Terrorism, Organized Crime, and WMD Smuggling: Challenge and Response

Strategic Insights, Volume VI, Issue 5 (August 2007)

by Phil Williams

Introduction

Contemporary threats to United States security are characterized by high levels of synergy. Although intelligence collection and analysis is still stove-piped in ways that treat these threats as separate and independent, in practice, they can no longer be demarcated from one another. The WMD proliferation threat, the threat posed by global jihadists and the threat from transnational organized crime overlap and intersect in important ways.[1] The nightmare scenario is that these intersections will result in a WMD being brought into the United States and used to inflict large-scale casualties that would dwarf those of September 11, 2001. Consequently, this analysis focuses on the possible smuggling of an improvised nuclear device (IND) into the United States. In considering this threat several distinct stages of activity need to be identified:

- Phase 1: the acquisition of nuclear materials by terrorist networks. This can be done directly or indirectly. One possibility is that terrorists will themselves acquire highly enriched uranium or weapons grade plutonium through theft and diversion or even a raid on a nuclear facility. Another is that terrorists will seek to acquire such materials on the black market, particularly from a criminal organization. In this case, it is important to distinguish between the upstream phase involving the initial acquisition of strategic nuclear materials and the downstream phase where the materials are sold to terrorists hostile to the United States. Although there is some, albeit imperfect, knowledge on the upstream phase, there is very little on the downstream transactions.

- Phase 2: creation of an IND. Assuming that terrorists have acquired HEU or weapons grade plutonium, they then have to use this to create a nuclear device. This is not an easy task, but is certainly not beyond the global jihad movement, with its access to financial resources that could be used both to find a safe haven and to acquire the scientific and technological expertise necessary to ensure the successful development of at least a rudimentary nuclear weapon.[2]

- Phase 3: the end game. In this phase terrorists seek to bring their nuclear device into the United States. Once again, this can be done either directly or using the smuggling expertise of organized crime. The terrorists could exploit the routes and methods drug traffickers and people smugglers have developed or look for alternatives of their own. With the latter alternative, their menu of choices is extensive.

The focus in this chapter is on the initial material acquisition phase and the end game; the weaponization process itself is not considered. Although the second phase is critical, it goes beyond the scope of this chapter—which seeks to illuminate the smuggling dimensions of the threat.

Links or contacts between criminal and terrorist networks could be of critical importance in the acquisition phase but are unlikely to be nearly as relevant in the end game. Put somewhat differently, while criminal organizations might well sell nuclear materials to terrorists, they are unlikely—at least knowingly—to assist in smuggling a nuclear device into the United States. This should not encourage complacency. Even if criminal organizations were willing to assist in the end-game smuggling effort, terrorists would almost certainly want to retain a high degree of control over both the process and the weapon. Furthermore, the choices available to terrorists pose formidable challenges for both detection and interdiction. Countering these requires additional approaches that go beyond the very substantial steps the United States is already taking to counter the smuggling threat. Some of these approaches to both the acquisition stage and end-game are outlined briefly in the final section.

The Acquisition of Nuclear Materials

The possibility that terrorists will engage in their own nuclear theft and smuggling activities has been raised by reports from Russia that terrorists have engaged in surveillance of nuclear facilities.[3] They might even have considered a “smash and grab” raid that would acquire strategic materials through direct assault and blatant theft. The difficulty is that this would be noisily overt, resulting in hot pursuit and a systematic mobilization of state resources to track down both perpetrators and materials. The risks would be very high as would the potential costs. And even if the subsequent pursuit was unsuccessful, the incident would reverberate internationally, confirming that nuclear terrorism is a real threat and thereby making the end game of getting an IND into the United States more difficult.

A second possibility is that terrorists would simply contract out the materials acquisition process, hiring a criminal organization or trafficking network to steal the materials and then transfer their ownership for the agreed upon payment. Such an arrangement would be far less likely to set off alarm bells than a direct assault. From the terrorists’ perspective, however, it would require a great deal of trust, as they would be required to make an up front payment prior to the theft and delivery of the materials. The criminals could then renege on the deal—quitting while they are ahead and disappearing with the advance—or prove unsuccessful in their efforts to acquire the material. Alternatively, they could be detected and turned by the authorities who could then carry out a seller sting operation against the terrorists. Such risks aside, the attraction of this approach from the terrorist perspective is that it does not leave acquisition to the vagaries of the market. The attraction might not be sufficient to outweigh the risks.

The third possibility, therefore, is simply for terrorists to work within the existing black market in nuclear materials, hope that sufficient material is available, and find a reliable seller. This will not necessarily be easy. Much of the black market trade has involved nothing more than radioactive junk, while scams and fraudulent offers of weapons-grade material have also been almost common-place. Yet, the number of cases involving weapons grade material has been sufficient to sufficient to make this a plausible option for the terrorists. According to the International Atomic Energy Agency (IAEA), between 1993 and 2005 there were 16 confirmed incidents involving trafficking in HEU or plutonium.[4] More recently, in January 2006, Georgian authorities arrested a Russian who was carrying 100 grams of highly enriched uranium.[5] Although the amounts of weapons-grade material have remained relatively small, the very discovery of this material being trafficked suggests that this might be the preferred option for terrorists.

