Inside this Issue

Recent Developments
- Singapore Parliament Passes Biological Agents and Toxins Bill

Changes in Personnel
- Newly Appointed Head of Ukrainian State Customs Service Resigns amid a Major Government Reshuffle
- Head of U.S. Customs and Border Protection Robert Bonner to Retire

Illicit Trafficking
- IAEA Releases New Statistics Showing Increase in Nuclear Trafficking
- Russian Customs Prevents Illegal Export of Dual-Use Goods
- MI5 Report Reveals Information on WMD Trade
- First Hafnium Seizure in Bulgaria
- German Businessman Accused of Exporting Uranium Enrichment Parts to Pakistan

International Assistance Programs
- Kyrgyzstan Receives EXBS Technical Assistance
- Two Radar Stations Become Operational in Azerbaijan under the U.S.-Funded Caspian Guard Initiative
- Slovakia Installs X-Ray Scanner Donated by China on the Slovak-Ukrainian Border

Summaries from the Regional Press
- Tajik Authorities Call for Support to Protect Sections of the Tajik-Afghan Border

International Supplier Regimes
- The Democratic Republic of the Congo Becomes State Party to the CWC

Embargoes and Sanctions Regimes
- U.S. Citizen Convicted for Smuggling Electronic Components to China
- International Arms Trader Linked to Californian Companies Charged with Illegally Exporting Military Aircraft Components
- Washington Waives Some Restrictions on Libya Allowing U.S. Companies to Help Libya Destroy Chemical Weapons Stockpile
- Two More Arrested in Case of Nuclear Smuggling to Libya

International Developments
- CSI Update — U.S., Canada Sign Partnership; Ports of Santos and Colombo Operational

Round-Up: Incidents Involving Radioactive Material
- Radiological Material Stolen from Factory in Philippines
- Cesium-137 Capsules Stolen in Venezuela
- Radioactive Source Found in Saratov, Russia
- Kyrgyz Authorities Secure 1,000 Radioactive Sources, Continue to Search
- Ukraine Secures Missing Radioactive Material

Workshops and Conferences
- OPCW Hosts Workshop for Customs Authorities on CWC Implementation

Special Report
- South Korean Export Control Awareness on Rise but Compliance Lacking, by Dave H. Kim, Research Associate, Center for Nonproliferation Studies
Recent Developments

Singapore Parliament Passes Biological Agents and Toxins Bill

On October 18, 2005, Singapore’s parliament passed the Biological Agents and Toxins Bill (BAT). According to its preamble, the bill seeks to prohibit or otherwise regulate the possession, use, import, transshipment, transfer, and transportation of dangerous biological agents, inactivated biological agents, and toxins, in order to ensure that such materials are handled with the appropriate safety measures. The BAT also calls for related amendments to be made in Singapore’s Infectious Diseases Act.[1]

Editor’s Note: The BAT does not deal with the export of biological agents and toxins. Singapore’s export controls for these and other weapons of mass destruction—(WMD—)related items are addressed in the 2002 Strategic Goods (Control) Act (SGCA). The SGCA contains a control list of more than 50 biological agents and toxins.[2] The WMD-related control lists in the 2002 act are consistent with, though not identical to, existing international export control regimes, such as the Australia Group, the Wassenaar Arrangement, the Missile Technology Control Regime, and the Nuclear Suppliers Group.[3]

During a speech delivered to Singapore’s parliament on October 17, 2005, Dr. Balaji Sadasivan, the Senior Minister of State for Information, Communications, and the Arts and Health, pointed out that the threats posed by the SARS, avian influenza, and Nipah viruses have resulted in more laboratories doing research with dangerous biological agents. In this context, if safety lapses occur, workers in laboratories could become infected—as has already happened to researchers studying SARS in China, Taiwan, and Singapore. Dr. Sadasivan noted that these accidents highlighted the importance of biosafety and the necessity for strong legislation to ensure it.[4]

The BAT focuses on three key issues: (a) the requirements for the import or use of biological agents and toxins, (b) the duties and responsibilities of laboratory operators and those involved in the transportation of biological agents and toxins, and (c) the enforcement powers of Singapore’s Director of Medical Services (DMS).[4] The bill categorizes biological agents and toxins into five schedules. Biological agents listed in the first and second schedules, and toxins listed in the fifth schedule, have the greatest potential to cause serious illness and hence are subject to the most stringent regulatory controls. These schedules consist of 93 high-risk biological agents and five toxins in total; 37 of these biological agents and all of the toxins are identified as posing a bioterrorist risk. Biological agents listed in the third and fourth schedules have been assessed to pose a low threat to public health and therefore are not subject to stringent regulations.[4]

The BAT sets up clear provisions for the import and acquisition of pathogens and toxins. Regulations on importation are outlined in three clauses of the BAT. The first clause prohibits the importation into or transshipment through Singapore of any biological agent listed in the first or second schedules without permission from the DMS. In order to receive permission to import or transship such agents, a person or organization must have prior authorization from the DMS to handle high-risk agents. The second clause of the bill requires those permitted to import agents listed in Part II of the first schedule to notify the DMS in the event that an order is not received within 24 hours of the expected reception date. The final clause requires permit holders to ship or store agents listed on the first schedule at designated locations and in accordance with prescribed requirements.[1]

The bill prohibits the transshipment of all biological agents by regular mail or public transportation. Further, a person or entity granted a permit to transship a biological agent through Singapore must ensure that, while it remains in the country, the agent is stored at a safe and secure facility and that the storage is carried out in accordance with the conditions listed in the permit.[1]

According to Dr. Sadasivan, the bill empowers the DMS to investigate suspected lapses in biosafety procedures and to take action to correct such situations. These powers include the ability to close facilities and/or to destroy pathogen stocks. The provisions in the bill do not apply to clinical-care facilities doing research for diagnostic purposes, or to pathological labs in carrying out autopsies. Fines for violating the bill range from SG$5,000 (US$3,000) and/or imprisonment for no longer than six months, up to fines of SG$1 million (US$600,000) and/or life imprisonment, depending on the severity of the violation.[4]

The drafters of the bill took into consideration the recommendations of Singapore’s National Biosafety Committee and its Technical Working Committees. The bill also adopted the Laboratory Biosafety Manual (Third Edition) prepared by the World Health Organization (WHO) as the biosafety standard for Singapore.[5]

Changes in Personnel

Newly Appointed Head of Ukrainian State Customs Service Resigns amid a Major Government Reshuffle

On September 8, 2005, President Viktor Yushchenko of Ukraine signed Edict No. 1235/2005 dismissing Volodymyr Skomarovsky from his position of chairman of the Ukrainian State Customs Service (SCS), in accordance with Skomarovsky’s own resignation request.[1] [Editor’s Note: Skomarovsky was appointed SCS Chairman on March 4, 2005.][2] Skomarovsky was replaced by Oleksandr Yehorov on September 23, 2005, in accordance with Presidential Edict No. 1334/2005.[3] Prior to this appointment, 48-year-old Yehorov served as head of Ukraine’s State Customs Committee in 1992-1996 and as first deputy chairman of the State Customs Committee in 1996-1997. From 1997 until October 2003, he was the first deputy head of the SCS.[4,5] [Editor’s Note: In January 1997, the State Customs Committee of Ukraine was renamed State Customs Service of Ukraine.]

