CSIS

TRANSNATIONAL THREATS UPDATE

Volume 1 • Number 10 • July 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

Osama bin Laden Receives Accolades from Carlos the Jackal, Incarcerated Mastermind Terrorist

Imprisoned in France since 1994 for 3 murders, Carlos the Jackal has published a book on "revolutionary Islam," extolling Osama bin Laden's successes. One of the most infamous terrorists of the 1970s and 1980s, the Jackal—Illich Ramirez Sanchez of Venezuela—has called bin Laden an exemplary "shining" figure and refers to the September 11, 2001, attacks as a "lofty feat of arms."

The Jackal was known as a ruthless "terrorist for hire" and has worked for President Assad of Syria, Mu'ammar Qadhafi of Libya, Fidel Castro of Cuba, George Habash and the Popular Front for the Liberation of Palestine (PFLP), the Italian Red Brigade, Colombia's M-19 Movement, the Baader-Meinhof Gang, Saddam Hussein and various other "communist and socialist" employers. He was an exceptionally elusive figure and was not captured until 1994, when a French intelligence team drugged him in Khartoum, Sudan, to bring him back to France for trial.

The Jackal's bloody career as an international terrorist is exemplified by his suspected involvement in the capture of the French embassy at The Hague, the murder of two French intelligence agents, the 1976 kidnapping of OPEC oil ministers in Austria and the 1976 Air France hijacking that led to the famous Israeli Entebbe raid in Uganda. He was also involved in innumerable other bombings and hijackings.

Sanchez converted to Islam after he began serving his life sentence. He links bin Laden's campaign to what he refers to as an "armed struggle" to save Islamic holy sites and the Palestinians. Furthermore, the Jackal believes that the Islamic faith is a "Transnational force capable of standing up to the enslavement of nations." He states that the movement will continue and "from now on terrorism is going to be more or less a daily part of the landscape of rotting democracies." *(Combined Dispatches)*

Russia Proposes Stalinist Tactics for its Internal Security Apparatus in Order to Fight Terrorism

Citizens in Moscow encounter shades of yesteryear as they await domestic counterterrorism measures that could infringe on their privacy and personal security. Concerns of a terrorist presence in Russia are strongly evidenced by a bill under consideration by the Moscow City Assembly that would implement a network of informants throughout the city's 600 districts. The city government has already contracted street and building sanitation workers who have agreed to take on these roles.

Increasing the number of eyes watching for suspicious behavior could prove to be an effective tool to thwart terrorism. Nevertheless, though proponents argue that such a program increases levels of awareness throughout Moscow, others argue that this initiative could lead to the unjustified police brutality and imprisonment that characterized the Stalin era. Supported by both the police force and Moscow's mayor, Yuri Luzhkov, the program could become law in early fall.

In the new security environment Moscow's program is not extreme. The law raises questions about civil liberties, but the initiative takes note of new domestic counterterrorism laws in the United States, Britain, Germany, and other Western states.

New government efforts to make citizens' lives more transparent are controversial and remove varying degrees of legal protection under legislation that covers government enforcement. *(The Guardian Unlimited)*

Jemaah Islamiah and its Terror Courier Service

Jemaah Islamiah (JI), the al Qaeda–affiliated Southeast Asian terrorist group, uses transnational couriers to carry documents and money to support its operations. The organization has recruited a network of individuals who travel to Indonesia from abroad. In many cases they are returning Indonesians who sought employment in the Middle East or other countries; in most instances they are unaware of any connection to JI. The couriers accept small cash "donations" from foreign donors, agreeing to bring the money to charities and other needy social institutions in Indonesia. The carriers deliver to their final destination without the knowledge that the money will be funneled to the terrorist group. The consignments are typically small, no greater than a few thousand dollars.