This is reinforced by the involvement of criminal organizations, criminal-controlled companies, and ethnic trafficking networks in the nuclear material smuggling business.[6] In 2001, for example, the Balashikha criminal organization was involved in two separate incidents of nuclear material trafficking. In March, members of the group were arrested while trying to buy cesium and authorities seized $250,000 dollars in cash. Reportedly the gang members were acting as intermediaries and already had buyers from the Middle East.[7] Six members of the same group were arrested in December 2001, while trying to sell 1.068 kilograms of low enriched uranium for $30,000 dollars.[8] Cases of organized crime involvement in nuclear material trafficking have also occurred in various parts of Ukraine including Odessa and Dnipropetrovsk. In some cases, there has also been a high degree of sophistication in trafficking modes and methods, with the use of import-export companies to provide cover for illegal transactions.

The trafficking networks also appear to regard nuclear materials as simply another illegal product that can turn a profit. Turkish networks traditionally engaged in antiquities smuggling, for example, became involved in the nuclear material black market, simply adding nuclear materials to the other illegal goods they traded. In short, nuclear materials have become merely another commodity, and those who have stolen or diverted them have looked for buyers simply to make money. This deprives these materials of any special status apart from their worth on the black market. What is considered at a strategic level by the United States government as a key component of countering both proliferation and terrorism is seen at a micro-level as simply a business transaction—albeit an illegal one—and a potential source of profit. From the terrorists' perspective this is a source of opportunities.

Since the mid-1990s, the major nuclear smuggling routes have gone through the Caucasus, the Balkans, Turkey and Central Asia—all areas where the global jihad movement has had a significant presence.[9] Although there is no evidence in open sources of nuclear materials being supplied to terrorists, it is certainly conceivable that connections were made between sellers of diverted nuclear material and representatives of terrorist organizations. Those who have stolen, diverted or otherwise acquired nuclear materials are interested in finding buyers. During the 1990s, seizures and arrests made through sting operations made this much riskier, while the deployment of portal monitors made successful smuggling through border posts more difficult. Penalties have also been increased as governments have started to realize the dangers involved. Yet, this has had little impact: continued reports of seizures and arrests suggest that the business has continued more or less as normal. Risks might have increased but are not prohibitive. In these circumstances, it is conceivable that a criminal group might well be willing to supply nuclear material to a terrorist organization. Any scruples criminals might have about this, could be overcome by terrorists using a designated buyer not obviously connected to them. This would allow the criminals to do a deal with plausible deniability.

There is also considerable distance—both functionally and geographically—between the sale of these materials and their subsequent use as part of a weapon. In contrast, smuggling an IND into the United States involves an entirely new dimension of risk. It is not something that could easily be treated as simply another product and the smugglers would know that if the weapon were subsequently used, they would become the target of a global dragnet. Nevertheless, the possibility that criminal organizations might assist terrorists in smuggling an IND into the United States cannot simply be ruled out without further consideration.

The End Game: Organized Crime and Smuggling an IND into the United States

Would a criminal organization be willing and able to smuggle an IND into the United States? The answer under most, but not all, circumstances is probably no: those willing to do so would not have the capacity while those with the ability would not have the willingness. There are complex but reinforcing reasons for reluctance, ranging from concerns about risk and retribution to a

reluctance to disrupt existing illegal markets and their accompanying revenue streams. Moreover, organized crime is about the provision of illegal goods and services, and the exploitation of criminal opportunities for profit. Criminal organizations frequently use violence but it is generally limited and selective. They are not typically in the business of killing a lot of people. This is not moral inhibitions; the criminal calculation is utilitarian and while limited violence might be good for criminal business, large-scale violence is just the opposite. Not only does such violence bring unwanted attention to the criminals, it also tends to lead to crackdowns by authorities. For criminal organizations intent on maximizing opportunities and limiting risks, therefore, large-scale violence is imprudent. So too is an overly close connection with terrorists

Nevertheless, under some circumstances, some criminal organizations might be willing to assist terrorists in smuggling an IND into the United States. While this would be a high-risk activity for any criminal organization, the risk might not always be prohibitive. In fact, the willingness of a criminal organization to assist in this task would probably depend on: the degree of risk that a criminal organization is willing to accept in relation to the rewards that are offered; the extent to which a criminal organization also has a political agenda or an ideological or religious affinity that makes it willing to cooperate with a terrorist organization; and the degree of knowledge that the criminal enterprise has about the task it is being asked to carry out and what is really involved. Each of these dimensions must be considered in order to provide a broad assessment of the options available to terrorist organizations.

1. The unwilling: criminal organizations with low propensity for risk-taking

Most criminal organizations not only seek to obtain significant profits from crime, but also want to enjoy the proceeds. Consequently, risks have to be modest and controllable. Even if very high rewards were offered by a terrorist organization for smuggling an IND into the United States, these rewards would not be sufficient so long as a group was making significant profits from its existing criminal enterprises, believed it would continue to make such profits in an environment characterized by acceptable risks, and recognized that agreeing to smuggle IND would be a high risk activity—which if successful would almost certainly lead to subsequent identification and retribution. In short, for a successful criminal organization, the risks incurred in assisting a terrorist organization to smuggle an IND into the United States would be prohibitive.

For some criminal groups—particularly Mexican drug trafficking organizations and Mexican and Chinese alien-smuggling networks—additional considerations militate against this kind of cooperation with terrorists. Not least, the United States is their most important market and they would not want to do anything that disturbs the market. Moreover, for Mexicans, there are often family members and friends in the United States who would be put in harm's way by an IND attack. Chinese alien smugglers, often called snake-heads, are in a similar position. They have displayed a capacity to bring ships to the United States and offload them before law enforcement and immigration authorities can react. Consequently, they are a natural candidate for terrorists looking for smuggling partners. Yet, they have a long-term business in which the United States is promised land and customer for cheap labor, rolled into one. Assisting a terrorist organization in turning the United States into a target for an IND is not readily compatible with maintaining it as the major destination for Chinese immigrants. A one-off payment would have to be particularly attractive, therefore, for the offer even to be considered, let alone accepted.