The announcement of Skomarovsky’s dismissal was part of a general reshuffling of the Ukrainian government that started with the decision by President Yushchenko to fire Prime Minister Yulia Tymoshenko. On September 8, 2005, citing continuous infighting among factions of cabinet members that threatened to harm national interests, Yushchenko signed Edict No. 1234/2005, which terminated Tymoshenko and disbanded the entire Cabinet of Ministers.[6,7,8]

Earlier that day, Deputy Prime Minister Mykola Tomenko had announced his resignation at a press conference, where he also accused the government of widespread corruption.[7,8] Another shockwave came from the resignation letter submitted on the same day by National Security and Defense Council of Ukraine (NSDCU) Secretary Petro Poroshenko, which was accepted in Presidential Edict No. 1231.[9] The presidential edict that dismissed the prime minister and disbanded the Cabinet of Ministers also appointed 57-year-old economist Yuri Yekhanurov acting prime minister.[6] On September 27, 2005, President Yushchenko appointed Anatoly Kinakh, formerly acting deputy prime minister, as the new NSDCU secretary (Presidential Edict No. 1379).[10]

In the context of these dramatic changes in the Ukrainian government, it should be recalled that in summer 2005 President Yushchenko harshly criticized the SCS and dismissed some high-ranking regional customs officials.[11] However, it appears that the misconduct and corruption permeated the highest levels of the Ukrainian customs administration, as demonstrated by the charges that have been leveled against Skomarovsky since his dismissal. In particular, the Security Service of Ukraine (SBU) is investigating allegations of corruption and smuggling against Skomarovsky.[12] Former SBU chief Oleksander Turchinov stated at a press conference on September 15, 2005, that the SBU had already been investigating Skomarovsky’s alleged involvement in contraband operations when the latter was appointed the SCS chair. Turchinov went on to claim that Skomarovsky was appointed despite the opposition of then- Prime Minister Yulia Tymoshenko simply because he was a protégé of then-NSDCU Secretary Petro Poroshenko.[13]


Head of U.S. Customs and Border Protection
Robert Bonner to Retire

On September 28, 2005, Robert Bonner, commissioner of the U.S. Customs and Border Protection (CBP), announced his plan to retire from public service. The precise date of his departure has not been announced, but Bonner plans to remain in his position until a successor is found.[1,2] Bonner was appointed head of the then-U.S. Customs Service in 2001 and took charge of the newly created CBP in 2003. Prior to heading the Customs Service, Bonner was U.S. Attorney for the Central District of California (1984-1989), U.S. District
Judge for the Central District of California (1989-1990), and Administrator of the U.S. Drug Enforcement Agency (1990-1993).[3]  

Editor’s Note: The CBP was created under the Department of Homeland Security (DHS) in 2003 and brought together the U.S. Customs Service and the U.S. Border Patrol, as well as parts of the U.S. Department of Agriculture’s Animal and Plant Health Inspection Service and the U.S. Immigration and Naturalization Service.  

With the pending retirement of Bonner, three key agencies within DHS are currently without a permanent head. The Director of the Federal Emergency Management Agency (FEMA) resigned in September 2005.[4] The post of DHS assistant secretary responsible for U.S. Immigration and Customs Enforcement has been vacant since July 2005 when the previous assistant secretary was named U.S. Attorney for the Southern District of New York.[5]  


Illicit Trafficking

IAEA Releases New Statistics Showing Increase in Nuclear Trafficking  

On September 27, 2005, the International Atomic Energy Agency (IAEA) released the latest statistics on nuclear trafficking that the agency gathered in its Illicit Trafficking Database (ITDB). Although the ITDB was formally established in 1995 to track down information on illicit trafficking incidents and other unauthorized activities in nuclear and other radioactive materials, the IAEA first started collecting information on nuclear trafficking in 1993. The database includes incidents that involve unauthorized acquisition, provision, possession, use, transfer, or disposal of nuclear and other radioactive material, whether intentional or unintentional, with or without crossing international borders. The database also includes unsuccessful or thwarted events and incidents involving inadvertent loss or discovery of nuclear and radioactive materials, i.e., orphaned sources. Eighty-two IAEA member states report these incidents to the agency. In addition to confirmed incidents, the agency also investigates several hundred unconfirmed cases.[1,2]  

According to the statistics recently released, for the first time since 2000, the number of reported incidents significantly increased: 121 incidents of “illicit trafficking and other unauthorized activities involving nuclear and other radioactive materials” were reported in 2004, while only 60 cases were reported in 2003.[1,3,4] This increase, however, may be partially attributed to improvements in reporting. In addition, the majority of 2003-2004 incidents did not show evidence of criminal activity.[3]  

Between 1993 and 2004, 662 incidents involving the theft or loss of nuclear and radioactive materials were confirmed. Of these incidents, 220 involved nuclear materials, the majority of which were low-grade that could not be used as fuel for nuclear weapons. Most of the nuclear material incidents were the result of criminal activity, such as theft, illegal possession, transfer, or transaction.[3] The largest number of cases reported in the database—424—involved radioactive materials, mostly in the form of radioactive sources.[3] About 50 of those incidents concerned materials classified by the IAEA as “dangerous,” or having potential to cause deterministic health effects if not properly controlled or if used for malicious purposes, such as in a radiation dispersal device, or “dirty bomb.”[4] [Editor's Note: “Deterministic health effects” is a term used by the IAEA to refer to the “radiation effect for which generally a threshold level of dose exists above which the severity of the effect is greater for a higher dose.” Radiation sickness is one example of a deterministic health effect.][5]  

Only 18 incidents in the ITDB involved trafficking in highly enriched uranium (HEU) or plutonium—fissile materials directly usable for nuclear weapons—most of which concerned very small quantities of material. Among the incidents reported since 2003, only one involved fissile material. In June 2003, Georgian border guards arrested an Armenian citizen on the Georgian-Armenian border and confiscated several boxes with radioactive material. The ITDB reported that the confiscated material was HEU in the amount of approximately 170 grams.[3] No further details regarding the enrichment level, origin, or destination of the material were provided.  

Russian Customs Prevents Illegal Export of Dual-Use Goods

On September 28, 2005, head of Russia’s Siberian Operational Customs press service Aleksandr Malik announced that customs officers in Novosibirsk prevented an attempt to illegally export 300 night-vision devices to the United States. [Editor’s Note: Siberian Operational Customs is the division of the Siberian Regional Customs Directorate headquartered in Novosibirsk, one of the seven regional customs directorates of the Russian Federal Customs Service.] As reported by Malik, “a well-known Novosibirsk company” engaged in the production of optoelectronic instruments for military and civil purposes signed a contract with an unspecified U.S. company to supply night-vision devices. According to Malik, several shipments of the devices had been sent to the United States earlier without being stopped by the customs authorities because the company had deliberately understated the technical characteristics of the high-precision items, declaring them as tourist equipment. Malik claimed that the items were dual-use goods equipped with optoelectronic transducers used by the Russian military, and if declared properly, the company would have had to obtain an export license from Russia’s Federal Technical and Export Control Service. The official said that the Novosibirsk Oblast Federal Security Service Directorate is now conducting a criminal investigation into the case, in accordance with Article 188 of the Russian Criminal Code, “Smuggling.”[1,2]

As reported later by local Novosibirsk media, the enterprise in question was the Novosibirsk Instrument-Making Plant (NPZ), and the items illegally exported were PN-14K night-vision goggles. According to Sergey Maslikov, NPZ assistant director general for export control issues, the plant won a contract from a U.S. company in April 2005 and between May and July sent six shipments of night-vision goggles to the United States. In late July, Siberian Operational Customs questioned the validity of the declared technical characteristics and seized the next shipment. Customs officials claimed that export of the night-vision goggles was subject to licensing because the sensitivity of the optoelectronic transducer exceeds 350 units (microamperes per lumen), the threshold that divides civil-use from dual-use in Russian export control regulations.

Referring to the results of two independent expert examinations conducted by the Siberian division of the Russian Academy of Sciences and the Siberian Center for Standardization and Metrology, Maslikov indicated that both studies agreed that the sensitivity of the optoelectronic transducer did not exceed 350 units and therefore their export did not require a license. However, Siberian Operational Customs sent the night-vision goggles to a third, unspecified laboratory, which found that the sensitivity of the transducer in one of the devices was higher than the permissible level. Based on the results of this last examination, customs officials initiated a criminal case, while the NPZ appealed to the Novosibirsk Oblast Prosecutor’s Office. According to Sergey Maslikov, in mid-August, the U.S. customer broke the contract, citing the delay in the shipping schedule, and other NPZ export shipments have also been halted due to the ongoing investigation. The NPZ management believes that the customs incident was initiated by the plant’s competitors in Russia.[3,4] The International Export Control Observer will provide additional information on the case as it becomes available.