JI also uses more advanced methods to move these items, such as hawala transfers and money laundering. However, the group continues to utilize the more antiquated courier system because it remains effective, even in a heightened security environment. Ordinarily the authorities do not search all the possessions of returning co-nationals. In a case where there were such a search, law enforcement officials would find it difficult to distinguish between the courier's own money and the "illegal" funds he was carrying on behalf of the terror network. *(Combined Dispatches)*

UK Nuclear Power Plants' Security Breached

Infrastructure at an unspecified number of Britain's 31 nuclear plants could be at risk after "sensitive" documentation concerning plant security was officially declared missing. Authorities fear that this information could aid terrorists in an attack on the country's critical infrastructure. The government has admitted that in the past year there have been multiple incidents in which critical information has disappeared. Britain's Office of Civil Nuclear Security (OCNS), in charge of protecting the government's nuclear facilities from terrorist attack and other forms of sabotage, disclosed that two "protectively marked documents" with critical security information were gone. In a separate instance, an officer at a nuclear company discovered that his laptop had been stolen from his hotel room in London. The computer stored information that could endanger security at undisclosed nuclear sites. OCNS will not specify which plants could be compromised if the information were in the wrong hands, but two locations—Sellafield in Cumbria and Dounreay in Caithness—have been labeled "high risk." Consequently, in the past year the government has spent £55 million securing each location. *(Combined Dispatches)*

Defending Airborne Commercial Jets from Terrorists

After September 11 and a failed terrorist attack on an Israeli passenger jet using shoulder-launched surface-to-air missiles, the Department of Homeland Security has emphasized that the civil aviation industry faces yet another terrorist threat. The defense industry is heavily engaged in research and development on missile defense to thwart the threat of these man-portable air defense systems (MANPADS). Although these defenses are intended for military use, many speculate that they will also be utilized to protect commercial aircraft in the future.

In response to the growing threat, aviation defense contractor Northrop Grumman has designed the Hazardous Ordnance Engagement Toolkit (HORNET) ground-based laser defense. The system is intended to defend aircraft from MANPAD attacks, especially those taking place when a plane is taking off or landing. The HORNET system will use a high-intensity deuterium-fluoride chemical laser that can intercept and jam the guidance systems in heat-seeking missiles. This system has been designed to work in conjunction with airborne passive countermeasures, such as flares or chaff launched from the commercial aircraft itself.

There are approximately 500,000 to 700,000 MANPADS throughout the world. The most common missiles are American Stingers, and Russian Strela and Igla missiles. An unknown but formidable number are in the hands of terrorist organizations. In the 1980s the United States armed the mujahideen in Afghanistan with an estimated 400 to 900 missiles. In the aftermath of the Soviet campaign, the CIA launched a $60 million MANPAD buyback program, offering the mujahideen fighters $30,000 per missile. The program saw little success. Only 70 missiles were returned. *(Combined Dispatches)*

Cyber Terrorism

A Critical but Unclassified Blueprint for the Cyber Terrorist is in the Public Domain

A computer science Ph.D. candidate at George Mason University has accidentally developed an invaluable tool for terrorists. Sean Gorman has mapped fiber-optic networks for all business and industrial sectors throughout the United

States. An innovative mix between cartography and telecommunications, this project could become a doorway to a devastating terrorist attack on the country's critical infrastructure. The project is so comprehensive that its greatest limitations would likely be the mind of its user, rather than the program itself. Currently, George Mason University is treating the information as a sensitive matter and prohibiting its public exposure in the media. However, the university and the scientist are not bound to secrecy, as the project is not classified.

With Sean Gorman's dissertation, a saboteur could use the computerized map to find any number of vulnerabilities in the country's cyber infrastructure. For example, a cyber terrorist or a cyber criminal could select a specific bank in Manhattan; then the diagram could be manipulated to identify what companies run communications lines through that bank. Gorman's maps could also allow a user to find the optimal point to sever crucial fiber-optic cables linking two states, or even center on a particular U.S. city and mark the telecom "choke points" for the city's trucking warehouses.

The project has attracted attention in the post–September 11 environment, as it is highly relevant to building security. The controversy surrounding Gorman's creation also highlights new questions regarding the public right to information and the dangers that may accompany these liberties. Although of great use to those who are devising defense strategies, this same information threatens the government, the business sector, and the privacy of consumers themselves.

Thus Gorman's case falls into ongoing slippery-slope argumentation. What is too sensitive, and what is acceptable? The computer scientist has no rebellious intentions, but his project could still have serious repercussions. *(Washington Post)*

Narcotics Trafficking

Counterfeiting…Medication?