Groups more susceptible to such offers would typically be struggling and looking for an opportunity to turn things around. A criminal organization not doing particularly well might be willing to engage in high-risk behavior for significant financial gains. For such a group a terrorist offer would certainly be more attractive than for competitors with large, diverse, and reliable income streams—although the obvious risks might still be sufficient to act as a deterrent. Even for groups not particularly successful in their criminal ventures, there is no point in making enormous amounts of money from a one-off venture without subsequent opportunities to enjoy the proceeds. Consequently, an offer to pay for IND smuggling is an offer that can, and probably will, be refused.

Accepting the offer is unlikely if the group has any real capacity to assess risk. And even this, assumes that the terrorist network would deign to use a second-rate as opposed to a highly successful criminal organization. Moreover, it is unlikely that a second-rate group would have the capacity to smuggle a weapon into the United States even if it were willing to try.

2. Willing collaborators

The only kind of criminal organization responsive to an offer by a terrorist network to pay large amounts of money to smuggle an IND into the United States is likely to be either sympathetic to the cause pursued by the terrorists or particularly hostile towards the United States. Such an organization will be more predisposed than most other criminal organizations towards acceptance of such a proposal, even though in strictly business and risk management terms it is not compelling. Chechen groups linked to the global jihad might be particularly willing to entertain such ideas, less because of a cost-gain calculation of criminal business than some kind of attachment to the common cause. Similarly, Albanian criminal organizations with a fundamentalist orientation might be prepared to take greater risks in support of global jihad. Yet, even if such groups are willing, it is not clear that they able to meet the demands of the task required

In sum, most organized crime groups will want nothing to do with smuggling an IND into the United States on behalf of a terrorist organization. Exceptions cannot be ruled out, but such groups are likely to be handicapped by limited skills and resources. There is, however, an additional wrinkle in all this. The rejection scenarios depend on a criminal organization having comprehensive and clear information about what it is being asked to do. Unfortunately, a criminal organization could be used by a terrorist network to smuggle an IND into the United States without knowing exactly what it is doing.

3. Unwitting collaborators

At first sight the prospect of a criminal organization being duped into smuggling an IND into the United States might appear somewhat far-fetched; in fact it is plausible. It requires simply that a terrorist organization approach a criminal organization specializing in smuggling and offer some kind of contract for services rendered. This could be done through an intermediary or front and would typically involve a container of contraband (which might be drugs, arms, endangered species, cultural artifacts, stolen goods, or even illegal aliens). Every aspect of the transaction—including the price that is paid, the route that is followed, and the methods of deception or circumvention—would be typical of such illicit transactions. The only difference would be an IND concealed within the contraband. Unless the criminal organization typically inspects such containers (and the probability is that criminal brokers and traffickers of this kind are simply concerned about being paid and do not do due diligence on customer or cargo) then it could provide unwitting assistance to a terrorist organization.

In short, a criminal organization could become the unwitting tool of terrorists. So too could marginal businesses that are ostensibly legitimate but do not ask too many questions to those for whom they provide services. Couriers, transportation services, and even moving companies could all too easily be exploited by terrorist organizations. Even in the United States some of these companies are disreputable in their behavior, in some cases, bordering on the criminal. In many other countries, criminality and corruption pervade the freight-forwarding business, thereby providing opportunities for terrorist groups to use their services, without questions being asked or suspicions being raised. In other words, when considering the prospects for a criminal organization or shady business to work with terrorist networks and smuggle an IND into the United States, the degree of knowledge of an organized crime group about who is hiring its services and what the shipment might contain is critical.

There is another side to this equation however. A terrorist network might not want to entrust an IND to a criminal organization. Concerns that the criminals will discover the real nature of their cargo and balk at the prospect might be prohibitive. Furthermore, most criminal organizations will typically be regarded by terrorists as mercenary and for sale to the highest bidder. Because an IND is a precious commodity for terrorists, they will be reluctant to transfer it to a group not committed to the cause and, therefore, not fully trusted. In the final analysis, therefore, terrorist networks might prefer to take on the task themselves. Consequently, the next section looks at some of the conveyances, routes, and methods available to a terrorist group intent on smuggling an IND into the United States. In effect, it develops what might be understood as a process model of IND smuggling.

The End Game: Terrorists and the Smuggling Process

Although terrorists as smugglers have a variety of options, their choices are not unlimited. On the contrary, smuggling is a bounded activity. This makes it possible to disaggregate the process and develop a generic smuggling model, which can be understood in terms of three dimensions:

- Smuggling as a geographic problem. Smuggling can be understood, in part at least, as the movement of a product (whether drugs, diamonds, endangered species or an IND), from its existing location to a desired location that can be a target market or a target for destruction.
- Smuggling as a transportation issue. Unless an IND is developed by terrorists within the United States city in which they intend to use it, certain kinds of conveyances have to be used to move it to the target. Unless a weapon is developed in the Western Hemisphere then air or maritime conveyances are essential at some stage in the transportation process.
- Smuggling as an adversarial process. Smuggling always involves efforts to outsmart those with the responsibility for preventing it. Consequently, the smuggling process involves choices about methods that can overcome the obstacles. In some countries, these barriers are little more than minor complications easily overcome. In others, the challenge for the smuggler is more formidable. Yet smugglers have a repertoire of options available for overcoming the barriers: concealment, deception, circumvention, and facilitation. These can be understood in part as alternative options, but can also be combined in ways designed to make it harder to detect and interdict the smuggling process.

