CSIS

TRANSNATIONAL THREATS UPDATE

Volume 1 • Number 11 • August 2003

"Defending our Nation against its enemies is the first and fundamental commitment of the Federal Government. Today, that task has changed dramatically. Enemies in the past needed great armies and great industrial capabilities to endanger America. Now, shadowy networks of individuals can bring great chaos and suffering to our shores for less than it costs to purchase a single tank. Terrorists are organized to penetrate open societies and to turn the power of modern technologies against us."

President George W. Bush, *2002 National Security Strategy*

CONTENTS

Terrorism

Dialogue of Fire: Saudi Arabia's Robust Reply to Al Qaeda

International counterterrorism authorities have been unrelenting in the face of recent terror activity, but few have stood out more prominently than Saudi Arabia's forces. Experts assess that Al Qaeda is on the move again, planning multiple attacks most probably in the Near East and Southeast Asia. However, the terror organization's initiative has coincided with Saudi Arabia's visceral reaction to a series of pressure points, including Western accusations of negligence and fresh wounds wrought from the bombing in Riyadh. Since the bombing, the kingdom has arrested over 200 suspects and killed 6 confirmed Al Qaeda associates.

The international community braced itself after the recent hotel bombing in Jakarta, Indonesia, and this heightened state of alert has yielded positive results, especially in Saudi Arabia. Saudi authorities have conducted over 15 raids, uncovering documents that revealed an Al Qaeda plot to attack a British Airways flight in the kingdom. In another case, a gun battle led to the arrest of 10 suspected members of a terrorist cell. Tragically, in an episode that followed, 3 security officers and 1 suspected terrorist died in a firefight. The raid resulted in another triumph for the Saudis: the capture of 7 more suspected terrorists. *(Combined Dispatches)*

Could Organized Crime in Russia's Eastern Region Aid Terrorists?

Russia's southeastern port cities, long-time breeding grounds for organized crime syndicates, have recently been identified as potential sites for the nuclear black market. In late July two separate consignments of nuclear materials were intercepted by a joint operation consisting of the Russian Federal Security Service (FSB) and an anti-organized crime police directorate. The first seizure took place in the city of Spassk-Dalniy and was followed two days later by another interception to the south in Ussuriysk. The Spassk-Dalniy operation prevented the sale of three containers of Caesium, while the subsequent sting uncovered the sale of 4.5 grams of Uranium-238. Each city is a point along the trans-Siberian railway and is also in close proximity to the coastal ports of Vladivostok and Nakhodka.

Like most maritime cities in the region, Vladivostok and Nakhodka have become international hubs for organized crime gangs. Shortly after the fall of the Soviet Union, they were infiltrated and then dominated by Russian mafia gangs. The cities were overrun by gangland warfare, and the streets were filled with gambling, drugs, and prostitution rings. Currently, the environment has changed. The gang wars that characterized the mid- 1990s in former Soviet Republics resulted in the self-induced extinction of many large Russian syndicates, especially in the east. Today, according to *Jane's Intelligence Review*, the contingent of organized criminals

has drastically increased, but the demographics have changed.

Eurasian and Central Asian gangs control major smuggling operations in the middle of cities, but the commercial infrastructure is largely controlled by Chinese triads. Ethnic gangs from Tajikistan, Kazakhstan, and Chechnya oversee the drug traffic originating in the West that flows into Japan and other areas of East Asia. Though these gangs direct the narcotics operations, they control little else. The triads have moved into the territory from Northeastern China. These gangs control the thriving casino and gaming industry in the region and own an abundance of hospitality businesses. They also prosper from major extortion networks linked to local businesses, as well as the thriving legal and illegal immigrant communities around the cities.

Together, these crime syndicates represent a strong multinational criminal infrastructure centered at the crossroads of an ocean trade route. Some of these groups, like the Chechens, may have links to Islamic militants and help fund their operations. The question remains unanswered whether the nuclear materials that were discovered have anything to do with the regional gangs. However, its presence in the area requires the international community to reexamine the vulnerabilities that exist in the Russian region with the highest per-capita crime rate. *(Combined Dispatches)*

Organized Crime

Achilles Heel: The ATM as a Vehicle for Debit Card Fraud

The automated teller machine (ATM) has become an easy target for fraudsters and a source of vulnerability in the banking industry. At their inception two decades ago, these cash machines were virtually infallible. The first method for debit card fraud consisted of peering over a consumer's shoulder in an attempt to record their personal identification number (PIN). If this procedure was a success, it was then up to the criminal to steal the actual card from the victim.

