Pakistan.[6]
As part of an effort to strengthen export controls to prevent the proliferation of WMD-related technology to North Korea, the Japanese government will attempt to integrate China and Southeast Asian countries into a regional trade control system that operates under “catch-all controls.” Such controls can be used to bar exports of goods, even if they are not itemized on national control lists, in cases when there is reason to believe they will be used by recipients in weapons of mass destruction programs.[8]


Chronology Details WMD Events of 2003

A chronology of events for January-July 2003, covering developments relating to weapons of mass destruction and efforts to limit their use and further proliferation, is now available on the Nuclear Threat Initiative's WMD411 website [http://www.nti.org/f_wmd411/f_index.html]. This chronology details events of the past six months that relate to nuclear, chemical, biological, and radiological weapons, as well as cruise missiles and ballistic missiles. Its easy-to-use format contains useful links for a more in-depth look at the issues. WMD411 is a comprehensive resource guide for those interested in efforts to prevent the spread and the use of weapons of mass destruction. It is produced by the Center for Nonproliferation Studies at the Monterey Institute of International Studies for the Nuclear Threat Initiative.

Workshops and Conferences

Kazakhstan Hosts Seminar on Export Control Lists

On June 24-26, 2003, Kazakhstan’s Ministry of Industry and Trade and the U.S. Department of Commerce (DOC) co-hosted a workshop on export control lists in Astana, Kazakhstan. The workshop was organized by Commonwealth Trading Partner, Inc. (CTP), a DOC contractor, with funding from the U.S. Department of State Bureau of Nonproliferation.

Forty-three participants, representing various Kazakhstani government agencies – including the Ministries of Foreign Affairs; Industry and Trade, Energy and Mineral Resources; Justice; and Defense; the Customs Administration; and the Committee for National Security (KNB) – as well as non-governmental organizations, private and state-owned enterprises attended the workshop.[1]

The main purpose of the workshop was to train government officials and industry representatives on issues related to the use of the European Union (EU) control list, which served as a model for the development of the national control list of Kazakhstan. Discussions concentrated on the structure of the EU model control list and the methodology for classifying goods, and also included classification simulations.[2]

The seminar generated a number of discussions, during which the participants had the opportunity to address such issues as the classification of a commodity if a manufacturer no longer exists and technical specifications are not available; the authority of the Customs Committee to detain shipments and determine whether or not they should be released; the use of Soviet-time Tariff Codes (or TNVED) and Control List codes; and the decision-making process of the Kazakhstani Ministry of Industry of Trade.[3]

IAEA Seminar on the Strengthened Safeguard System Held in Tashkent, Uzbekistan

From June 23 to 25, 2003 a seminar entitled “The Nonproliferation of Nuclear Weapons: the Strengthened Safeguards System,” was held in Tashkent. The event was sponsored by the International Atomic Energy Agency (IAEA) in cooperation with the Government of Uzbekistan. Representatives from Armenia, Azerbaijan, Georgia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan attended the seminar. Representatives from China, Japan, and the United States joined as observers.

The seminar is one in a series of meetings organized by the IAEA and regional partners in Asia, Africa, and Latin America, which aim to promote the implementation of the Additional Protocol. The Additional Protocol is an agreement with the IAEA which provides the inspection agency with supplementary authority to that provided in the state’s basic Safeguards Agreement. The added authority enables the agency to ensure not only the correctness of state declarations and information regarding its nuclear material, but also the completeness of this information. It also provides the IAEA wider authority with respect to information and access to locations in the signing state, in the interest of strengthening confidence in the safeguards system.

Discussions during the meeting addressed such issues as the IAEA safeguards system and the Central Asian Nuclear Weapon Free Zone proposal. A session on export controls organized by the Office of Export Control Policy and Cooperation of the National Nuclear Security Administration at the U.S. Department of Energy concentrated on the role of export controls in the global nonproliferation regime. IAEA representatives also made a presentation on import/export reporting under the Additional Protocol.

Time was set aside for bilateral talks between the IAEA and participating state representatives to deal with issues particular to the individual states. A final session addressed broader themes: Mr. Marat Usupov of the Ministry of Foreign Affairs of Kyrgyzstan emphasized the importance of strengthening nuclear nonproliferation and disarmament in the region, generally, and Dr. Lawrence Scheinman of the Monterey Institute of International Studies spoke on the future of the nuclear nonproliferation regime and the challenges confronting it. An issue of interest to a number of the participants was the question of whether Iran might adhere to the Additional Protocol and what the impact of Tehran deciding not to adhere might be. One participant asked whether the same transparency being demanded of Iran should also be required of Israel. The session on the nuclear free zone was constrained by the fact that negotiations were still ongoing. The addition of a session on export control, a crucial component of the nonproliferation regime, gave added meaning to the discussion on safeguards and verification.

Meeting of Export Control Technical Experts Held in Ukraine

A meeting of the Technical Experts Working Group on Nuclear Export Control was organized by the U.S. Department of Energy in Alushta, Ukraine on June 24 - 26, 2003. The meeting was the fourth in a series of Working Group meetings (1999, 2001, 2002) that has brought together government officials and experts from the United States, Kazakhstan, Russia, and Ukraine. Representatives from Georgia and Azerbaijan also attended the June meeting.

The meeting focused on the role of technical experts in establishing nuclear export control systems, and their cooperation with government agencies. Other issues discussed at the meeting included the participation of experts in the development of national legislation; support of multilateral measures on export control compliance; creation of national control lists; assistance with nuclear export licensing; support of customs operations; and assistance to exporters in creating internal control systems. The participants agreed that such meetings should continue in the future and offered recommendations for further cooperation in the field of export control.