Each of these dimensions must be examined with particular attention to the advantages and disadvantages of the available options for a terrorist network seeking to smuggle WMD into the United States.

1. The Geography of Smuggling

Thinking about smuggling as a geographic issue requires explicitly consideration of locations and the spaces between locations. Certainly terrorists intent on smuggling an IND into the United States have many choices to make in terms of locations and routes.

The target could be anywhere in the Continental United States, but is likely to be a major city, probably—but not necessarily—on or near the coast. The United States has numerous cities with a million people or more and there are three major port cities on the Atlantic coast—Boston, New York, and Miami—three on the Pacific coast—Los Angeles, San Francisco, and Seattle—as well as several on the Gulf Coast—most notably New Orleans and Houston—all of which are attractive targets for an IND attack by terrorists.

The point of entry could be a major container port; a remote coastal area; an official port of entry from Canada or Mexico; a remote portion of the Southwest Border with Mexico; or a remote part of the Northern Border with Canada. Each of these points of entry presents different kinds of obstacles and risks. Coming in to a major container port or official points of entry at the land borders would encounter monitoring devices that could result in detection. Coming in at a remote coastal area, therefore, might be preferable. The problem is that it would still be necessary to move the weapon to its final target. In contrast, a major port could itself be a very attractive target for terrorists, particularly if the objective is to hurt the United States economically through the disruption of trade.

The point of embarkation could be in an Islamic country, a country hostile to the United States, or a less obvious country subject to less scrutiny. In this connection, the United States has added an additional layer of scrutiny and security through the Container Security Initiative (CSI), designed "to protect containerized shipping from exploitation by terrorists."[10] The scheme exploits "intelligence and automated information to identify and target high-risk containers" pre-screens high-risk containers at the port of departure, makes use of detection technologies for screening and emphasizes "smarter, tamper proof containers."[11] The scheme has developed rapidly and by September 2006 operated at about 50 ports worldwide.[12] In addition, in December 2006 the Departments of Energy and Homeland Security launched the Secure Freight Initiative (SFI) and deploying radiation detection equipment for container scanning to foreign ports.[13] Initially operating at six ports this scheme will gradually be extended. Consequently, terrorists trying to smuggle an IND into the United States will confront a choice: do they try to embark from a port that is included in the CSI and/or the SFI or do they opt for an easier point of dispatch. Opting for a port that is part of the CSI carries additional risks at the point of embarkation. These are likely to be even greater with the SFI monitors. On the other hand, if the container with an IND inside passes through a CSI port, it might be subject to less scrutiny as it enters the United States. Conversely those containers that do not come with a prior seal of approval are more likely to be subject to intense and thorough scrutiny when they reach the United States. The tradeoff calculation depends in part on the perceived effectiveness of the CSI.

Another key component of the geographic of smuggling is the choice of a direct or indirect route between the point of embarkation and the point of entry into the United States. Coming in from Canada or Mexico is obviously an indirect route for shipments from other countries and might be an attractive option for terrorists seeking to smuggle a WMD into the United States. Alternatively, they might seek entry not via the immediate neighbors of the United States but via a country such as Britain or Italy, which would arouse little suspicion. A South American country such as Brazil might also be attractive as it would possibly be seen as an innocuous point of departure. The difficulty with an indirect route is that it is first of all necessary to get the weapon to this location and then transfer it to a container or vessel bound for the United States. Even if this creates additional risks of detection en route, these might be outweighed by less scrutiny at the US border.

2. Smuggling as a transportation issue

Another critical issue for terrorist organizations intent on smuggling an IND into the United States is choice of conveyance. Initially this appears simply as a matter of choosing land, sea, or air, but in fact the issue is both broader and deeper than this. It is broader since it is possible to develop both dual and triple combinations using all three types of conveyance; it is deeper because of the availability of multiple options within each category. If the choice is made to smuggle an IND into the United States by air, for example, terrorists could opt for air freight, or a small private plane, perhaps coming from the Caribbean into Florida. This last option was widely used by Medellin drug trafficking organizations in the 1980s. They brought large planes into Norman's Cay in the Bahamas and offloaded drugs onto smaller planes that merged with the weekend leisure traffic flying into Florida. Similarly, if the choice is made to use ships, there is once again the issue of whether to opt for a container ship, an oil tanker, a passenger ship or a small private boat. It is

also possible to envisage a route that mixes the conveyances. One alternative, for example, might be to ship or fly something into Mexico or Canada and then try to bring it over the border into the United States either by truck or private vehicle (whether van or car), or via the railway system as some kind of freight. The possible drawback to mixing conveyances is that the point of transfer might also be a potential point of vulnerability, although in part this would depend on the size of the weapon and the methods of concealment. The smaller, more portable the weapon, the less vulnerable transfer would be and the fewer inhibitions on adopting such an approach.

Several other aspects of the transportation issue are also worth considering. Decisions on conveyances depend on variations in the level of scrutiny likely to accompany an incoming conveyance, the ease of minimizing detection, the degree to which one kind of conveyance is regarded by United States authorities as less threatening than others, the ease of loading and unloading without arousing suspicion, and the proximity to the final target using this method of transportation.

