THE FUND FOR PEACE

THREAT CONVERGENCE

Summary Report: Planning Workshop April 2006

THE FUND FOR PEACE

Threat Convergence: Possible New Pathways to WMD Proliferation?

Background Paper on Threat Convergence Workshop Convened in April 2006

Project Description

Threat Convergence refers to the dangers emerging from the confluence of weak and failing states, terrorism and WMD proliferation. No longer bound by the rules of a system of states, criminal and illicit networks flourish in the facilitative environments of ungoverned spaces, cultural enclaves in strong states, and in weak and failing states (hereafter referred to as WFS). These networks of terrorists, criminals and traffickers, and the volatile settings that enable their activities, create an entirely different world from that which was originally envisioned by the crafters of WMD policies and institutions.

The Fund for Peace initiated the Threat Convergence Project to explore how ongoing work in the fields of terrorism, WMD proliferation, and WFS can be integrated to address this emerging global threat. This summary paper highlights the ideas generated by leading experts during an April 2006 mapping workshop, convened to promote information exchange on alliances, networks and other pathways that could lead to a catastrophic terror attack. Workshop participants also laid groundwork for scenario development and provided guidance on a multidisciplinary research agenda that will follow a larger conference in Warrenton, Virginia in November/December 2006. This paper summarizes and highlights some of the major insights and observations of the April mapping workshop.

After considering a number of approaches, workshop participants concluded that a model that considered the "supply and demand" sides of threat convergence, specifically, looking at phases in the chain of events leading to a potential nuclear attack by a terrorist entity, presented the most robust set of comprehensive research questions. This framework looks at the chain of events leading to a potential nuclear attack by a terrorist entity. Examining the "sites" that provide the facilitative environments where threats will most likely converge will both advance learning from past cases and inform scenario planning for emerging and anticipated cases.

Supply

The role of WFS in the Supply Side

Studies of A.Q. Khan's Pakistan-based transnational alliances provide ample evidence that WFS have already played a pivotal role in increasing the risk of terrorist entities gaining access to nuclear technology. Much remains unknown about the Khan network. The current status of Khan's associates is also unknown: while many top-level players have been arrested, they have not been interviewed outside of Pakistan and many lower-level functionaries may still be active. The Pakistan case raises serious questions about the availability of nuclear expertise and technology that could be used by terrorists to construct a nuclear explosive device. There is evidence that al Qaeda members operating in Afghanistan sought bomb designs and had some contact with Pakistani nuclear scientists as well. The present status of the A.Q. Khan network and the role of WFS, like Pakistan and Afghanistan, in nuclear proliferation among terrorist groups provide further opportunities for research.

Trafficking Information and Expertise

Knowledge gaps exist concerning diffusion patterns of technical information relevant to weapons and materiel acquisition and manufacturing, and the means by which technical expertise related to WMD production has or could become available to weapons traffickers. Advancements in centrifuge technology, combined with wider access to digitized technical information and the undetected spread of such information, present a serious challenge.

Trafficking Materials

Most experts believe that terrorist groups are more likely to build a low-tech nuclear explosive device, perhaps signaling their perception of the relative availability of matériel to technology. Researchers attending the mapping workshop expressed serious concern about the amount, quality, and availability of fissile material. Depending upon the design and method of delivery, a nuclear explosive device may require relatively little fissile material, and terrorists could feasibly steal or buy fissile material on the black market or even construct a low-tech plant for reprocessing spent fuel.

Beyond the black market, unsecured state sources of proliferation abound.[1] For instance, according to European intelligence sources, Sudan imported one and a half billion dollars worth of dual-use nuclear equipment over a three year period before 2001, the location of which is unknown. In addition, the Khan network demonstrates the

[1] Please see David Albright's catalogue of fissile material possessing countries in Appendix I

international character of the problem of outsourcing, e.g., the manufacture of bomb or enrichment components to partners in Europe, a reliance on unregulated transit points in the Middle-East, and collection of technological expertise in India.