MI5 Report Reveals Information on WMD Trade

The British newspaper The Guardian reported on October 8, 2005, that the UK security service MI5 compiled a report in 2003 entitled, “Companies and Organizations of Proliferation Concern.” According to reporters at The Guardian who saw the report, the MI5 document revealed names of organizations involved in the supply or trafficking of goods and technologies intended for use in the development of WMD or their delivery systems.[1]

The MI5 document—which was not released by the newspaper and is not available publicly—reportedly listed more than 360 private companies, university departments, and government organizations that have conducted proliferation-related business aimed at procuring goods and/or technologies for WMD programs in Egypt, India, Iran, Israel, Pakistan, Syria, and the United Arab Emirates, as well as for front companies in Cyprus and Malta. According to The Guardian, the only diplomatic institution on the list was the Pakistan High Commission in London, which denied the allegation.[1]

The report claimed that 114 Iranian organizations, including chemical and pharmaceutical companies, universities and medical schools, have acquired nuclear-, chemical-, biological-, or missile-related technologies. There were also 95 entities from Pakistan, 73 from India, and 11 from Israel listed as having been involved in obtaining items for WMD-related programs. Front companies in the United Arab Emirates were noted as being the hub for much of the trade. The Syrian Atomic Energy Commission and a private chemical company in Egypt were also identified in The
Guardian article as having acquired technology for use in a nuclear weapons program.[1]

While the entities listed have not specifically committed offenses under British law, the report suggests that the arms trade market is larger than is publicly known. Although The Guardian article pointed to a few of the government agencies listed in the MI5 document, the newspaper did not specifically name any of the companies mentioned in the report.[1]


First Hafnium Seizure in Bulgaria

On September 17, 2005, the Bulgarian police detained four men—three Romanians and one Bulgarian national—in connection with an attempt to smuggle 7.5 pounds (3.4 kg) of a rare earth metal—hafnium—through the border checkpoint near the town of Rousse (Ruse) on the Bulgarian-Romanian border.[1,2,3,4] [Editor’s Note: Hafnium (Hf) is a silvery grey, non-radioactive metal that is used in the control rods of nuclear reactors. Since nuclear reactors are used for both civilian and military purposes, hafnium is included as a dual-use commodity in the “List of Nuclear-Related Dual-Use Equipment, Materials, Software and Related Technology” that is controlled by the Nuclear Suppliers Group.][1,2,3,5,6,7]

Describing the incident, Bulgarian police chief Valentin Petrov told the bTV television channel that the four men were riding in a Volkswagen Golf across the bridge over the Danube River into Romania when they were detained by the Bulgarian police and customs officials. A bag with hafnium in the form of an ingot was found on the driver, a Bulgarian national.[2] A spokeswoman for the Bulgarian police later clarified that the Romanian nationals had been released after they were questioned, and the Bulgarian national admitted that the seized rare metal was his.[1,2] Hafnium is included in the list of substances that cannot be transported across the national borders of Bulgaria without a proper license.[1]

At a press conference arranged in Rousse after the seizure, Valentin Petrov told the BTA news agency that the smuggled hafnium was extremely pure (purity level of 99.999 percent).[2] He added that the Bulgarian police suspected that organized crime elements in Bulgaria might be involved in this smuggling incident.[1,2] Commenting on the hafnium seizure, Bulgarian authorities estimated that the material was of foreign origin. Marina Nizamska, the head of the accident planning department of Bulgaria’s Agency for Nuclear Regulation, noted, “The element [hafnium] cannot be isolated in Bulgaria. We definitely do not have the means.”[2] The Bulgarian police also stated that there were no facilities in Bulgaria capable of producing purified hafnium in a metal shape.[1,3]

On May 29, 1999, at the same Rousse border checkpoint, Bulgarian customs officials detained a man who was trying to smuggle across the border 10 grams of highly enriched uranium (HEU). This case was included in the IAEA Illicit Trafficking Database (ITDB).[8] [Editor’s Note: See “IAEA Releases New Statistics Showing Increase in Nuclear Incidents” on page 4 of the current issue.]

At the time of publication, no additional information on the origins of the metal or the identity of the Bulgarian citizen who attempted to smuggle it across the border has been released in the media. The International Export Control Observer will provide additional information on the case as it becomes available.


German Businessman Accused of Exporting Uranium Enrichment Parts to Pakistan

On October 27, 2005, a businessman accused of illegally exporting nuclear dual-use items to Pakistan went on trial in Germany.[1] German authorities claim that between 2002 and 2004 the businessman’s company bought and exported parts for use in uranium enrichment in violation of Germany’s Foreign Trade Law and War Weapons Control Act. Media reports indicated that the items were exported to companies tied to Pakistan’s nuclear weapons program, and in particular, the Khan Research Laboratories.[1,2]

German media identified the accused as “Rainer V.,” noting that he is head of the trading company Vacom, in the town of Pullach outside Munich.[1,2]

According to a September 26, 2005, report by the Munich-based magazine Focus, beginning in 2002, the businessman allegedly obtained vacuum pumps, “special valves,” and other items from another German firm, Pfeiffer Vacuum.[2] [Editor’s Note: Vacuum pumps are key components for uranium enrichment centrifuges.] In 2004, he also reportedly
obtained from Pfeiffer a high-frequency generator and an ion source, which are replacement parts for a mass spectrometer. The businessman was charged with exporting these items without the appropriate licenses to a number of Pakistani companies linked to Islamabad’s nuclear weapons program. The Focus report claimed that the end-user of many of these items was ultimately Khan Research Laboratories—Pakistan’s main nuclear laboratory and its primary source of fissile material for its nuclear weapons program.[2,3] The facility, which has focused heavily on uranium enrichment, was founded by Dr. A.Q. Khan and was an important part of the Pakistani scientist’s black-market nuclear suppliers network.[3]

Pfeiffer Vacuum appeared unaware of the diversion of its materials to Pakistan by Rainer V. In an interview with Focus, Pfeiffer Chairman Wolfgang Dondorf surmised that after looking at the list of items purchased by Vacom, Islamabad must have needed “new pumps and replacement parts in order to keep their uranium enrichment going. Now they have them.”[2]

The International Export Control Observer will provide additional information on the case as it becomes available.


International Assistance Programs

Kyrgyzstan Receives EXBS Technical Assistance

On September 29, 2005, the State Rescue Training Center under the Kyrgyz Ministry of Ecology and Emergency Situations received US$190,000 in technical assistance for use in border security and nonproliferation efforts from the U.S. Embassy in the Kyrgyz Republic. The assistance was granted under the U.S. Department of State’s Export Control and Related Border Security Assistance (EXBS) program. The donation included ten Russian-made UAZ jeeps that will be used for towing six previously provided all-terrain vehicles and four snowmobiles, as well as office furniture, computers, one projector, and a local area network (LAN) for information technology classes. According to a U.S. Embassy’s press release, in the future the EXBS program plans to provide equipment and training worth several million dollars to Kyrgyzstan.[1,2]


Two Radar Stations Become Operational in Azerbaijan under the U.S.-Funded Caspian Guard Initiative

In an interview given to Agence France Presse on September 21, 2005, the U.S. ambassador to Azerbaijan, Reno Harnish, provided details about the current status of U.S.-Azerbaijani border defense and maritime security assistance programs.[1] Ambassador Harnish stated that the U.S. government provided funds for the construction of two radar stations in the northern and southern parts of Azerbaijan in the framework of the Caspian Guard Initiative (CGI). One radar station is located near the town of Khizi (also spelled Khyzy, Xizi or Chyzy) in the mountainous northern part of Azerbaijan, approximately 50 km from the border with Russia. The other radar station is located near the town of Astara, located on Azerbaijan’s Caspian Sea coastline in close proximity to the border with Iran. The Astara radar station is about 20 km from the town with the same name on the Iranian side of the border.[1,2,3] According to Ambassador Harnish, the new radar stations are operational and have been integrated into the radar network that Azerbaijan inherited from the Soviet era.[1]

Developed by the European Command (EUCOM) of the U.S. armed forces (headquartered in Stuttgart, Germany) and financed by the Office of the Secretary of Defense (OSD), the CGI (also referred to as the Caspian Guard) is aimed at strengthening air, ground, and maritime border defense of Azerbaijan and Kazakhstan by addressing proliferation, terrorism, and trafficking trends around the Caspian Sea. Since its launch in the fall of 2003, the CGI has evolved from the concept development phase to full implementation with the establishment of an integrated airspaces, maritime, and border control regime for Azerbaijan and Kazakhstan. With a primary focus on maritime security and border defense, the CGI represents a unique effort in which the U.S. military, civilian agencies, and commercial entities are engaged in partnership arrangements with host countries to protect key offshore oil industry infrastructure and to counter regional security threats emanating from weapons proliferation,
terrorism, and illicit trafficking of narcotics, small arms and contraband commodities.[4,5,6,7,8]