One possibility is that of using a ship to bring in an IND. This is not as outrageous as it might appear. A few years after September 11, reports suggested that al-Qaeda owned or controlled a number of cargo ships.[14] Estimates differed with some suggesting 15 and others putting the figure anywhere between 12 and 50.[15] Although some progress has been made in identifying and monitoring these ships, it is unlikely that this task is complete—largely because of the problem of differentiating them from most of the 120,000 merchant ships plying their trade around the world.[16] Flags of convenience (FOC) for ship registration remain the equivalent in the maritime sphere of offshore financial centers and bank secrecy havens in the financial world, hiding beneficial ownership, minimizing transparency, and facilitating criminal and other malevolent activities. According to the General Secretary of the International Transport Workers Federation, “Corruption and lack of accountability are endemic in the FOC system, which is built on two pillars: no questions asked of ship owners and no questions answered to anyone else. When a ship is registered with one of these flags, a curtain of secrecy descends--as valuable if you're a terrorist as if you're a money launderer, someone who wants to sink a ship for insurance, or work its crew half to death before abandoning them unpaid in a foreign port.”[17] The FOC system and the layers of corporate ownership and front companies that accompany it, provide a veil of anonymity that allow criminals and terrorists alike to transport all sorts of illicit goods including possible an IND.[18] Inroads have been made against flags of convenience as both Liberia and Panama, the two largest shipping registries for these flags have “agreed to allow those countries that are part of the US-led Proliferation Security Initiative (PSI) to board ships sailing under their flags in the high seas if they are suspected of carrying weapons of mass destruction.”[19] Nevertheless, the system still provides an additional opportunity for deception.

The task of vessel monitoring is further complicated by the capacity of terrorists for using deception and what have been termed “phantom ships” In Southeast Asian waters at any one time there are believed to be as many as a dozen ships operating under false names and with false papers. These ships never make their destination port; instead cargo is offloaded elsewhere and the ship renamed. Such schemes typically involve theft, insurance fraud, and the use of the ships for illegal shipments, and are difficult to combat.[20]

Even so, an attempt by al-Qaeda to sail a ship with an IND on board into a major United States port would face serious obstacles. Maritime intelligence has been enhanced through the use of “large databases to track cargo ships and their crews and check them for ‘anomalies’ that could indicate terrorist plots”.[21] At the same time, the volume of licit trade provides a high degree of noise and clutter, making indications of an IND plot difficult to detect. Constant flux in the shipping business with changes of ownership and registration make it extremely difficult to distinguish between legitimate ships carrying licit cargos, legitimate ships carrying illicit commodities, and a terrorist ship with an IND on board. In these circumstances, and in spite of the PSI, the ship option could be a viable alternative for al-Qaeda, with success depending on the ability to create a plausible front, obtain a legitimate cargo for cover, and come to the United States from a port

regarded as relatively innocuous. None of these requirements presents an insurmountable obstacle for a global jihad movement with a long and successful history of document fraud, experience in the use of front companies, and considerable involvement in the import-export world.

These skills are also relevant to containers. In this connection, terrorists not only have to contend with the CSI discussed above, but also with the Automated Targeting System used by Customs to identify high-risk containers, and the more recent SFI.[22] Yet given the size and complexity of the global freight-forwarding industry, the opportunities for terrorists to embed themselves in reputable and trusted companies are very real. The insider threat has received a lot of attention in the world of computer or cyber crime; it requires similar attention in the world of freight-forwarding, shipping and even government. Insiders in a government or security agency can provide false authentication that security standards are met or that security checks have been completed. An insider or front company in contrast simply establishes a set of standard operational procedures for shipment that become the norm: a malevolent or illegitimate shipment that does not deviate (apart from the IND in its contents) from this norm will not raise red flags. When compliance becomes both routine and expected, the prospects for exploiting the trust that has been established are very real. This is linked to the notion of smuggling as a competitive or adversarial process.

3. Smuggling as an adversarial process

For those intent on smuggling an IND into the United States, choices of routes and conveyances will be determined part by assessments of the US capacity for detection and interdiction. The defensive measures that have been put in place since September 11 have clearly increased this capacity. Yet, given the problem of discrimination between commerce and smuggling and the implicit and sometimes explicit requirement for balancing security against the facilitation of trade, vulnerabilities remain. Given the sheer impossibility of sealing the borders and ensuring that all feasible points of entry are equally impermeable to smuggling, soft spots, whether geographic (point of entry) or functional (transportation method of entry) remain. The notion of smuggling as an adversarial process, although hardly novel, also suggests the need to consider the smuggler's toolkit. In this connection, four methods of smuggling can be identified: concealment, deception, facilitation, and circumvention. The first three all involve efforts to pass through the inspection process without detection; the fourth simply seeks to circumvent inspections altogether.

Concealment methods are based on an explicit acknowledgement that if the shipment is discovered it will be seized; deception methods generally involve the portrayal of the shipment as legal in the expectation that entry would be permitted without too much scrutiny; while facilitation is designed to degrade the quality of the inspection process. Circumvention (which is related to the prior discussion about points of entry) will be the preferred option when confidence is lacking about the prospects for effective concealment, deception, or facilitation. The categories are not quite as distinct as this discussion suggests however. Overlap between concealment and deception is common, while one or more of these methods might be combined with efforts at facilitation. Nevertheless, this typology of smuggling methods highlights the choices are available to terrorists.

To suggest that the simplest trafficking method is concealment is not to under-estimate the ingenuity or effort involved in many concealment schemes. Smugglers using overland routes to bring drugs, endangered species, antiquities, or other contraband into the United States often develop elaborate schemes for concealment in their vehicles. There have even been cases where a compartment has been created underneath the car dashboard for a small person to hide. The opportunities for concealment are even greater in commercial loads. Significantly, however, trucks crossing the Mexican border with drugs inside are often not modified in any way, relying simply on legitimate loads such as fruits and vegetables to hide the contraband. A shotgun approach ensures passage of enough of the drugs to yield healthy profits. Once again, though,

such an option is not really available for a terrorist organization—partly because of the use of portal monitors to detect radioactivity and partly because they cannot afford any seizure. Consequently, an effort to bring an IND into the United States would have to rely on other methods such as deception.