Supply Chain

Focusing on particular regions or countries that have the attributes of WFS -- including widespread corruption, the lack of government control over territory, porous borders, and the known presence of militias, criminal traffickers or terrorist networks -- is an important starting point when examining the supply side of WMD proliferation. In determining potential state threats, several key countries that were identified as having features of WFS, such as Pakistan, Iran, Russia, and North Korea, also possess civilian nuclear facilities or high-tech industrial resources.

These countries run a significant risk of potential leakage, supplying terrorists with knowledge and matériel, while providing safe havens for their activities. Experts at the meeting emphasized the need to move beyond the mere identification of WFS that possess nuclear fissile matériel and the potential for such states to be used by terrorists intent on acquiring WMD. They recommend instead a focus on how the supply chain to WMD proliferation is actually fed.

Several experts stressed the need to identify potential pathways to proliferation stemming from corruption, e.g., low wages and poor morale among those responsible for securing nuclear facilities. Terrorists could bribe underpaid security guards to gain access to nuclear sites, and take advantage of lax border regimes to traffic materials out of the country. Characterized by symptoms referred to as the "hollowing out of bureaucracy," such countries present a grave risk of becoming suppliers, notwithstanding stated or perceived adherence to nuclear regulatory norms.

Participants noted that one opportunity for future research is to examine the different types of connections necessary for bringing together the disparate elements of a successful nuclear attack by a terrorist organization. These components include official and unofficial financial transactions, technical expertise, and logistical and ancillary networks. The United States, and the international community as a whole, must first explore *who* participates in predatory enterprises, *where* criminal networks might be collaborating with terrorists, and *how* such networks have spread and continue to evolve.

Demand

The role of WFS in the Demand Side

The steps necessary for terrorists to build and subsequently deploy a nuclear weapon, including matériel and technology acquisition, establishing a safe haven, constructing an explosive device, acquiring access to a target, and, finally, acquiring a method of delivery, may not necessarily unfold in a sequential manner. These events may be happening simultaneously. While studying the various phases of the supply chain can

offer direction for information analysts, equally important is the identification of likely perpetrators, their motivations, connections, resources, and perhaps, most importantly, the directions in which they will evolve.

Network Evolution

Terrorist motivation, action, and direction cannot be understood solely by deconstructing the behavior of lone actors. Analysis of grand societal and situational themes is equally hard to translate into actionable information. Patterns with probative and predictive value begin to surface at the "meso-relational" level of analysis, which focuses on *the relationships among actors* involved in terrorist groups. For example, the perpetrators of the March 2004 bombings of Madrid passenger trains were recruited by al Qaeda loyalists through mosque connections while criminal connections provided the means to acquire the dynamite used in the attacks.

Such complex and often surreptitious dynamics of network evolution stretch the capacity of traditional terrorism and WMD analyses. The Madrid case was localized; similar network evolution, entailing connections and sanctuary for actors in WFS, could facilitate a catastrophic attack. Too many unknowns remain regarding the nationalities, mobility, actions, and communication preferences of individuals involved in terrorist networks. Moreover, network functioning may differ in its instantiations in a country or enclave. In addition, a “disconnect” exists between local, on-the-ground actors and large, transnational agencies or corporations, such as international charities or banks, which could provide assistance to terrorist entities seeking to expand their reach through existing channels.

Capabilities

An open-classification assessment of terrorist group capabilities could produce insight into how terrorists are collecting information and how their network is arrayed, allowing for inferences regarding a group’s tactical intentions. The difference between hard capabilities (matériel, weapons, and equipment) and enabling capabilities (money laundering, safe havens) presents further refinement of this theme. Cross-referencing a potential catalogue of matériel and expertise with known and suspected terrorist capabilities could inform ongoing threat assessment tools and programs.

