2010 007

DEFENSE THREAT REDUCTION AGENCY
Scientific & Technical Review Information

PA CONTROL NUMBER:	10-216 PA 9-Apr	SUSPENSE:	May 9, 2010
PM / PHONE / EMAIL:	Amber Stewart 767.6355	DATE:	Apr 9, 2010
BRANCH CHIEF / PHONE /EMAIL:			
DIVISION CHIEF / PHONE:		DATE:	
DIRECTORATE / DIRECTOR /PHONE	Rob Gregg 767.5707	DATE:	
ENTERPRISE / OFFICE / PHONE:		DATE:	
PUBLIC AFFAIRS:	CLEARED AS AMENDED		14 APR 2010

1. TTLE: Criminal Networks, Smuggling, and Weapons of Mass Destruction — CONTRACT NUMBER: DTRA01-03-D-0017

ORIGINATOR: TTCCC, GMU School of Public Policy; ASCO Oscar Vaughn

2. TYPE OF MATERIAL: [X] PAPER [ ] PRESENTATION [ ] ABSTRACT [ ] OTHER

3. OVERALL CLASSIFICATION: [X] CONTRACTOR Unclass [X] PROJECT MANAGER Unclass

A. Review authority for unclassified material is the responsibility of the PM. Your signature indicates the material has undergone technical and security review. [ ] FRD [ ] CNWDI [ ] NATO RELEASABLE

B. Warning Notices/Caveats: [ ] RD [ ] SUBJECT TO EXPORT CONTROL LAWS

CLEARED AS AMENDED for public release

APR 14 2010

Public Affairs
Defense Threat Reduction Agency

C. Distribution Statement:

[X] A. Approved for public release; distribution is unlimited (unclassified papers only).

[ ] B. Distribution authorized to U.S. Government agencies only; (check the following):
- [ ] Contractor Performance Evaluation
- [ ] Foreign Government Information
- [ ] Administrative or Operational Use
- [ ] Specific Authority
- [ ] Premature Dissemination
- [ ] Proprietary Information
- [ ] Test and Evaluation
- [ ] Software Documentation
- [ ] Critical Technology

[ ] C. Distribution authorized to U.S. Government agencies and their contractors: (check the following):
- [ ] Critical Technology
- [ ] Specific Authority
- [ ] Administrative or Operational Use
- [ ] Software Documentation
- [ ] Foreign Government Information

[ ] D. Distribution authorized to the Department of Defense and U.S. DoD Contractors only; (check the following):
- [ ] Foreign Government Information
- [ ] Critical Technology
- [ ] Administrative or Operational Use
- [ ] Software Documentation
- [ ] Foreign Government Information

[ ] E. Distribution authorized to DoD Components only; (check the following):
- [ ] Administrative or Operational Use
- [ ] Premature Dissemination
- [ ] Critical Technology
- [ ] Foreign Government Information
- [ ] Direct Military Support
- [ ] Software Documentation
- [ ] Specific Authority
- [ ] Proprietary Information
- [ ] Test and Evaluation
- [ ] Contractor Performance Evaluation

[ ] F. Further dissemination only as directed.

[ ] G. Distribution authorized to U.S. Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25 (unclassified papers only).

OPSEC - APPROVED [illegible] 13 APR 10

4. MATERIAL TO BE: [ ] Presented [X] Published Date Required: 9 May

Name of Conference or Journal:

Remarks: To be distributed to conference participants, and through DoD and DoS channels

Criminal Networks, Smuggling, and Weapons of Mass Destruction

Conference Report

The Terrorism, Transnational Crime and Corruption Center
George Mason University School of Public Policy

March 2010

Defense Threat Reduction Agency
Advanced Systems and Concepts Office
Report Number ASCO 2010 007
Contract Number DTRA01-03-D-0017, T.I. 18-09-05

Criminal Networks, Smuggling and Weapons of Mass Destruction Conference Report

Background

The Terrorism, Transnational Crime and Corruption Center (TraCCC) at George Mason University's School of Public Policy held a two-day conference on February 25-26 2010 to address major challenges facing Weapons of Mass Destruction (WMD) policymakers. The conference, sponsored by the Defense Threat Reduction Agency's Advanced Systems and Concepts Office (DTRA/ASCO), brought together diverse global experts from government, academia, journalism, and the private sector to examine the problems of WMD proliferation, nuclear smuggling, and the links between criminal and terrorist networks. This report provides key findings from the conference. Following Chatham House rules, the names of speakers are not identified. This report was prepared by Dr. Louise Shelley, Director of TraCCC, and Ms. Alison Rea, a research assistant at TraCCC.