The Khizi and Astara radar stations are capable of spotting objects within a 400-450-km area at a maximum altitude of 300 km. The Astara radar station is designed to monitor the entire southern coastline of the Caspian Sea and the northern and northeastern parts of Iran, whereas the Khizi radar station covers the southern part of the Russian Federation, including Chechnya and Dagestan, as well as the entire northern coastline of the Caspian Sea. While the stated purpose for the construction and operation of the Astara and Khizi radar stations is to monitor the borders of Azerbaijan, these stations are also capable of detecting ballistic missile launches and intercepting radio communications and cellular phone conversations, not only on the territory of Azerbaijan, but also in the aforementioned parts of Russia and Iran.[1,3,9,10]

In his discussion of U.S. assistance to Azerbaijan, Ambassador Harnish also noted that the U.S. government has already spent US$30 million on upgrading Azerbaijan’s coast guards’ equipment with a sophisticated radar system, personnel training, and ship repair, and that the United States intends to spend the same amount on strengthening the Azerbaijani navy.[1,9,11,12] Over the next six years, the U.S. government plans to invest US$135 million to strengthen the naval forces of Azerbaijan and Kazakhstan within the framework of the CGI.[1,4,9,11,12] Other complementary U.S. maritime border defense assistance programs include the US$20-million program launched in July 2004 and implemented by the U.S. Defense Threat Reduction Agency (DTRA) to train the Azerbaijani maritime border guards, as well as exercises organized by the U.S. Navy SEALS to train Azerbaijan’s elite 41st Special Naval Warfare Unit in June 2004.[4,10] The focus of these programs is to train the Azerbaijani maritime border guards and naval forces to intercept terrorists, weapons, and narcotics on the Caspian Sea.[5] Ambassador Harnish emphasized that the CGI is not directed against any country in the region.[1,11,12]

In Iran, the news about the construction of the two radar stations in Azerbaijan initially elicited a negative reaction. On September 25, 2005, the Iranian English-language newspaper Iran News featured an editorial stating that by allowing the United States to increase its military presence in the region under the guise of border defense cooperation, the Azerbaijani leadership was jeopardizing the country’s long-term national security interests. The author of the editorial argued that the growing U.S. military presence will ultimately curtail the influence of such regional powers as Russia, Iran, and China, which would inevitably lead to increased competition over the oil and gas resources of the Caspian Sea.[13]

The official reaction of the Iranian government, however, was milder. On October 7, 2005, at the 18th meeting of government officials from the Caspian Sea littoral states held in Baku, Azerbaijan, Mohsen Baharvend, head of the Iranian Foreign Ministry’s legal department, told the press that “Iran has no problem with countries that are cooperating to fight terrorism and drug trafficking. These are issues which all five Caspian nations are interested in resolving.”[14,15,16]

Considering that Russia operates an early-warning radar installation in Azerbaijan, Moscow has shown some concern about the construction of two U.S.-funded radar stations in Azerbaijan. On September 26, 2005, an unnamed top Russian military official told the Interfax news agency that, while the construction of any radar station in close proximity to Russian borders is undesirable, the radar station built in Azerbaijan “will not affect the combat readiness of the Russian Defense Ministry’s units and subunits deployed in the North Caucasus.”[17] The Russian official added that the main concern for the Russian side would be possible electromagnetic interference between the frequencies of Russian radar stations and the Khizi radar station in Azerbaijan.[17]

In a strategic move, the Russian delegation at the aforementioned meeting in Baku of the working group on the status of the Caspian Sea, which was held on October 6-7, 2005, called for the establishment of a new joint naval operations group—CasFor—that would include the naval forces of all five Caspian Sea littoral states. Closely mirroring the objectives of the CGI, the purpose of CasFor would be to protect the Caspian Sea from terrorism and to fight against trafficking in WMD, arms, and narcotics. The important condition embedded in the CasFor proposal is that it rules out the participation of non-regional powers, such as the United States. Clearly intended to serve as a potential counterweight to the CGI, CasFor would allow Russia to dominate this arrangement, since its naval forces would dwarf the combined naval forces of the remaining Caspian Sea littoral states.[18]

According to the Russian Minister of Defense, Sergey Ivanov, the first meeting of government representatives of all Caspian Sea littoral states for the creation of the CasFor will take place in Moscow on November 14, 2005.[19]

Editor’s Note: The legal status of the Caspian Sea, including the central issue of delimitation of maritime borders, has not yet been determined by the five littoral states. The negotiations on the legal status of the Caspian Sea have been under way for more than a decade since the breakup of the Soviet Union. Rich in oil and gas resources, the Caspian Sea represents a strategically important area for all five littoral states. In this context, whether the Caspian Sea is a lake or a sea spells out either benefits or losses for each of the five states. If the Caspian Sea is classified as a ‘sea’, under international law, each state would have a ‘territorial sea’, an exclusive economic zone, and a continental shelf. If on the other hand, it is treated as a ‘lake’ the sovereignty, rights of navigation, and terms of use of waters for non-navigation purposes would have to be determined by the border states.[20,21] For a


**Slovakia Installs X-Ray Scanner Donated by China on the Slovak-Ukrainian Border**

On September 8, 2005, the Customs Administration of the Slovak Republic installed an X-ray scanner designed for customs control of passenger cars, trucks, buses, and transport containers at the Vyšné Nemecké-Uzhhorod border crossing on the Slovak-Ukrainian border. This container/vehicle inspection system, worth about 100 million Slovak korunas (US$3.1 million), was donated by the government of the People’s Republic of China during Slovak president Rudolf Schuster’s visit to China in January 2003.[1,2,3]

The screening equipment, capable of detecting smuggled goods under a 26-centimeter- (cm) -strong steel layer, will help Slovak customs officers curb the smuggling of numerous types of goods. According to experts, radiation from the scanner poses no danger to people, since it does not exceed the level of radioactivity in regular medical X-ray equipment.[1]

The inspection system was produced by the Chinese company NUCTECH, which specializes in research, development, and manufacture of X-ray inspection technology with support from the Beijing-based Tsinghua University. According to the company’s website, the container/vehicle inspection system is the first system in the world that uses linear accelerators as the radiation source. The equipment does not need stationary buildings to shelter and operate and can be relocated to a new site within a short period of time.[4]


**Summaries from the Regional Press**

**Tajik Authorities Call for Support to Protect Sections of the Tajik-Afghan Border**

On September 27, 2005, Major General Nuralisho Nazarov, first deputy chairman of the Committee for State Border Protection of Tajikistan, acknowledged that a section of the Tajik-Afghan border covering 53,000 hectares (130,910 acres) is controlled neither by Tajik border guards nor by their Afghan counterparts. The statement was made at the international donor conference entitled “Partnership for Security and Development on the Tajik-Afghan Border” organized in the Tajik capital Dushanbe, on September 27-28, 2005, by the European Union’s (EU) Border Management
Program for Central Asia (BOMCA) and Central Asia Drug Assistance Program (CADAP).