Today computer science continues to advance at a rapid pace, making widely accessible the technologies that facilitate security breaches in ATM banking. Previously unsophisticated, small-time criminals can acquire this equipment and defraud the banking system on a large scale, often leaving consumers to foot the bill. Most recently, offenders have purchased private ATMs, machines that are often available in convenience stores, gas stations and a multitude of retail businesses. The market for private ATMs does not undergo much regulation—acquisition of a machine does not even require a criminal to show a legitimate driver's license.

Ownership has its privileges because once in possession of the ATM, criminals can add a "skimming" apparatus before the machines are used in stores. These devices record bank account information for all ATM clientele who use the machine. The culprit is left with the information necessary to replicate the plastic bankcard. The machines used to recreate the card are often available for under $200. Then, equipped with the user PIN, the criminal is ready to use the debit card. Other similar cases of ATM fraud have been carried out on commercial banks' teller machines.

A single operation can provide information on thousands of card owners, and unlike instances of credit card fraud, victims find it difficult to prove to their banking institutions that they did not make the withdrawals themselves. The financial services industry admits that it suffers losses, but it claims that they are manageable. Meanwhile this form of fraud has spread from North America to Southeast Asia to the Middle East. *(Combined Dispatches)*

Smuggling in Central Asia: States Go it Alone in the Race against Criminal Adaptation

Central Asian economies are sagging beneath the economic losses incurred from smuggling, and it appears that efforts to curb these shadow economies will likely be moot in the long term. In a new strategic era characterized by asymmetric warfare, the international community seems to have forgotten that smuggling may present its largest threat to national economies. Not only does illicit trafficking contribute to the proliferation of terrorist weapons and materials, but the movement of alcohol, tobacco, petroleum products, medication, and other contraband deteriorate the economic infrastructure in poorer nations, such as Uzbekistan,

Kazakhstan, and Kyrgyzstan. In this geographic region, it has done so for years.

Central Asian countries have fostered efforts to eliminate smuggling within their own borders, but in the face of criminal innovation, success is unlikely without interstate cooperation. Kyrgyzstan, for example, has created domestic antismuggling legislation. These policies have not delivered optimal success in the short term and are even less likely to work in the future. Specifically, the Kyrgyz government has passed legislation decreasing excise taxes on gas and diesel fuel in an attempt to compete with the price of the same items being sold on the black market. These policies lowered the gas tax by 50 percent and diesel by 37.5 percent. The Kyrgyz government also passed antismuggling laws that expand the duration of prison sentences for convicted smugglers.

These policies have brought mixed results. The amount of gasoline sold legally has tripled, and there has been a 34 percent rise in the production of domestic vodka. However, there are also reports stating that close to 50 percent of beer and wine, as well as 38 percent of vodka purchases, take place on the black market. The new legislation has not overcome the problem, partially because of apathy—there is a lack of accountability between states in the region. Liquor production facilities are almost entirely based in Kazakhstan, although most of the alcohol produced there is sold outside of the country. If Kyrgyzstan is to put an end to this cross-border smuggling, it will need the cooperation of the Kazak authorities. As Kazak markets are not plagued by the sale of black market liquor, it has little motivation to help its neighbor. Moreover, major smugglers in the region have found it useful to hire impoverished couriers from the frontier regions who are willing to take greater risks carrying the contraband, even in the face of harsher punishments. In many instances the courier provides anonymity because he or she will not know the name of their employer. Even in instances where law enforcement can make a difference, there is often widespread corruption among government officials who take as much as 30 percent of smugglers' proceeds.

At a recent meeting of the Central Asian Cooperation Organization (CACO), its members agreed that information sharing and joint operations were critical if terrorism is to be eliminated in the region. The group did not focus on antismuggling initiatives. Even as each suffers from the toll of black markets, there is no collective reaction dealing with that aspect of security. *(Eurasianet)*

Cyber Terrorism

Hackers Come Together, Testing Cyber-security Capabilities in "Root Fu" Cyber-warfare Game

Every year computer hackers gather at a conference in Las Vegas, Nevada, where part of the event's schedule includes a live cyber war between hacker teams. This gathering has taken place for nine years, evolving from an underground phenomenon to a major affair with over 4,000 attendees. Despite varying levels of disapproval emanating from the U.S. government, the annual DefCon conference has proven to be an excellent forum for hackers and security types alike to learn about network defense and hacking.