Key Observations

- The threat of nuclear terrorism must be taken more seriously given the growing sophistication of terrorists in obtaining funding, applying technology, and utilizing criminal networks. Lessons learned should be applied to combating biological threats as well.

- Understanding links between criminals and terrorists and identifying and tracing their fast-changing networks is crucial to setting effective policy and implementing prevention and detection strategies. Analysis of actual cases is essential to understanding the threat.

- Nuclear smuggling travels the same routes as drugs and other illicit commodities. The expanding links between criminal networks in regions such as Latin America and West Africa raise the possibility that nuclear smuggling could become more widespread.

- Criminals are involved in the trafficking of nuclear materials, and many nationalities are represented among the traffickers.

- The lessons of the A.Q. Khan network have not been fully implemented. There is still the possibility that a state-supported WMD network could engage in this trade.

- Technology alone is not sufficient to detect and deter nuclear smuggling, but must be combined with action based on careful intelligence and footwork by law enforcement and on findings from independent field research.

- Efforts by the U.S. government to combat WMD and nuclear smuggling are hampered by a lack of cooperation and coordination between different agencies, which have a history of operating from competitive stovepipes.

- Global efforts to fight WMD and nuclear smuggling are similarly hampered by jurisdictional disputes between law enforcement groups in different countries and by a lack of communication and cooperation across borders.

- Training law enforcement to be more aware of WMD smuggling and the methods to fight it is critical to making progress. Regional training centers should fill a critical need in bringing together people and skills from different countries, government entities, and areas of expertise.

Terrorism and Transnational Crime

The conference began by discussing the "unholy trinity" of terrorism, transnational crime, and corruption. Not only do terrorists and transnational criminals thrive in corrupt environments, but terrorists can use widespread corruption to promote recruiting, as is currently the case in Afghanistan. Terrorists increasingly are using crime to fund and facilitate their activities. Presentations revealed the increasing professionalism of some criminals as they gain experience and sophistication in smuggling, using technology, and evading technology-based countermeasures such as nuclear detectors. Some arrested smugglers have developed their skills over time.

Panelists concurred that illicit networks can consist of criminals and terrorists as well as corporations that deliberately participate and sell commodities, sometimes as front companies for states or non-state actors. Facilitators can include officials of all levels, as seen in Pakistan (high-level officials) and Georgia (low-level officials). Illicit networks are increasingly transnational, reflecting changes in crime itself. Newer crime groups tend to have shorter-term financial horizons and fewer ties to existing state and economic structures, making them more likely to consider favorably the quick profits to be gained from smuggling high-risk materials than older, hierarchical, mafia-style organized crime groups. Such groups tended to focus more on generating consistent, steadier profits through relatively low-risk activities.

Newer criminal networks favor conflict regions, areas of "frozen conflict", and territories outside of central state control, such as the Caucasus, Afghanistan, Waziristan, Nepal, Sri Lanka, Sierra Leone, Pacific Islands, and the Amazon region. These networks thrive on the absence of effective governance and grow as states become weaker.

Terrorist networks connect with and exploit the legitimate world by using existing transport systems and establishing seemingly legitimate businesses to facilitate terrorist activity and the pursuit of WMD. Cell phone and computer stores have widely served as cover for illegal pursuits in Turkey. WMD networks commonly have access to legitimately produced commodities used as materials for terrorist attacks, such as fertilizer.

The consensus among experts at the conference was that WMD smuggling operates through the same routes as the drug trade and coincides with other forms of smuggling – illicit arms, antiquities and human trafficking – as evidenced by confiscated materials. The transfer of undeclared amounts of money across borders is rife, as is the use of professional thieves and counterfeiters to help spirit nuclear and biological materials around the globe. Understanding the range of networks, their activities in relation to one another, and their links to past terrorist attacks are as important to disrupting potential attacks as is following the crime footprint to penetrate individual networks.

Evolving Alliances Among Unlikely Networks

The conference highlighted the dangers posed by the evolution of unlikely partnerships between criminal and terrorist networks from disparate regions such as Latin America, Africa, and Iran. In the past, these relationships were not well-developed.

Latin America was spotlighted. Here, new corridors are being cleared for the flow of illicit commerce, including, potentially, WMD. The oldest insurgency group, Colombia-based FARC, is believed to be expanding its narco-terrorist reach into Ecuador, Bolivia, and Venezuela, and is doing more business directly with Mexican drug cartels. FARC's increasing focus on profits over ideology could easily propel its expansion into the highly-profitable WMD trade. FARC exemplifies the new links being forged between disparate and far-flung terrorist groups both from within Latin American and from outside the area. FARC, under the alleged aegis of Venezuela, is working to build stronger ties with terror groups such as the Basque ETA, the Irish Republican Army, Peruvian groups, and Hezbollah.