The conference discussed border management issues and related assistance following the withdrawal of Russian border guard troops from Tajikistan. Nazarov added that the Tajik border guard service hopes to receive about US$30 million from foreign donors in 2005-2007 to strengthen security on the Tajik-Afghan border. The funds are to be spent on constructing and equipping border posts that meet international standards and on upgrading border outposts that have been transferred by Russian border guards to the Tajik side. As Nazarov noted, “donors have to render effective assistance to Afghan border guards too,” since strengthening only the Tajik side of the border will not yield positive results if no similar actions are taken on the Afghan side.[1]

Following the donor conference, on September 29, 2005, the Committee for State Border Protection of Tajikistan and Ministry of Internal Affairs of Afghanistan signed a Memorandum of Understanding (MOU) to serve as a basis for border security and management cooperation between the two countries. According to the MOU, the two sides agreed to open a border crossing on the Khorog section of the border, exchange information and expertise, and conduct joint training sessions. Speaking at a press conference after the signing ceremony, Nuralisho Nazarov said that Afghan authorities helped release several Tajik nationals previously held hostage in Afghanistan. According to Nazarov, as many as 27 Tajiks, mainly from the border district of Shurobad, are still being held hostage in northern Afghanistan because of debts owed to Afghan drug lords for smuggled narcotics.[2,3] However, Afghan Ambassador to Tajikistan Muhammad Dovud Panjsheri reported that, according to information obtained from the Tajik Ministry of Foreign Affairs, the number of hostages is much lower.[3]

In a related development, on October 10, 2005, Nikolay Bordyuzha, secretary general of the Collective Security Treaty Organization (CSTO), stated that equipping and reinforcing controls at the Tajik-Afghan border is not solely Tajikistan’s task but that of all the CSTO member states. According to Bordyuzha, speaking at the roundtable meeting in Moscow entitled “The Role of Russian-Kazakhstan Cooperation in Strengthening the Security System in Central Asia,” Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia should allocate funds for equipping the Tajik-Afghan border because these nations all suffer from Afghanistan-originating drug trafficking. Noting that until recently Russia had been responsible for security of the entire Tajik-Afghan border, the CSTO secretary general remarked that the Tajik government currently lacks resources to ensure security on the border independently. Bordyuzha concluded that “if CSTO member states provide the resources to Tajikistan, we will be able to seal this border.”[4]

Editor’s Note: The Collective Security Treaty was signed by Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan in May 1992. In 1999, Azerbaijan, Georgia, and Uzbekistan withdrew from the treaty. It was transformed into the Collective Security Treaty Organization in May 2002. The CSTO is a joint security program that commits member states to support and sustain regional security. Current CSTO members are Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia, and Tajikistan.


International Supplier Regimes

The Democratic Republic of the Congo Becomes State Party to the CWC

On October 12, 2005, the Democratic Republic of the Congo (DROC) deposited its instrument of ratification of the Chemical Weapons Convention (CWC), and thirty days after that date, on November 11, 2005, the DROC became the 175th state party to the convention. The DROC is the 44th African state to become party to the convention.[1]

In November 2003, the Organization for the Prohibition of Chemical Weapons (OPCW) created the Action Plan on Universality, which seeks to achieve universal adherence to the treaty by April 29, 2007, the tenth anniversary of the CWC’s entry into force.[1] As part of this plan, the organization has conducted a series of outreach activities in Africa to assist countries in the region with capacity building and implementation support. These activities included a meeting held October 20-21, 2005, of African states’ national authorities (the government entities charged with CWC implementation) in Abuja, Nigeria. The DROC attended this meeting as a contracting state to the CWC.[2]

Editor’s Note: State parties to the CWC must abide by various restrictions on the trade of chemicals controlled under the convention. CWC-controlled chemicals are listed in three schedules. Schedule 1 contains chemicals that have been developed or used as chemical weapons or are the immediate precursor compounds used in the production of chemical weapons. Schedule 1 chemicals do not have “significant legitimate commercial use” in large quantities.[3] According to the CWC Annex on Implementation and Verification,
OPCW state parties “may transfer Schedule 1 chemicals outside [their] territory only to another State Party and only for research, medical, pharmaceutical or protective purposes,” and the parties must notify the OPCW of any transfer within 30 days of its occurrence. Re-export of Schedule 1 chemicals is not allowed.

Schedule 2 chemicals are considered to have some commercial value, but also have “warfare potential.”[3] Since April 29, 2000, (three years after the CWC’s entry into force), exports of Schedule 2 chemicals have been limited to OPCW states parties.

Schedule 3 chemicals are toxic chemicals or chemical weapons precursors that are generally produced in large volumes and have significant commercial value. These chemicals can be exported to non-parties to the CWC, as long as an end-use certificate is provided, confirming that they will not be used for the production of chemical weapons.


**Embargoes and Sanctions Regimes**

**U.S. Citizen Convicted for Smuggling Electronic Components to China**

On September 21, 2005, Ning Wen, resident of Manitowoc, Wisconsin, was convicted by a federal court in Milwaukee, Wisconsin, on nine counts of conspiring to export controlled electronic components worth more than US$500,000 to China’s Beijing Rich Linscience Electronic Company (BRLE). The charges against Wen also included money laundering and making false statements to federal officials.[1] Wen and his wife Hailin Lin—both naturalized U.S. citizens originally from China—were arrested in September 2004.[2,3] Two other individuals, Jian Guo Qu and Ruo Ling Wang, both Chinese citizens and employees of the Beijing-based BRLE, were also arrested in Wisconsin in September 2004 while on their way to visit Wen and Lin.[1,2] Wen faces up to 25 years in prison and will be sentenced at a later date. Lin, Qu, and Wang have all pled guilty in the case.

According to Steven M. Biskupic, U.S. Attorney for the Eastern District of Wisconsin, “The case involved the export of restricted electronic equipment components that had a wide variety of uses including military radar and communications applications.”[1] On more than 30 occasions between June 7, 2002, and September 17, 2004, Wen’s company, Wen Enterprises, illegally exported components controlled under the U.S. Export Administration Regulations (EAR) to BRLE with the knowledge that these items required an export license from the U.S. Department of Commerce (DOC).[4] Wen Enterprises shipped semiconductors and other electronics to Qu and Wang at BRLE, who then transferred the items to the 54th Research Institute in China. The 54th Research Institute has been identified by the DOC as posing “an unacceptable risk in the development of missiles.” According to conversations monitored by the U.S. Federal Bureau of Investigation (FBI), Wen and Lin indicated that the equipment would ultimately be used by Chinese military against Taiwan.[2]

Temporary Denial Orders (TDOs) were issued against Wen, Lin, Wen Enterprises, and BRLE on February 7, 2005.[5] These TDOs were extended on July 27, 2005.[6] [Editor’s Note: A temporary denial order is issued by the U.S. Bureau of Industry and Security (BIS), specifically, by the assistant secretary for Export Enforcement, in order to “prevent an imminent or on-going export control violation.” A TDO denies a company or individual the right to engage in export activities and is issued for a renewable 180-day period.][7]

Advanced semiconductors can be used in military radar applications to enhance missile and nuclear programs. Therefore, exports of these items are controlled by the U.S. government under the EAR and are included on the control lists of the Wassenaar Arrangement. According to testimony given to a committee of the U.S. Congress in June 2005 by acting undersecretary of Commerce for Industry and Security Peter Lichtenbaum, “Under U.S. export control policy, license applications for semiconductor manufacturing equipment and technology are reviewed on a case-by-case basis by the Departments of Commerce, Defense, State, Energy and the intelligence community. The review process is thorough as the interagency vets the end-user to mitigate concerns that the technology will be diverted. There is a policy of denial for exports for military-end users/end-uses in China.”[8]

Editor’s Note: Wen worked at the Chinese consulates in San Francisco and Los Angeles from 1986-1992. According to court documents filed by U.S. prosecutors, Wen acted as an informant for the FBI from 1989-2004.[2,6] While the period in which Wen worked as an informant overlapped with the period of his unlicensed transfers to BRLE, it is unclear from available sources when the FBI became aware of Wen’s illegal activities.

On September 27, 2005, Arif Ali Durrani, a Pakistani national and long-time arms dealer, appeared in a federal court in California to face charges of conspiring to export illegally military equipment included in the U.S. Munitions List. According to federal prosecutors, Durrani, who had previously served five years in prison for other arms export violations, worked with two Southern California–based businessmen to acquire and export parts for military aircraft to the United Arab Emirates, Malaysia, and Belgium. According to media reports, federal agents suspect that the ultimate destination for the controlled components was Iran, although this claim is not mentioned in the indictment.

The arms dealing activities of Arif Durrani have occupied the attention of U.S. authorities for two decades. In 1986, Durrani was arrested by U.S. federal agents for illegally exporting components of the HAWK anti-aircraft missile to Iran. Durrani has argued that his actions were authorized by the Reagan administration—and in particular by Lt. Col. Oliver North—as part of the Iran-Contra “arms-for-hostage” affair. These claims did not impress the jury in his case, and Durrani was convicted in 1987 of violating the U.S. Arms Export Control Act. Durrani has argued that his actions were authorized by the Reagan administration and in particular by Lt. Col. Oliver North—as part of the Iran-Contra “arms-for-hostage” affair. These claims did not impress the jury in his case, and Durrani was convicted in 1987 of violating the U.S. Arms Export Control Act. However, these charges were dropped shortly before Durrani appeared in court in September 2005, since his customer had obtained the required licenses. Commenting on this initial indictment, Durrani’s attorney stated that the U.S. government was “forced to dismiss charges because [they] were fake,” adding that Durrani “has done nothing wrong.” However, a new set of charges against Durrani—including activities in 2004 and 2005—was immediately filed by prosecutors.