At the heart of DefCon is the Root Fu contest, in which eight hacking teams meet and match skills in network defense and cyber warfare. This year each team was given its own server running five computer applications. A team's objective was to maximize the running time for each of the five running programs, while their adversaries tried to bring the programs down. Each team engaged in defense, but at the same time tried to hack its opponents. The team with the greatest cumulative application running time at the end of the contest was the winner. Team leader for this year's Immunix team, Crispin Cowan, asserts that "this sort of adversarial testing shows what is possible—and not—with security." He adds that the competition is valued "because [hackers] think it is a better evaluation of security than common criteria."

Many may frown upon Root Fu, but it supports the notion that security professionals need to know how to hack systems in order to protect them. This was very evident a week after the DefCon conference when hundreds of thousands of machines worldwide were hit by the "MSblast" worm and the "SoBig.F" worm, the fastest and most prolific virus to date. According to experts a new version of "SoBig.F" may arrive before the latest version expires in September.

(Combined Dispatches)

Trafficking

Operation Trifecta: A Giant Purge of Mexico's "Narcotraficantes"

A task force consisting of U.S. and Mexican federal agencies brought Mexico's Zambada-Garcia drug empire to its knees in an operation culminating an 18-month organized crime investigation. Operation Trifecta has resulted in the indictment of Ismael Zambada-Garcia and two of his most senior officers for conspiracy to import and distribute cocaine. The three men are accused of respectively distributing 23, 1,003 and 1,770 kilograms of cocaine in California, New York–New Jersey, and Chicago. The narcotics trafficking organization is known for its wide distribution of cocaine, marijuana and methamphetamines. The operation alone ended with the seizure of 11,759 kilograms of cocaine, 24,409 pounds of marijuana, and almost 108 pounds of methamphetamines. In addition, authorities charged over 175 suspects in the United States and Mexico and subsequently launched a wave of 650 Mexican federal agents into Tijuana to smother remaining criminal elements associated with the Zambada-Garcia operation, along with corrupt local officials.

Originating from the Central-Western Sinaloa and Nayarit states, the Zambada-Garcia organization holds its greatest power along Mexico's west coast. The cartel concentrates on the drug market in the United States, using multiple modes of transportation to smuggle narcotics into Los Angeles, Chicago, and New York. Ismael Zambada-Garcia's organization was designated a Consolidated Priority Organization Target (CPOT) by the U.S. Justice Department, indicating that the cartel was considered one of the greatest transnational organized crime threats to the United States. *(Combined Dispatches)*

Interdiction Program against Illegal Trafficking: North Korea Cited as Country of Concern

Eleven countries will participate next month in maritime exercises led by the United States and Australia as part of the Proliferation Security Initiative (PSI), established in May of this year. The goal of the initiative is to intercede in the trafficking of weapons of mass destruction, delivery systems, and other illegal contraband to and from state and non-state actors. Eleven countries currently participate in the initiative: the United States, Britain, France, Germany, Italy, the Netherlands, Poland, Portugal, Spain, Australia, and Japan.

Although the program is not focused on any particular country, North Korea has been cited as one country of concern. It is the world's leading proliferator of nuclear technology and missile parts. Three German businessmen, Optronic president Hans Truppel and two of his associates, were recently charged with attempting to illegally export 214 aluminum tubes to North Korea, key components for the centrifuges used to enrich uranium. The men were charged with violating the Military Material Control Law and the Foreign Trade Law. The 22 tons of aluminum tubes were discovered on a French-flagged ship heading for China. German authorities, however, believe the North Korean trading company, Nam Chong Gang, ordered the tubes.

Earlier this month, a North Korean freighter, *Be Gae Hung*, was discovered by Taiwanese authorities to have 2,000 tons of aluminum materials and 40 tons of phosphorus pentasulfide, a toxic component used for producing chemical weapons.
(Combined Dispatches)

This update is produced by the Transnational Threats Initiative at the Center for Strategic and International Studies (CSIS) and provides monthly news on terrorism, drug trafficking, organized crime, money laundering, and other transnational threats.