Protecting the United States Against Terrorist Nuclear Attacks: A System of Systems Approach

Alan Shaw
25 October, 2001
Advanced Systems and Concepts Office
Report Number ASCO 2001 014

This paper was produced for the Advanced Systems and Concepts Office (ASCO) of the Defense Threat Reduction Agency (DTRA) in partially fulfillment of purchase order DTRA01-00-P-0155.

SUMMARY

The threat of a nuclear weapon delivered against a US city by unconventional means has been recognized and studied for almost 50 years. For most of that time the threat was assumed to emanate from the Soviet Union, and as the Soviet arsenal of long range ballistic missiles and bombers grew, the threat of unconventional delivery receded. During the 1990s, the demise of the USSR, the end of the cold war, and improving relations with Russia all signaled a further decline in the threat. However, that same decade saw an increase in "rogue states", state-sponsored terrorists, and non-state actors with great antipathy toward the US, and displaying greater success in obtaining weapons of mass destruction than in acquiring long-range means of delivering them. There was also an increase in nuclear proliferation—aided in part by the partial chaos that followed the end of the Soviet Union, and in part by the increasing accessibility of nuclear weapons technology now about 60 years old. There is ample reason for renewed concern about a terrorist nuclear threat.

Most studies of preventing terrorist nuclear attacks have reached the same basic conclusion--none of the available basic techniques is sufficiently capable to preclude a successful attack with a high degree of confidence. These techniques are generally: (1) arms control and related diplomatic measures to control proliferation and access to technology and materials for making nuclear weapons; (2) physical security and control of existing weapons and materials; (3) pre-emptive actions; (4) deterrent threats of retaliation for attacks; (5) border controls and related domestic security measures aimed at preventing the movement of weapons or materials into the US; and (6) intelligence collection and law enforcement measures leading to the discovery and apprehension of would-be perpetrators. Effective consequence control and mitigation—still a long way from reality—could be at best a distant second in desirability.

Draconian measures--such as stringent border controls, greatly expanded domestic controls, or the application of military force against any suspicious activity in another country--would be extremely destructive of commerce, foreign relations, or civil liberties. These measures would also be virtually unaffordable. Moreover, nothing that had occurred prior to September 11, 2001 was sufficiently dramatic to generate public support for any such approach. While that attack and its aftermath have produced increased support for the institution of more security measures, such severe measures are still remote possibilities.

Nevertheless, the threat cannot be dismissed. And it is reasonable to believe that in the absence of counter measures it will increase over time. The technology will become more accessible, and new methods that make aspects of bomb manufacture easier may emerge. Groups can exploit time to accumulate nuclear materials and tools, or to establish access to bombs, materials, tools, and expertise. Commercial globalization will increase the difficulties of controlling what moves into and within the US. Hostile

entities will have time to emerge, develop, and create connections with like-minded groups.

It is extremely unlikely that the US will be able to be build an impenetrable defense against terrorist nuclear attacks. Doing so would require an unacceptable degree of isolation and control. However, it is possible to build a complex system that makes it very unlikely that such an attack can be carried out successfully. While basic trends—largely beyond US control—will make it easier for terrorists to obtain, move, and use nuclear weapons, the opportunity exists to influence other trends to reduce the threat and to make the defensive system more effective.

The US can exploit the coming years to put into place a "system of systems", a combination of measures each of which impedes the ability of malefactors to successfully acquire or build a nuclear weapon, move it to the United States, place it near a target, and detonate it. This system would exploit measures that already exist, enhancing them as necessary and adding others. Although composed of an array of measures, a system of system is more than simply a collection of measures. What makes it a system is that the measures are correlated in some logical way, and that someone is at least nominally in charge. Integration into a coherent whole would be an important key.

A great many attack paths are possible, therefore the system would have to be sufficiently broad to cover them all. It would exploit two basic aspects of these attack paths, and indeed should be designed to ensure that these continue. First, nuclear weapons are rare and costly commodities. And there are generally no partial successes[1]; either an attacker gets his weapon to its target and detonates it, or he does not. If his chances of penetrating the defense are low, he will have a low expectation of any "positive" outcome, coupled with wasting much effort and money. Having a 10% probability of success does not mean that he will kill only 10% of his intended victims, or that he will have to try ten times in order to have one successful attack. It means that he is very likely to fail. He may also incur the displeasure of sponsors or collaborators. Effective retaliation, apprehension and punishment can raise the expected costs still more. A defense that is reasonably effective, although far from 100%, will be more useful against a threat of this type than it would be against one in which more weapons can be expended to compensate for losses to the defense, or one in which partial successes are still successes.

Second, each threat path is a complex one involving multiple steps, each of which has to be accomplished successfully. A layered defense is in order. Several steps of modest defensive capability can combine to make the likelihood of accomplishing the entire threat path process quite low.

At the heart of this approach is the creation of the expectation in the mind of the potential attacker that he is very unlikely to succeed, and that failure will carry substantial

[1] The attacker might be prevented from getting all the way to his target, and forced to detonate in a less desirable location. That might be a partial success. A bomb that doesn't operate at full yield, or one that doesn't achieve a nuclear detonation but only scatters nuclear material might also be a partial success.

costs, costs that go beyond wasted effort and funds and resources expended for no result. Part of the cost of failure will be discovery and retribution. This expectation should certainly be based on reality. Should the perpetrator not be dissuaded, he indeed will be very likely to fail at great expense. However, uncertainty and ambiguity also have a role to play. Some defensive capabilities are best kept hidden, while others might be exaggerated to enhance deterrence.