As part of the investigation into Durrani’s arms dealing, U.S. federal prosecutors recently indicted George Charles Budenz II of Escondido, California, and Richard Tobey of Temecula, California. Budenz and Tobey were charged with acquiring controlled components ordered by Durrani for his customers and exporting them without the required licenses. According to statements given by Budenz, he met Durrani in 1999 in Mexico. Durrani suggested to the California businessman that he work as Durrani’s agent in the United States. Budenz, a retired Navy commander, agreed to help acquire aircraft parts for Durrani’s customers from U.S.-based aerospace firms. On October 18, 2005, Budenz, pleaded guilty to illegally exporting components for U.S. F-5 fighter jets, T-38 military trainer jets, and Chinook military helicopters to Malaysia and Belgium. His sentencing is scheduled for January 9, 2006. Under a plea bargain agreement, he likely faces approximately six years in prison.

Tobey, who headed Airpower Supply, a Temecula-based firm, pleaded guilty in August 2005 to charges that he worked with Durrani to export illegally a rear canopy panel for a T-38 aircraft to the United Arab Emirates in July 2004. According to ICE, Tobey admitted purchasing and exporting the controlled components at the behest of Durrani. In August 2005, Tobey pleaded guilty to a felony charge of conspiracy to violate the U.S. Arms Export Control Act.

Durrani’s June arrest by ICE was based on a 1999 indictment that charged him with illegally shipping components for J-85 jet engines to Iran in 1994. [Editor’s Note: J-85 engines are used in T-38 military training aircraft. The engine was originally designed to propel the U.S. Air Force ADM-20 “Quail” decoy missile.] However, these charges were dropped shortly before Durrani appeared in court in September 2005, since his customer had obtained the required licenses. Commenting on this initial indictment, Durrani’s attorney stated that the U.S. government was “forced to dismiss charges because [they] were fake,” adding that Durrani “has done nothing wrong.” However, a new set of charges against Durrani—including activities in 2004 and 2005—was immediately filed by prosecutors.

According to statements given by Budenz, he met Durrani in 1999 in Mexico. Durrani suggested to the California businessman that he work as Durrani’s agent in the United States. Budenz, a retired Navy commander, agreed to help acquire aircraft parts for Durrani’s customers from U.S.-based aerospace firms. On October 18, 2005, Budenz, pleaded guilty to illegally exporting components for U.S. F-5 fighter jets, T-38 military trainer jets, and Chinook military helicopters to Malaysia and Belgium. His sentencing is scheduled for January 9, 2006. Under a plea bargain agreement, he likely faces approximately six years in prison.

Released from prison in 1992, Durrani moved to Ventura, California, and went back into the business of selling aircraft components—despite the fact he was not legally allowed to do so after his 1987 conviction. His business activities once again became the target of U.S. investigators and, in 1998, Durrani left the United States, ultimately resettling in Mexico. U.S. authorities allege that Durrani masterminded an arms ring from the town of Rosarito, about 30 miles from the U.S.-Mexican border, and illegally exported controlled aircraft components from the United States to third countries. In June 2005, Mexican authorities arrested Durrani in Rosarito on immigration violations and deported him on a plane bound for Pakistan, with a stopover in Los Angeles. Durrani was arrested by U.S. Immigration and Customs Enforcement (ICE) agents when he reached Los Angeles.

Editor’s Note: U.S. officials apparently informed Mexican authorities that they had a sealed indictment for Durrani. According to media reports, the Mexican authorities could not hand over Durrani directly to U.S. authorities because he was a third-country national. However, Mexican authorities appear to have deported Durrani via the United States in order to give U.S. agents the opportunity to apprehend him.
Washington Waives Some Restrictions on Libya, Allowing U.S. Companies to Help Libya Destroy Chemical Weapons Stockpile

On September 28, 2005, U.S. President George W. Bush waived restrictions against Libya under Sections 40 and 40A of the Arms Export Control Act (AECA), which prevent transactions with countries supporting acts of international terrorism and countries not cooperating fully with U.S. anti-terrorism efforts.[1,2] The waiver allows U.S. companies to work with Libya to destroy its declared chemical weapons stockpile, which consists of 23 metric tons of mustard gas.[2,3,4] The waiver also allows the Libyan government to refurbish eight C-130 transport planes it purchased from the United States in 1973.[5]

Diplomatic relations between Washington and Tripoli were restored in June 2004 after the Libyan government agreed in August 2003 to pay US$2.7 billion in compensation to the victims of the 1988 bombing of a Pan Am airliner over Lockerbie, Scotland. In December 2003, Libyan leader Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs, and on February 5, 2004, Mu’ammar Al-Qadhafi’s announced that Libya was dismantling all its WMD programs. Libya was also willing to make reparations for the Lockerbie bombing.

Despite advancement in bilateral relations, Libya still remains on the State Department’s list of states that sponsor terrorism.[9]

Two More Arrested in Case of Nuclear Smuggling to Libya

On September 10, 2005, Swiss authorities announced that two more individuals have been arrested in a case involving Swiss engineer Urs Tinner, who is accused of working with Pakistani scientist A.Q. Khan and his nuclear black-market network. Tinner was arrested in Germany in October 2004 for allegedly conspiring to supply nuclear weapons–related materials to Libya.[1] Specifically, Tinner is reported to have overseen the manufacturing of gas centrifuge parts in factories in Malaysia that were connected to the Khan network. Some of these parts were meant for the now abandoned Libyan nuclear weapons program.[1] Tinner is currently in jail in Switzerland awaiting adjudication of his case. He was extradited from Germany to Switzerland in May 2005.[2] [Editor’s Note: The Urs Tinner case was reported previously in the NIS Export Control Observer. For more details on the case see, “Germany and Switzerland Investigate Suspected Members of Proliferation Network,” NIS Export Control Observer, No. 21, October 2004, pp. 24-26; and Kenley Butler, “How the Abdul Qadeer Khan Network Circumvented Export Controls,” NIS Export Control Observer, No. 27, May 2005, pp. 22-24.]

Swiss federal prosecutor spokesperson Hansjürg Mark Wiedmer did not identify the two arrested individuals and refused to confirm or deny whether they were family members of Tinner.[1] Both Urs Tinner’s brother and father have been previously implicated in the nuclear smuggling ring. Marco Tinner, Urs Tinner’s brother, reportedly sold materials to the company with which Urs Tinner worked in Malaysia, and their father, Fredrick Tinner, has been accused by authorities of being associated with Khan.[1] Additionally, Fredrick

International Developments

CSI Update — U.S., Canada Sign Partnership; Ports of Santos and Colombo Operational

On October 20, 2005, U.S. Customs and Border Protection (CBP) and the Canada Border Services Agency (CBSA) signed a Container Security Initiative (CSI) partnership arrangement, formalizing CBP-CBSA cooperation under the U.S.-Canada “Accord on Our Shared Border.”[1] Previously, on July 15, 2005, Canadian Deputy Prime Minister and Minister of Public Safety and Emergency Preparedness Anne McLellan announced that the Canadian government would budget CA$134 million (US$114 million) over five years to fund Canadian participation in CSI, allowing CBSA to deploy officers to overseas ports, and thereby enhancing security and harmonizing risk assessment systems with the United States in order to better protect North America.[2]

CBP also announced recently that the Brazilian port of Santos and the Sri Lankan port of Colombo have become, respectively, the 39th and 40th ports operational under CSI. The port of Santos became operational on September 22, 2005, and the port of Colombo became operational on September 29, 2005. The port of Santos is the largest port in South America and a major export center, making it a strategic port for container traffic to the United States.[3,4]

Marking the 40th port milestone, CBP Commissioner Robert Bonner announced that currently 75 percent of container traffic bound for the United States either originates or is transshipped through a port operating under CSI. He stated: “Because of the sheer volume of sea container traffic and the opportunities it presents for terrorists, containerized shipping is uniquely vulnerable to terrorist attack. CSI is one of the most revolutionary and successful homeland security initiatives developed and implemented after September 11, 2001.”[4]

CBP plans to increase the CSI program to 50 operational ports by the end of 2006, which will account for 90 percent of all U.S.-bound containers.[4] The governments of Argentina and Portugal have signed declarations of principles with CBP and are currently preparing for CSI programs at the ports of Buenos Aires and Lisbon. [5]

Under CSI, U.S. CBP agents are stationed at overseas ports to secure maritime containerized cargo shipments from terrorist tampering. Working with local host nation counterparts, the CBP agents perform risk assessments on all containers destined for the United States and make requests to the host country officials to use non-intrusive inspection equipment to conduct pre-screenings of all containers considered to present a risk.