The use of deception is an important alternative and has at least two dimensions. The first is disguise. Commodities being smuggled are sometimes kept in plain sight and simply presented as legitimate in declarations to customs authorities. This approach is particularly effective in the case of dual use items where it is difficult to distinguish a weapon or component from something innocuous. For this method to be used for an IND, however, would probably require some concealment too. Bringing in a weapon in a load of scrap metal or integrating it into medical equipment—which could also provide a rationale for radioactivity—would mix deception and concealment and compound the problem of detection.

An integral part of deception is the use of false documents. This is widespread in the smuggling of endangered species where false export permits and re-exports certificates under CITES (the Convention on International Trade in Endangered Species) greatly facilitate the trade.[23] Such an approach might well have at least a partial counterpart in an IND smuggling venture. It is possible, for example, to change bills of lading to provide a false point of embarkation from a low-risk jurisdiction unlikely to provoke suspicion or concern. Alternatively, it might be possible to use legitimate export and import licenses for weapons or machinery along with efforts to disguise an IND as a legitimate part of a consignment. In this connection, a GAO test in December 2005 (detailed of which were released in March 2006) showed how false documentation could be used to bring radioactive materials into the United States. Although this proved controversial with critics claiming that the amount was so small that it was meaningless, the exercise clearly revealed a potential vulnerability of customs to deception.[24] One congressional staffer noted that although the good news was that the radiation portal monitors were effective, the bad news was that the use of fraudulent documents facilitated the passage of the material into the United States anyway.[25]

Smuggling, of whatever kind and form is made easier through corruption and cooption of insiders. In the drug business, for example, buying the acquiescence of customs officers who simply have to look the other way has been a very important facilitator. Sometimes acquiescence is obtained through a mix of bribery and coercion, or what Colombian drug traffickers traditionally described as a choice between lead and silver. For most of those faced with two such stark alternatives there is no real choice. This is more difficult at the port of entry to the United States than it is at either the point of embarkation or in transshipment countries.[26] Nevertheless, corruption on US borders is a huge vulnerability that can not be dismissed. It is not something that simply exists in Russia and Central Asia, Colombia and Mexico; it is also something that has become increasingly pervasive on the US side of its southern border with Mexico. There have already been major convictions of corrupt officials on the Southwest border who accepted bribes to facilitate the passage of people or drugs.[27] Moreover, it was reported in October 2006 that since 2004 at least 200 public employees had been charged with helping to move drugs and people across the border while thousands more cases of corruption were under investigation.[28] Disturbing as the numbers was the pervasive nature of the phenomenon which included “Border Patrol agents, local police, a county sheriff, motor vehicle clerks, an FBI supervisor, immigration examiners, prison guards, school district officials and uniformed personnel of every branch of the U.S. military.”[29] Although it could be argued that even those who accept bribes from drug traffickers or people smugglers would not do so from terrorists, the problem is that corrupt officials are unlikely to do due diligence on their paymasters. Consequently, corruption has become a national security problem for the United States.

The other approach is to opt to go around customs check points and enter the United States without coming through an official port of entry. This is a method that Mexican coyotes use to bring illegal aliens into the United States, smuggling them through inhospitable desert and hostile

terrain as an alternative to the formal points of entry. Such an approach, however, carries its own risk, not only from the United States Border Patrol but also from vigilante groups, intent on combating illegal immigration. Certainly, on the Southwest border such an approach is a high risk activity as is evident from the number of illegal aliens who die in the desert after crossing the border. The northern border with Canada is, in parts at least, less inhospitable and drug traffickers, people smugglers and other contraband smugglers use Indian reservations and remote crossing areas to outwit efforts at interdiction. Such an approach could work for a terrorist organization. Indeed, had Ahmed Ressam come into the United States through circumvention rather than a formal port of entry, the Millennium plot to attack LAX might well have succeeded.

Conclusions and Recommendations

In net assessment terms, there is both good news and bad news. The bad news is that the smugglers have the advantage. The capacity to embed illegal or dangerous cargo in legitimate shipments poses major problems of discrimination and detection for those attempting to combat smuggling. Consequently, smugglers are successful most of the time. Interdiction rates vary, depending on the product being interdicted, but rarely exceed a third of all shipments. Moreover, smuggling is highly dynamic. As customs authorities and law enforcement agencies become aware of which methods and modalities are being used, and close them off with interdiction strategies, smugglers adapt their strategies and tactics to ensure minimal losses.

The good news, as discussed above, is that significant initiatives have been taken to secure commerce against terrorist exploitation. Moreover, terrorist organizations, as yet, have developed only limited skills in smuggling. Furthermore, an IND being smuggled into the United States differs significantly from a marketable product for which there is a highly lucrative demand. Terrorists are less likely than criminals to have a smuggling infrastructure; they do not have established routes, highly effective methods of concealment or deception, or existing patterns of corruption and facilitation. In addition, an IND being smuggled into the United States is likely to be a unique asset; its seizure would be an enormous setback.