The pharmaceutical industry has become a new arena for criminals who illegally duplicate medication and subsequently distribute it to the public. As counterfeiting operations have become more sophisticated with the evolution of imaging and graphics technologies, as well as Internet access, organized crime groups have been able to replicate the appearance of packaged medications. In certain cases the active ingredients are included in the counterfeit samples, but in many other instances consumers end up ingesting medications that have either minimal or dangerous effects, or no content at all. The World Health Organization estimates that approximately 8 percent of medications circulating throughout the world are counterfeit, while in poorer nations the figure can be as high as 25 percent. These drugs find their way to pharmacies via intermediary criminal sources. The problem surfaces most in the new market for online mail-order medications. Experts estimate that 14 percent of drugs arriving through the mail have defects. *(U.S. News & World Report)*

CSIS Speaker: Ronald K. Noble, Interpol Secretary General

Secretary General Ronald Noble of Interpol visited CSIS on July 17, 2003, to conduct a breakfast meeting sponsored by the Transnational Threats Initiative (TNT). Interpol is based in Lyon, France, and counts 181 member countries. Notably absent is North Korea, along with Turkmenistan and Tajikistan. Interpol's annual budget is $31 million with headquarters staff numbering 400 people from 60 nations. At CSIS, Mr. Noble spoke to various representatives of think tanks, private-sector firms, the U.S. government, and foreign embassies. Earlier in the week, he spoke to the American Bar Association's Standing Committee on Law and National Security and testified before the House International Relations Committee on the threat of intellectual property crime (IPC) and its connection to terrorism.

Mr. Noble gave a brief overview of Interpol and its interaction with other law enforcement agencies. He then spoke about the threat of bioterrorism, placing particular emphasis on educating law enforcement and intelligence communities on what is the most serious potential terrorist threat to society. Mr. Noble also addressed the convergence of organized crime and terrorism, specifically intellectual property crime (IPC) and terrorist financing. IPC is defined as the counterfeiting or pirating of goods for sale where the consent of the rights holder has not been obtained. Mr. Noble warned that IPC is becoming a preferred method of funding for many terrorist groups, as it is a low-risk/high-return crime. He also stated that it is not a victimless crime. Groups such as the Irish Republican Army (IRA) and the Kosovo Liberation Army (KLA) are two notable examples of this phenomenon. Mr. Noble emphasized the importance of information sharing among law enforcement agencies, as well as tracing the proceeds of counterfeiting, rather than simply seizing the goods and arresting those involved.

Following is a summary of Mr. Noble's testimony on Capitol Hill, July 16, 2003

"The Links Between Intellectual Property Crime and Terrorist Financing"

- Interpol—sounding the alarm that IPC is becoming preferred method of funding for many terrorist groups. In general, law enforcement does not treat IPC as high-priority crime.
- Law enforcement agencies must recognize that IPC is not a victimless crime, as terrorist groups use IPC proceeds to fund activities.
- Examples of IPC and terrorist financing:
    - Northern Ireland: paramilitary groups involved in IPC.
    - Kosovo: a significant proportion of consumer goods are counterfeit. There is long-standing relationship between criminal organizations and local ethnic Albanian extremist groups.
    - Chechen separatists: a counterfeit CD plant was a source of financing for Chechen separatists.
    - North African Radical Fundamentalist Terrorists in Europe: sympathizers pass proceeds from IPC in form of charitable giving or zakat (charitable giving based on religious obligation in Islam). Fundamentalist militants support themselves through IPC or credit card fraud while not on active service duty.
    - Al Qaeda: investigation into shipment of fake goods from Dubai to Copenhagen, Denmark, suggests Al Qaeda may have indirectly funded activities through counterfeit goods. Sender of counterfeit goods was allegedly member of Al Qaeda.
    - Hizballah: Interpol is aware of three cases of IPC-related activity and terrorist funding in South America. These cases involve ethnic Lebanese who are involved in remittance of funds to Hizballah.
- IPC is likely to become a more important source of financing for terrorist groups because it is low risk/high return. IPC is low priority for law enforcement compared to illicit narcotics or counterterrorism investigations. One estimate of IPC returns: 10 euros for each euro invested.
- Interpol should coordinate international action against IPC through Interpol Intellectual
  Property Crime Action Group (IPCAG). Interpol proposes three-year private/public IP crime program with aim of developing private/public IP crime partnership.

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.