Editor’s Note: The following 40 ports are currently operational under CSI: Antwerp and Zeebrugge, Belgium; Santos, Brazil; Halifax, Montreal, and Vancouver, Canada; Hong Kong (SAR), Shanghai and Shenzhen, China; Le Havre and Marseilles, France; Bremerhaven and Hamburg, Germany; Piraeus, Greece; Genoa, Gioia Tauro, La Spezia, Livorno, and Naples, Italy; Kobe, Nagoya, Tokyo, and Yokohama, Japan; Port Klang and Tanjung Pelepas, Malaysia; Rotterdam, the Netherlands; Singapore; Durban, South Africa; Pusan, South Korea; Algeciras, Spain; Colombo, Sri Lanka; Göteborg, Sweden; Kaoksiung, Taiwan; Laem Chabang, Thailand; Dubai, UAE; Felixstowe, Liverpool, Southampton, Thamesport, and Tilbury, United Kingdom. Also see Shi-Chin Lin, “The U.S. Container Security Initiative in Asia,” Asian Export Control Observer, No. 2, June 2004, pp. 18-21, <http://cns.miis.edu/pubs/observer/Asian/pdfs/aeco_0406.pdf>.


Round-Up: Incidents Involving Radioactive Material

Radiological Material Stolen from Factory in Philippines

Three industrial machines containing radioactive krypton-85 were reported lost after looting occurred in June 2005 at an abandoned paper manufacturing plant in the Mapulang Lupa District of Valenzuela City, the Philippines.

The basic weight gauges, used to measure the thickness, density and weight of paper, disappeared from the Paper City Corporation plant, which closed in 2002 due to foreclosure.[1] The krypton-85 was encased in titanium capsules and shielded within a steel container. If the intact capsules were removed from the container, the krypton-85 would emit 1,330 millisieverts of radiation per hour, sufficient to cause third-degree burns.[2] Though krypton-85 is a gas and cannot be used in a nuclear weapon, Teofilo Leonin, Jr., head of the Philippine Nuclear Research Institute’s (PNRI) Radiological Impact Assessment Unit, did not discount the possibility that a group could make an “outrageous” claim to have constructed a bomb with the material.[1] On September 8, 2005, the PNRI published an alert about the missing material and called upon the public to assist in retrieving the equipment.[3]

Editor’s Note: Because krypton-85 is a gas, it is not typically thought of as a radioactive material useful for a radiological dispersal device, one type of which is popularly known as a “dirty bomb.” However, the relatively large amount of radioactivity in the gauges could pose a radiation safety hazard if not handled properly.


Cesium-137 Capsules Stolen in Venezuela

On September 20, 2005, Venezuelan authorities announced that an undetermined number of containers filled with capsules of radioactive cesium-137, used by the Venezuelan Health Ministry to treat uterine cancer, were stolen from the Metropolitan Mayoralty storeroom in the Cementerio zone of Caracas. Chief of the Venezuelan Civil Defense Antonio Rivero suggested that the thieves were most likely interested in the value of the lead containers and not the contents, since many of the cesium capsules had been discarded.[1,2] Venezuela has had problems in the past securing radioactive materials used for industrial purposes. In two separate incidents in April 2005, capsules of radioactive iridium-192, which the oil industry uses to check for cracks in pipes, disappeared from a barge on Lake Maracaibo and from the back of a truck in the state of Monagas. Antonio Rivero expressed concern that the iridium capsules might be used for terrorist purposes.[3] [Editor’s Note: Cesium-137 and iridium-192 are among the material considered suitable for use in radiological dispersion devices or “dirty bombs.”]


Radioactive Source Found in Saratov, Russia

According to Russian media reports, on August 23, 2005, a radioactive source was found in the village of Tarkhany in Russia’s Saratov Oblast. The item, 5 cm by 4 cm in size and marked with a radioactivity sign, was discovered under a seeding machine in the yard of a private house. Measurements made by regional emergency response officials showed that radiation from the container was about 70 microsievert per hour, which exceeds the background level by 350 times. Upon examination, specialists from the Saratov Radon Special Combine who were called to the site suggested that the item might contain cesium-137 or strontium-90/yttrium-90 isotopes. According to Nikolay Aktyayev, Radon’s deputy chief engineer, the item was probably a component from an instrument used for testing the performance of radiation dosimeters. Officials claimed that the local population was not exposed to radiation and that the source did not cause radioactive contamination. The item was placed in a special storage site, and an investigation is under way to determine the origin of the radioactive item.[1,2] [Editor’s Note: Radon is a network of Russian state enterprises responsible for the disposal of radioactive waste.]


KyrgyzAuthorities Secure 1,000 Radioactive Sources, Continue to Search

In the past 12 months, Kyrgyzstan has secured or disposed of 1,000 items of radioactive material deemed to be vulnerable to theft or terrorism, BBC News reported on October 7, 2005. According to Kyrgyz authorities, there are 500 more items to secure, and an unidentified amount of material is still missing.[1]

When the Soviet Union disintegrated, the centralized control of radioactive materials collapsed, and many radioactive sources were lost or abandoned. With U.S. assistance and in cooperation with the IAEA, the Kyrgyz government is now working to secure radioactive materials and prevent terrorists from acquiring them.[1]
At present, Kyrgyzstan does not have a complete inventory of radioactive sources. According to IAEA representative Carolyn McKenzie, the Kyrgyz government needs a plan of action to search for the missing sources. Currently, radioactive materials often end up as scrap, and it is typically scrap workers who find them and run the risk of radiation poisoning, McKenzie said.[1]

The largest missing sources are believed to be Radioisotope Thermoelectric Generators (RTGs) that were used to power mountain-top radio transmitters. They are easy to carry and therefore can be attractive to terrorists.[1] [Editor’s Note: RTGs were built during the Soviet era to power space facilities, remote lighthouses, meteorological stations, naval navigational aids, and some military facilities. RTGs are powered by strontium-90, a radioactive material with a half-life of 200 years, and contain 30,000-300,000 curies of radioactivity, making them extremely dangerous if dismantled. As such, they could provide material for a radiological dispersal device (RDD). No data is available on the number of RTGs remaining in Kyrgyzstan, but according to a May 2003 report by the U.S. General Accounting Office, there were, at that time, approximately 1,031 of them in the former Soviet Union.][2]

According to Kubanychbek Noruzbayev, section head at the Department of Ecology and Nature Management of the Kyrgyz Ministry of Environment and Emergency, the movement of sources across national borders is an area of concern. He noted that Kyrgyzstan lacks a sufficient number of border guards, that radiation monitoring of vehicles crossing the border is unsatisfactory, and that villagers who live along the border complain corruption is high. According to Noruzbayev, there have been several cases of individuals trying to import radioactive sources illegally into the country.[1] No further details on these incidents were provided.


Ukraine Secures Missing Radioactive Material

On September 28, 2005, authorities at the Chernobyl nuclear power plant (NPP) announced that they had found a plastic bag containing 13 pipes and a 10-cm bar that resembled fragments of nuclear fuel rods in the compound of the closed nuclear power plant.[1] The bag, emitting background radiation of 50 microroentgens per hour, was found hidden under a railroad car during a routine radiation check in the area surrounding the sarcophagus—the concrete structure erected to isolate the remains of the collapsed Unit 4 reactor. Authorities at the Chernobyl NPP said the bag containing the pipes had been taken to a temporary storage area, and an investigation was under way.[2]

Ukrainian authorities believe that the pieces may have been stolen in 1995 along with 5 kg of fresh nuclear fuel from a fuel assembly in Unit 4 of the Chernobyl NPP.[3] In 1996, four people were detained and later convicted of the fuel theft. Following the discovery of the missing fuel, the Chernobyl NPP introduced additional controls over the nuclear fuel in Unit 4 and installed radiation detection equipment in the main building and the sarcophagus zone.[2] The plant’s spokesperson, Stanislav Shketela, said the recently discovered material could have been stolen by the same individuals involved in the 1995 incident, who may have then hidden the bag but never managed to remove it from the NPP due to the tightened security.[1] Previous reports on the case, however, did not mention any additional missing material.