The bad news about the good news is that it will not last. At best it spells only temporary relief. As terrorist groups engage in more and more criminal activities such as counterfeiting, smuggling of a variety of illegal products, document fraud, and credit-card fraud, their level of skill and sophistication is also likely to rise. Recognizing that insider connivance is a great facilitator of the smuggling process, terrorists will make long term efforts to embed individuals and companies in positions where they can facilitate that process. And even if “insiders” are not yet in place, their absence might be insufficient to forestall a smuggling attempt. After all, terrorists need too succeed only once. And a smuggling attack would appeal considerably to organizations that do not play by any rules, and typically seek to create surprise and shock. These organizations are extremely good at creating opportunities and exploiting government weaknesses—particularly the seams of vulnerability created and perpetuated by inter-departmental and inter-agency rivalries.

In the final analysis, therefore, the bad news outweighs the good news. Yet, there are several additional things, beyond the measures already taken, that can be done towards leveling the playing field. The first is the continued allocation of increased resources to inspection and detection. The further development and wider deployment of technological devices that provide high confidence screening while also ensuring that “check points do not become choke points” is an important component of a successful anti-smuggling effort.[30] Even more important, though, is how resources are used—and this depends on how the smuggling threat is understood. It is not simply an inspection or detection problem that can be reduced to manageable proportions by innovative technologies. Ultimately, it is an intelligence problem. As a former Customs official noted “The best scientific aid I know is a good informer.”[31] Indeed, interdiction is critically dependent on good intelligence. In connection with the preceding analysis, this is true both at the material acquisition stage and the end game. In both cases, it also requires that intelligence agents, recognize the importance of alternative power structures and criminals as a critical source

of information. The regions though which nuclear materials have been trafficked are typically thought of lawless. In fact, “regions beyond government control are rarely as chaotic as they seem to be to Western officials.”[32] Often they are subject to alternate forms of governance whether from drug lords, criminal bosses, tribal and clan leaders, or other local power brokers. “Eastern Turkey in the Kurdish hinterland along the border with Iran”, for example, is “prime smuggling country” for stolen nuclear material; yet as William Langewiesche has noted, “the entire region is entirely sewed up…nothing moves there without notice, and …any transborder activity requires approval.[33] Arriving at an understanding with the local power brokers, therefore, is critical to combating nuclear material smuggling in the region. Something very similar is essential on the US southern border. People smugglers and even drug traffickers can be an invaluable source for United States intelligence and need to be quietly mobilized and co-opted as part of a comprehensive detection effort. On the border with Canada efforts to develop informants on Indian reservations could also be critical. Similar levels of effort need to be expended on individuals and companies in the freight-forward industry. In the final analysis, intelligence is essential to ensure that the CSI does not provide opportunities for “trusted” firms to exploit the faith placed in them.

Another crucial innovation is the pooling and sharing of knowledge and information about smuggling methods—among agencies and across national borders. Precedents for this include efforts to combat money laundering through the Egmont Group, an informal association of Financial Intelligence Units from various countries, which engages in information-sharing, in part through face to face meetings and in part through a secure intra-net. It is perhaps not surprising, therefore, that the FBI has taken the lead in trying to create something similar to combat nuclear terrorism. In this connection, the WMD Directorate, established by the FBI in July 2006, ran a conference in June 2007 at which 28 nations participated.[34] The “Global Initiative to Combat Nuclear Terrorism Law Enforcement Conference” was presented as an attempt to build capacity of other nations but was also intended to enhance the dialogue with partner agencies, to strengthen international information sharing and perhaps ultimately to provide a basis for joint operations.

In effect, the FBI’s initiative can be understood as an attempt to create law enforcement networks to combat smuggling and terrorist networks. A critical part of this must be the development and refinement of a set of warning indicators related to smuggling of WMD—an indicator list that would represent the collective wisdom of the individuals and institutions involved in the network and could focus both intelligence collection and intelligence analysis. This development of warning indicators could also be strengthened by red teaming. The United States needs to do a candid two-level appraisal of its continued vulnerabilities to smuggling: an internal assessment of the continued vulnerabilities; and an effort to understand terrorists’ perceptions of those vulnerabilities. Red-teaming could identify what information is publicly and readily available to a terrorist organization about the degree of scrutiny at different ports of entry, the inspections typically applied to different modalities of transportation, and the standard operational procedures for search and discovery. The red team approach would also facilitate the development of richer, more fully-developed scenarios that could inform the efforts to combat IND smuggling.

None of these measures is a panacea. Even with a comprehensive multi-faceted attempt to develop intelligence for the terrorist smuggling threat, the challenges remain formidable, the prospects for success, uncertain. Yet, unless further efforts are taken in this direction, the prospects for the successful smuggling of an IND into the United States will remain unacceptably high.

About the Author

Dr. Phil Williams is Professor of International Security in the Graduate School of Public and International Affairs at the University of Pittsburgh. From 1992 until April 2001, Dr. Williams was the Director of the University’s Matthew B. Ridgway Center for International Security Studies and

he is currently the Director of the Ridgway Center's Program on Terrorism and Transnational Crime. Professor Williams has published extensively in the field of international security including *Crisis Management*, (1976) *The Senate and US Troops in Europe*, (1986) and (with Mike Bowker) *Superpower Detente: A Reappraisal* (1987). He has edited or co-edited books on the Carter, Reagan, and Bush Presidencies, as well as on Classic Readings in International Relations. During the last ten years his research has focused primarily on transnational organized crime and he has written articles on various aspects of this subject in *Survival, Washington Quarterly, The Bulletin on Narcotics, Temps Strategique, Scientific American, Criminal Organizations*, and *Cross Border Control*. In addition, Dr. Williams is editor of a journal titled *Transnational Organized Crime*.