Growing Iranian links with Latin America were also highlighted. Many panelists expressed concern about Iran's true motives in deepening diplomatic and commercial relations with a number of regional players, including Venezuela and Nicaragua, especially in light of the fact that an active pipeline is already in place to smuggle cocaine and humans between Latin America and Iran. This pipeline is a source of concern as it could be used to smuggle virtually anything, given Iran's continuing effort to acquire nuclear weapon-making materials, its global illicit procurement network, and its possible interest in sharing nuclear technology.

West Africa is another area where the rise in illicit-network connections could easily be exploited for WMD-related smuggling. A cocaine pipeline has developed between West Africa and Latin America, with terrorist training camps receiving Colombian drug shipments allegedly from Lebanon-based Hezbollah, which is supported and subsidized by Iran.

In both Latin America and West Africa, there is rising concern about overlapping bad actors with overlapping sponsors. Fueled by cocaine profits, illicit networks are likely to grow in these regions and potentially could forge links with existing Islamic terror groups. While direct ties may be not yet be fully documented and exposed, there is troubling evidence of connections between criminal and terrorist groups that could increase WMD risk. In this regard, it is worth noting that Venezuelan President Hugo Chavez has expressed

sympathy with and integrated into Venezuelan military doctrine concepts of asymmetric warfare and terrorism that highlight the use of nuclear, chemical, and biological weapons. [1]

Evolving Networks in Well-trafficked Zones

The crime-terror nexus is not static even in zones, such as much of the Middle East, Afghanistan and the Caucasus, where criminal and terrorist activities have been long entrenched. These areas are ideally situated to capitalize on already established transit routes for illicit goods, including WMD, and serve as breeding grounds for terrorists whether motivated by religion or not.

Particularly at risk for harboring criminal-terrorist networks are countries, like Georgia, that exhibit many of the characteristics that foster new-style criminals. These traits include insecure borders, high levels of corruption, conflict zones, and criminal groups well-versed in smuggling. Further, Georgia's proximity to NATO-border states and its role as a trade hub make it particularly vulnerable to criminal trade. Also of concern is the presence of more than 350 former Soviet military bases and installations, many of which are thought to have contained radioactive materials of some type. Arrests of serious WMD smugglers point to the importance of the threat.

Al Qaeda remains active in much of the Middle East, Pakistan, Waziristan, and Afghanistan. Organizations and movements in Turkey connected to WMD smuggling and to al Qaeda WMD plots were described as meticulously organized, adept in the use of sophisticated technology, and dependent on criminal facilitators. Smugglers of nuclear materials were agile in using illicit conduits originally set up for other types of smuggling, including drugs, human beings, cigarettes, and arms. In Turkey, sophisticated police work has been used to disrupt both nuclear smuggling and threats from al Qaeda.

Emerging Cyber Network Threats

The rising technological sophistication of criminal and terrorist networks is exemplified by cybercrime attacks on computer systems of individuals, governments, and corporations. Cyber criminals are devising new and ever harder-to-detect lines of attack that have the potential to create very tailored or large-scale effects. They do this in a variety of ways, using such stratagems as malware, botnets, and spear-phishing with malicious payloads. Primary attack vectors include operating systems, web applications, and wireless

[1] Chavez has adopted *Guerra Pereferica y el Islam Revolucionario: Origenes., Reglas y Etica de la Guerra Asimetrica* (Peripheral Warfare and Revolutionary Islam: Origins, Rules and Ethics of Asymmetrical Warfare) by the Spanish politician and ideologue Jorge Verstrynge. According to one of the conference participants, Verstrynge writes extensively in this book on how to produce chemical weapons and provides information sources on the manufacture of rudimentary nuclear bombs. He refers to "super terrorism" as an aspect of asymmetrical warfare involving chemical, biological, and nuclear threats.

networks. Cloud computing, in which information lives in cyberspace rather than on hard drives, introduces major systemic vulnerabilities that criminal networks already well-versed in defeating most security and anti-fraud measures will be capable of exploiting.

As with other illicit activities, cybercrime is transnational and features alliances between networks of cybercriminals and malware developers. Nation states and non-state actors with political objectives are believed to be complicit in some cybercrimes; the recent attempt, allegedly by Chinese hackers with ties to the Beijing government, to steal source code from Google and a number of other large U.S. companies is an example. Non-state criminal and terror organizations use the Internet freely for recruitment, propaganda communication, financing, money laundering, and as a method of attack.

Cyber crime is generally mundane and includes identity theft, brokerage fraud, market manipulation, and money laundering. Common targets are credit card and other consumer information that can be used to steal money directly or sold to other criminal networks. However, access to banking information can provide a terrorist organization with a major funding source.