Workshops and Conferences

OPCW Hosts Workshop for Customs Authorities on CWC Implementation

On October 4-5, 2005, the OPCW held the Workshop for Customs Authorities on Technical Aspects of the Implementation of the Chemicals Transfer Regime at its headquarters in The Hague, the Netherlands.[1] The European Union Joint Action Plan sponsored the workshop. The Joint Action Plan provides support to the OPCW’s implementation CWC, as a part of the European Union strategy against proliferation of WMD.[1]

Editor’s Note: The EU Council, the main decisionmaking body of the EU, adopted the Action Plan on nonproliferation of WMD in June 2003, and incorporated the Action Plan into the EU strategy against proliferation of WMD in December 2003. The strategy stipulates that the EU should enhance political, financial, and technical support to verification regimes, including the CWC.[2,3]

The workshop provided information to customs authorities on ways to improve domestic capabilities for tracking transfers of chemicals controlled under the CWC.[4] In his opening address, OPCW Director-General Rogelio Pfirter emphasized the key role that customs authorities play in the national implementation of the CWC and how improving their
understanding of the convention will enable better implementation.[1]

Representatives from more than 20 state parties and three organizations—the United Nations Environmental Program (UNEP), the World Customs Organization, and the Port Authority of Rotterdam—delivered presentations about specific implementation-related issues, including how states and organizations can cooperate with the OPCW to deal with the transfer of chemical substances.[1]

This was the first time UNEP representatives participated in an OPCW workshop. The head of UNEP’s OzonAction Branch, Rajendra Shende, stressed the importance of collaboration between the OPCW and the parties to the Montreal Protocol. [Editor’s Note: The Montreal Protocol is a multilateral treaty designed to protect the stratospheric ozone layer by phasing out the use of certain chemicals. The protocol entered into force in 1989 and currently 183 countries are party to the treaty.] [5] Shende stated that the OPCW would benefit from the implementation of the Montreal Protocol, and that parties to the protocol could learn from the effective verification and destruction measures developed by the OPCW.[6]

Special Report

South Korean Export Control Awareness on Rise but Compliance Lacking

By Dave H. Kim, Research Associate, Center for Nonproliferation Studies

Government and private sector cooperation are critical for any export control system, but in many cases company awareness and compliance lag behind the promulgation of laws and regulations. According to recent polling data, this is clearly evident in the Republic of South Korea (ROK), where it appears that greater private sector outreach may be necessary to raise export control compliance.

A recent poll by the Korea International Trade Association (KITA) revealed that, while most South Korean firms believe export control regulations for strategic items are necessary, few of them actually obtain government authorization prior to exporting controlled materials. The poll’s results, released on October 5, 2005, indicated that 66.7 percent of the 576 export companies surveyed were “aware of the export control system, though not well acquainted with the details,” while only 22.2 percent “had detailed knowledge of the regulations.” The remaining 11.1 percent responded that they “had never heard of the export control system.”[1,2]

When asked if they were checking whether the goods intended for export were subject to export controls, only 38.9 percent of all respondents answered yes, implying that the other 60 percent or so were not taking this step. [1] South Korea’s large companies (with 300 or more employees), however, appeared to perform better than smaller companies. For example, 52.6 percent of large firms claimed to have “detailed knowledge of export control regulations,” and 65.8 percent answered that they had been checking whether their intended exports were subject to control.[1]

The reasons most frequently given by respondents to explain why they did not seek to obtain government approvals for their exports were: (a) they were “not familiar with export control regulations” (50 percent), (b) they “didn’t think it would lead to problems” (28.7 percent), and (c) licensing procedures are “confusing and difficult” (8.0 percent).[1]

KITA’s poll, which was conducted via e-mail in August 2005, came after repeated international pressure on Seoul to step up its export control efforts. In particular, the United States had expressed concern about the South Korean government’s difficulty in stopping unauthorized export of strategic goods and technology, going as far as to hint at possible sanctions against offending South Korean firms.[3,4] [Editor’s Note: South Korea is a member of all international export control arrangements and nonproliferation regimes; however, Seoul does not participate in the Proliferation Security Initiative.]

The ROK government has admitted that many South Korean businesses have violated export control regulations due to a lack of knowledge of export control rules, and it has also taken significant steps to improve its export control system. For example, in December 2004, the South Korean Ministry of National Defense (MND) designated 8,023 materials and technologies in the Korean defense sector that are now subject to export controls.[5,6,7,8,9] The control list, which applies to 97 high-tech weapons systems produced by licensed defense firms, was divided into three categories: Level A, which must not be transferred to other countries; Level B, which may be exported to allies only; and Level C, which may be exported to most countries except those that sponsor terrorism or are hostile to South Korea.[5,6,7,8,9] [Editor’s Note: For details, see: “South Korea Set to Include More Than 8,000 Weapons Technologies on Export Control List,” Asian Export Control Observer. No. 5, December 2004/January 2005, p. 13, <http://www.cns.miis.edu/pubs/observer/asian/index.htm>].

Despite these efforts to improve its export control system and due in part to vast increases in exports of weapons and defense-related technologies, compliance by South Korean companies has been suboptimal. [Editor’s Note: Defense-related exports in 2004 surpassed US$400 million, an all-time high].[5] Many Korean exporters found the MND’s 500-page list of strategic items for export control to be too vast and cumbersome, and they often consider the average of 15 days to process their requests to be too long.[10,11]

In an effort to both streamline the process and reduce the likelihood of inadvertent violations of export control regulations, on February 17, 2005, the ROK Ministry of Commerce, Industry and Energy (MOCIE) launched the Korea Strategic-Item Export Control Information System.[10,11] MOCIE’s online database system [available at http://www.sec.go.kr] was touted as allowing registered users easy access via personal computers to information needed to make accurate determinations in 10-20 minutes of whether intended exports would require licenses. In addition, the ROK government announced a clemency for past unlicensed exports of sensitive material and a grace period that lasted until the end of June 2005 so that firms could learn the new system.[10,11] [Editor’s Note: See: “South Korea Launches Online Database for Strategic Items Exports,” Asian Export Control Observer, No. 6, February/March 2005, p. 2, <http://www.cns.miis.edu/pubs/observer/asian/index.htm>].

This decision to “pardon” past export control offenders was designed to elicit cooperation and the admission of mistakes from companies that have been, according to a MOCIE official, “ignorant of the fact that they were shipping products that were banned.”[3,10] Studies sponsored by the ROK government conducted from May to December 2004 revealed
that 1,277 export firms requested clarification on items intended for export, with 70 companies proceeding to mistakenly ship sensitive goods.[3,10,11]

Seoul’s move to pardon past offenses drew frowns from Washington, which judged this forgiveness as too lenient on South Korean firms. Pressure from the U.S. government may have played a role in prompting Seoul to promise, during high-level bilateral meetings, to tighten controls and to deal more harshly with future violations.[3,4] Putting words into actions, on August 16, 2005, MOCIE introduced plans to further tighten exports of strategic goods during the first half of 2006. MOCIE is expected to submit the new legislation to the ROK National Assembly at the end of October 2005.[12,13,14]

The MOCIE plan, which is expected to receive little opposition in the legislature, proposes three significant changes to South Korea’s export control system. Firstly, it shifts the burden of final accountability to trading firms, obliging them to report items if they are unable to determine whether the items are strategically sensitive.[12,13,14] According to a MOCIE official, this is intended to eliminate inadvertent violations. “Although old rules made it obligatory for companies to determine for themselves if an item was on the sensitive items list,” the official noted, “they did not have to ask the government if they were not certain, which resulted in such products being sent abroad by mistake on some occasions.”[12]

The second change expands the breadth of ROK export controls by including software and related technologies. The third reform is designed to eliminate a loophole in ROK foreign trade laws, by requiring government clearance on intermediary trade—where a middle person buys foreign goods and transfers them to a third country without the item entering South Korean territory.[12,13]