He is a consultant to both the United Nations and United States government agencies on organized crime and transnational threats and has also given congressional testimony on the subject. Most recently he has focused on alliances among criminal organization, global and national efforts to combat money laundering, and trends and developments in cyber-crime. Dr. Williams has edited a volume on *Russian Organized Crime* and a book on *Illegal Immigration and Commercial Sex: The New Slave Trade*. He is also co-editor of a recent volume on *Combating Transnational Crime*. He is currently completing a book for Polity Press on *Transnational Organized Crime*. In 2001-2002 he was on Sabbatical from the University of Pittsburgh and was a Visiting Scientist at CERT/CC Carnegie Mellon University, where he worked on computer crime and organized crime. Dr. Williams is currently directing a project for the Defense Intelligence Agency on the Financing of Terrorism. He is also focusing on methods of degrading criminal and terrorist networks.

References

1. This is sometimes described as threat convergence. For an illuminating and succinct analysis see Joshua Sinai, "The Evolving Terrorist Threat: The Convergence of Terrorism, Proliferation of WMD, and Enabling Conditions in Weak and Strong States" *Journal of Counterterrorism and Homeland Security International* 13, no.2 (Summer 2007): 10-16.

2. An interesting discussion of this can be found in William Langewiesche, *The Atomic Bazaar: The Rise of the Nuclear Poor* (New York: Farrar Straus and Giroux, 2007).

3. See, for example, "Russia: Terror Groups Scoped Nuke Site" *Associated Press*, October 26, 2001.

4. International Atomic Energy Agency, "Illicit Trafficking and Other Unauthorized Activities Involving Nuclear and Radioactive Materials: Fact Sheet," *International Atomic Energy Agency*, 2006.

5. Lawrence Scott Sheets and William J. Broad, "Georgia Says It Blocked Smuggling of Arms-Grade Uranium," *New York Times*, January 25, 2007.

6. This conclusion is based on a close analysis of the nuclear material trafficking database compiled by Paul N. Woessner when he was a Research Fellow at the Ridgway Center, University of Pittsburgh. For an early sample of the cases see Paul N. Woessner, "Chronology of Radioactive and Nuclear Materials Smuggling Incidents, July 1991-June 1997" *Transnational Organized Crime* 3, no.1 (Spring 1997): 114-209.

7. “Russia: Russian Police Arrest Caesium-137 Smugglers,” *Segodnya*, Moscow, in Russian, March 12, 2001 (*BBC Worldwide Monitoring*).

8. Jeffrey Kluger, “The Nuke Pipeline: The trade in nuclear contraband is approaching critical mass: Can we turn off the spigot?” *Time Magazine*, December 17, 2001.

9. This can be clearly seen in a careful examination of the Woessner database.

10. “Container Security Initiative Now Operational in Singapore,” March 18, 2003, Office of International Information Programs, U.S. Department of State.

11. *Ibid.*

12. "Ports in CSI," U.S. Customs and Border Protection Website, *CPB.gov*.

13. Office of the Press Secretary, Department of Homeland Security, “DHS and DOE Launch Secure Freight Initiative,” *DHS.gov*, December 7, 2006.

14. John Mintz, “15 Freighters Believed to Be Linked to Al Qaeda: U.S. Fears Terrorists at Sea; Tracking Ships Iis Difficult,” *Washington Post*, December 31, 2002, A01.

15. John Mintz, “Al-Qaeda Takes Terrorist Threat to Sea,” *Washington Post,* January, 1, 2003.

16. Mintz, “15 Freighters,” Op. Cit.

17. “U.S., International Authorities Track Terrorist Shipping Assets, Activities,” *American Maritime Officers*, 2002.

18. *Ibid.*

19. T Ország-Land, “Less Convenient Maritime Flags,” *Janes.com*, June 8, 2004.

20. For a good overview of the problem see Jayant Abhyankar “Maritime Fraud and Piracy ” in Phil Williams and Dimitri Vlassis, eds., *Combating Transnational Organized Crime* (London: Cass, 2001) 155-194.

21. Mintz, “15 Freighters,” Op. Cit.

22. *Ibid.*

23. Author interview with CITES official, Brussels, June 2002.

24. Toby Eckert, “Report: Radioactive material easily brought into U.S,” *Copley News Service*, March 28, 2006. For the text of the GAO report to Norm Coleman, Chair Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, United States Senate see “Border Security: Investigators Successfully Transported Radioactive Sources Across Our Nation’s Borders at Selected Locations,” *GAO-06-5458*, March 28, 2006.

25. Quoted in Eckert, *Ibid.*

26. For an analysis of the problems in transshipment countries see the Government Accountability Office Report, *Combating Nuclear Smuggling: Corruption, Maintenance, and*

Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries (Washington: GAO-06-311) released on March 28, 2006.

27. See John Pomfret, "Bribery at Border Worries Officials," *Washington Post*, July 15, 2006.

28. Ralph Vartabedian, Richard A. Serrano and Richard Marosi, "The Long, Crooked Line: Rise in Bribery Tests Integrity of U.S. Border," *Los Angeles Times*, October 23, 2006.

29. *Ibid.*

30. Tom White, of the Association of American Railroads, quoted in "Shippers, Carriers Rap Customs on Advance Notice Mandates: Industry worries that new regulations will create chaos at the borders and harm the economy," *Logistics Management* 42, no. 2 (Feb 2003): 13.

31. Timothy Green, *The Smugglers* (New York: Walker, 1969), 8.

32. William Langewiesche, Op. Cit., 61.

33. *Ibid*., 64.

34. See "Nuclear Terrorism: Talking Prevention in Miami," Federal Bureau of Investigation Website, *FBI.gov,* June 11, 2007.