State/ Non-State Collaboration

There are different degrees of terrorist involvement or penetration of a state, the most severe case being terrorist takeover of state structures. A knowledge gap exists regarding states not traditionally associated with terrorism or WMD issues, but which nonetheless are vulnerable to terrorist exploitation. A state’s inability to imprison a known rogue actor, for example, could indicate a lack of capacity or political will to confront potential terrorist activity on its territory. Thus, the impact of varying levels of stability and government presence in different parts of a state needs to be more thoroughly investigated.

Beyond WFS themselves, ungoverned spaces, separatist regions or remote locations in stronger states can be used not only for constructing WMD, but also for fundraising, planning and logistics, financing operations, and recruitment. The North Caucasus region of the Russian Federation, for example, poses enormous challenges in terms of WFS because the Russian government exerts minimal control over much of this territory. The border region between Pakistan and Afghanistan in South Asia, and between Brazil and its neighbors in South America, illustrate the same concern. Enabling environments within strong states cannot be overlooked. Israel, for example, known for its tough stance on terrorism issues and its efficient security services, is nevertheless weak on organized crime and money laundering, issues of great importance to terrorist networking. Some scholars have speculated that such activities could even take place within target countries, such as the United States.

Conclusion

As the threat of nuclear terrorism evolves across the frontiers of states, this project represents an inquiry of a new kind, evolving across the frontiers of knowledge and integrating well-charted fields of inquiry. Allied with, but not strictly bound to, these knowledge domains, the Threat Convergence project will seek to identify the most likely scenarios for an act of catastrophic terror and provide insights and advice to policy makers to thwart such designs. The experts involved in this workshop outlined the basic dimensions of the problem in terms of the "supply" of WMD technology and expertise, and the "demand" for such weapons by extremists. The task for the November/December conference is to connect the dots.

The emphasis on a systematic analysis of likely "sites" for threat convergence led participants to consider many broad categories of inquiry as well as numerous potential scenarios for possible gaming. A gaming exercise that utilizes the most likely scenarios for terrorists to gain and use WMD in the facilitative environments provided by weak and failed states would be useful to test hypotheses as well as generate directions for future research. Four scenario parameters proposed are: 1) existing groups that have pursued WMD; 2) existing groups that have not yet pursued WMD, but have the potential to do so; 3) hypothetical groups/situations; and 4) state/non-state actor collusion. These scenarios will be considered in the November/December conference. Mapping changes in the evolution of networks will be a primary objective in the gaming phase.

We are taking an approach based on case studies where the triple threats converge, grouping them according to where they fall in the 'supply and demand' chain. Then, we will use hypothetical scenarios to achieve what workshop participants called an "evidence-based situational analysis". With regard to hypothetical scenarios, future research should focus on groups, networks, and locations that have a high potential for action, taking into consideration variance among actual case studies.