Smuggling Behavior

WMD smugglers usually use trade routes that have already been established for other illicit goods, such as drugs. It was suggested that these routes have been changing over time. As an example, WMD-related interceptions by Turkish authorities show that since 2001, WMD trafficking has been routing south from Russia to Iran or through Iran to Jordan or Turkey and beyond, whereas before 2001, such smuggling was seen going directly westward from former Soviet territory to Europe or moving south via Turkey to Iran or Central Europe.

Detected cases reveal a significant overlap between groups involved in contraband in illicit goods and groups involved in radiological smuggling. Criminal facilitators for this type of smuggling are commonly used, though they may not be aware of the entire logistical chain or even what is being smuggled. However, smuggling groups are not always large. In Georgia, for instance, most smugglers engage in *ad hoc*, single-deal transactions, sometimes in partnerships or in collaborations based on family or friendships. These do not constitute an established organized crime group.

Cases in Georgia and elsewhere also suggest that members of organized crime groups tend not to be involved in the smuggling of items directly related to weapons of mass destruction. They view this "market" as uncertain and unstable as a source of regular income, and fear that involvement in such activities would harm their more traditional and lucrative criminal enterprises, e.g., by damaging relations with corrupt government bureaucrats and others who operate in the legitimate worlds of government and commerce, or by inviting sharper law enforcement scrutiny.

Indeed, it was not professional criminals but engineers and businessmen who created the most significant and sophisticated black market in WMD-related materials and technologies. The A.Q. Khan network working out of Pakistan and several other countries

operated at the level of a state enterprise, regardless whether it was sanctioned by the leaders of Pakistan. This network did business directly with other governments. One persistent concern is the risk of illicit WMD trade as a matter of state policy by so-called rogue countries will eventually involve terrorist groups who could gain access to highly-destructive materials and technologies.

Countering Crime-Terror-WMD Networks

Are the right approaches and tools being marshaled to combat illicit criminal and terrorist networks? Approaches that are highly dependent on technology were viewed as incomplete. For example, discovery rates of highly-enriched uranium (HEU) remain low partly due to over-reliance on electronic radiation portal monitors, which often fail to detect HEU and experience high false alarm rates on items such as bananas, cat litter, and concrete. Criminals often know where detectors are and how to dismantle or bypass them. Conference participants advocated more human-based solutions involving intelligence-led policing, use of informants, and infiltration operations. Turkey was noted as having been particularly successful using these methods to detect and disrupt criminal and terror activities.

Conference participants also expressed the belief combating transnational crime and illicit trafficking requires more and better qualitative field research, and that exploitation of knowledge acquired from field work and case studies was a key element in improved WMD smuggling prevention. More input by those with first hand experience combating WMD trade would help draw a clearer picture of how crime and terror networks operate, where supply and demand are for WMD, and the degree to which current policies are working.

More vital is breaking down the institutional barriers that inhibit cooperation among agencies in the U.S. government and collaboration between states across borders. Issues of national sovereignty can complicate the coordination of information flows and law enforcement activities. However, just as criminals, terrorists, and WMD smugglers increasingly operate in transnational networks that affect multiple countries, governments and international organizations must cooperate in systematic and structured ways to share information, strategies, and best practices.

Policy Implications

- Policymakers need to understand how criminal-terrorist networks behave, how pipelines operate across borders and continents, and how sophisticated technologies are being marshaled to assist WMD trafficking. Some regions of the world may require closer attention than given in the past. Law enforcement needs to be used to greater effect in combating illicit networks. Models of effective action based on experience and analysis need to be developed, studied, and promoted. Such models will have as their centerpiece robust information sharing and effective coordination at all levels – within governments, between governments, and across government and non-governmental sectors.

- Closer collaboration between field researchers, academic experts, and law enforcement and intelligence agencies is required, especially as the basis for developing long-term strategies. Strategies and policies focused on WMD smuggling should stress intelligence gathered through on-the-ground research and granular police work, and should avoid overemphasizing technology solutions. In governments, maintaining artificial distinctions between crime and terrorism analysis is counterproductive. In all cases, it is important to "follow the money."

- Improved international cooperation should include more advanced communications and information-sharing practices, and transnational training programs for law enforcement and military units. Additionally, the international community must focus greater attention on corruption, poor governance, and lack of transparency, which feed or enable crime, terrorism, and illicit trafficking.

- The risks associated with nuclear smuggling in particular can be addressed in part through ongoing efforts to "lockdown" nuclear-weapons related materials worldwide, and to criminalize illicit WMD trade. But this may have less impact on the availability of radiological materials that could be used in dirty bombs.