Appendix I

Nuclear Explosive Material Holdings by Country, end 2003, in tonnes

Country	***Plutonium***	***HEU***	***Np 237***	***Am***	***Total (rounded)***
Argentina	11	0.020	0.066	0.198	11.3
Armenia	1.4	0	0.097	0.209	1.7
Australia	0	0.35	0	0	0.35
Austria	0	0.005-0.02	0	0	0.005-0.02
Belarus	0	0.25-0.37	0	0	0.25-0.37
Belgium	23.5-24.5	0.70-0.75	1.28	1.742	27.2-28.3
Brazil	2.1	0-0.001	0.060	0.058	2.22
Bulgaria	8.5	0.006	0.595	0.852	9.95
Canada	135	1.35	0.807	2.330	139
Chile	0	0.005	0	0	0.005
China	9.1	22	0.156	0.119	31.5
Colombia	0	0	0	0	0
Denmark	0	0	0	0	0
Czech Republic	6.2	0.08-0.14	0.291	0.362	6.93-6.99
Finland	11	0	0.517	0.839	12.4
France	236.1	33-34.3	9.80	12.9	292-293
Georgia	0	0-0.001	0	0	0-0.001
Germany	93-96	1.4-2.7	4.87	7.67	107-111
Ghana	0	0.001	0	0	0.001
Greece	0	0.003-0.016	0	0	0.003-0.016
Hungary	7.5	0.15-0.25	0.289	0.429	8.37-8.47
India	13.9-14.9	0.005-0.01	0.142	0.290	14.3-15.3
Iran	0	0.007	0	0	0.007
Israel	0.56	0.034	0	0	0.594
Italy	6.5	0.10-0.20	0.096	0.355	7.1-7.2
Jamaica	0	0.001	0	0	0.001
Japan	151.6-153.6	2.0	5.12	8.87	168-170
Kazakhstan	3.0	10.59-10.94	0	0	13.6-13.9
Latvia	0	0.020-0.025	0	0	0.02-0.025
Libya	0	0.025	0	0	0.025
Lithuania	10	0	0.220	0.342	10.6
Mexico	2.4	0.012	0.076	0.095	2.58
Netherlands	3-3.9	0.73-0.81	0.147	0.249	4.13-5.11
Nigeria	0	0.001	0	0	0.001
North Korea	0.04	0.042	0	0	0.077-0.087
Norway	0	0.004	0	0	0.004
Pakistan	0.84	0.017	0.008	0.019	0.884
Philippines	0	0	0	0	0
Poland	0	0.49	0	0	0.49
Portugal	0	0.007-0.008	0	0	0.007-0.008
Romania	2.4	0.033-0.044	0.012	0.019	2.46-2.48

Country	***Plutonium***	***HEU***	***Np 237***	***Am***	***Total (rounded)***	
Russia	271.2	1088-1103	3.47	5.313	1370-1380	
Serbia	0	0.013	0	0	0.013	
Slovakia	8.4	0	0.390	0.561	9.35	
Slovenia	2.7	0-0.005	0.132	0.157	2.99	
South Africa	5.8	0.61-0.76	0.274	0.308	6.99-7.14	
South Korea	44	0.002	1.54	1.851	47.4	
Spain	26.9	0	1.13	1.843	29.9	
Sweden	41.8	0.002	1.17	3.086	46.1	
Switzerland	17.5-20	0.005-0.010	0.859	1.256	19.6-22.1	
Syria	0	0.001	0	0	0.001	
Taiwan	22	0.003-0.010	0.648	1.511	24.2	
Thailand	0	0	0	0	0	
Turkey	0	0.008	0	0	0.008	
Ukraine	41	0.16-0.25	2.34	2.608	46.1-46.2	
United Kingdom	96.3-102.4	23.4	1.01	3.81	125-131	
United States	507.5	705	16.5	27.12	1260	
Uzbekistan	0		0.12	0	0	0.12
Vietnam	0		0.0056	0	0	0.0056
15 Others	0		0-0.001	0	0	0
Totals (rounded)	1835		1900	54	87	3875

Source: ISIS, www.isis-online.org

Appendix II

Mapping Workshop, April 7th, 2006: List of Participants

David Albright, Institute for Science and International Security (ISIS)
Scott Atran, Research Center for Group Dynamics, University of Michigan
Pauline H. Baker, The Fund for Peace
Matthew Bunn, Managing the Atom Project, Harvard University
Chester Crocker, Georgetown University
James Forest, Combating Terrorism Center, U.S. Military Academy
Lukas Haynes, MacArthur Foundation
Bonnie Jenkins, Ford Foundation
Colin Kahl, Office of the Deputy Assistant Secretary of Defense for Stability Operations
Jason Ladnier, The Fund for Peace
John Parachini, RAND Intelligence Policy Center
Stewart Patrick, Center for Global Development
George Perkovich, Carnegie Endowment for International Peace
Marc Sageman, *Understanding Terror Networks*
Jim Schear, Institute for National Strategic Studies, National Defense University
Louise Shelley, Transnational Crime and Corruption Center, American University
Joshua Sinai, Logos Technologies
Leonard Spector, Center for Nonproliferation Studies
Scott Tousley, Logos Technologies
Karen Walker, The Fund for Peace