The system can be thought of as having three dimensions: (1) basic design and system elements; (2) overall plan for management and organization; and (3) plans for evolution of the system, including identification of needs, research, development, and acquisition. This report concentrates on the first.

The general structure of the system should mirror the threat paths, which consist of three basic elements: obtaining a weapon; bringing it to the US; and using it to cause great damage. System elements will generally consist of: (1) controlling the supply side; (2) impeding transportation; and (3) reducing vulnerabilities to attack and freedom of perpetrators to move weapons within the US.

Controlling the supply side is critical to the system plan. If nuclear weapons become cheap and easy to obtain, one basic premise for this approach will be undermined. The supply side consists of weapons, materials, technology, experience, equipment, and industrial capacity. Opportunities exist to control all of these, and indeed many programs are in place. It would be worthwhile, in formulating US policy in areas related to nuclear weapons, arms control, nuclear reductions, commercial applications of nuclear technology, and other related areas, for effects on the availability of nuclear weapons and materials to be explicitly considered.

Within the supply side, the farther from completed weapons the terrorists are forced to begin their efforts, the less likely they are to be successful. Eliminating access to weapons is probably more important than eliminating access to weapons-grade material, which in turn is probably more useful than keeping them away from radioactive materials that need to be enriched and/or separated before they can be used to make a bomb. In general, the farther from a completed weapon the terrorists begin their efforts, the more steps they have to complete, and the more opportunities there are to impede, prohibit or intercept necessary steps.

Impeding transportation is a complex topic. The demands of globalized manufacturing and the structure of shipping pose major problems. The global economy requires the movement of large amounts of goods, often on tight schedules. Fissile materials have radioactive signatures, but these can often be concealed. It is extremely unlikely that the actions of law enforcement agencies can close US borders and ports of entry against the introduction of radioactive contraband. However, opportunities may exist to work with companies to gain their cooperation in monitoring their shipments in exchange for facilitating cross-border movements. Moreover, the long and complex routes by which materials or weapons might get from points of origin to locations in the US may provide multiple opportunities for interception. Some basic synergies might be

explored. For example, integrated sensor networks can be used to detect and track certain amounts of fissile materials as they move through transportation networks. Smugglers might be able to evade such networks, but at a cost—for example using shielding or other packaging that has its own signatures, or breaking their load into many smaller ones, creating more opportunities for detection. Technology can be exploited to improve detection of nuclear materials, and to net together information from a variety of sources.

Terrorists who manage to get a weapon (or components) into the US pose a real danger even if they have great difficulty with further movements. However, benefit can still be gained by impeding further movements, or by forcing them to take actions that expose them to detection and capture. Networks of sensors deployed around potential major targets (e.g. cities) show some promise. Finally, should all else fail, effective consequence mitigation can help minimize loss of life and property, but will not avert catastrophe.

Main Points

- A nuclear attack using unconventional means of delivery within the US remains a very low probability, very high consequence event that is extremely difficult to defend against.
- In the absence of effective countermeasures, the probability is likely to increase over time, as the technology for making nuclear weapons becomes more accessible.
- Two other elements of the threat—access to nuclear materials and expertise, and motivations to attack—are amenable to influence.
- Studies have concluded that there are no individual measures that could be conceived and developed that could provide a highly effective defense. In the absence of a vastly increased public perception of the threat of attack, significantly increased funding is unlikely to become available to solve this problem.
- A reasonable approach is to construct a system of systems, i.e. a coherent array of existing, improved, and new measures that address all elements of all threat paths.
- The system would be designed to deter through likely denial of success of a very costly operation, coupled with the imposition of retribution and other consequences.
- This approach makes sense only as long as nuclear weapons remain extremely rare and costly items to potential attackers.
- The system would impose and integrate impediments to obtaining a nuclear weapon, transporting it to the US, and using it effectively against a target within the US. The first two are of higher priority than the third.

CONTENTS

INTRODUCTION AND OVERVIEW

Protecting US cities against

Terrorist Nuclear Attack

A system of systems approach

Of all the possible forms of terrorist attack on US cities, a nuclear attack is the most horrific. While major efforts have been devoted to deterrence and defense against long-range nuclear attacks on CONUS, little attention has gone toward designing measures to prevent a successful nuclear attack delivered by unconventional means[2]. Despite four decades of analyses that have described possible attack paths, this threat has largely been consigned to the "extremely low probability" category, in part because of the major technological difficulties that terrorists (of other would-be attackers) would face in building or otherwise obtaining a nuclear weapon. The term "terrorists" is used here as a shorthand to refer to any groups that might seek to deliver a nuclear attack by means other than those usually associated with military nuclear weapons, principally ballistic missiles, cruise missiles, and bomber aircraft. These groups range from independent groups, through groups with the support or sponsorship of governments that are hostile to the United States, to forces directly under the control of hostile governments.

A terrorist nuclear attack remains an event with low probability and very high consequences. However, in the absence of improvements in inhibitory measures, as years go by the probability of occurrence will undoubtedly increase, while the consequences will not decline. Each year the technology for making and employing nuclear weapons becomes more accessible. Furthermore, in the absence of effective measures, nuclear materials are also becoming more accessible. Unlike chemical and biological attacks, for which science holds out the hope that effective counters to exposure can be found eventually, the effects of nuclear blasts are unlikely to be mitigated.

During the Cold War, an effective strategic nuclear force was developed as the centerpiece of a posture to deter nuclear attacks on the United States by the Soviet Union, and by extension by lesser nuclear powers. In the aftermath of the Cold War, ballistic missile defenses are being developed to stop attacks by "rogue" national leaders having

[2] "Unconventional means" are taken here in the usual sense of means other than typical military means for delivering nuclear weapons: missiles and bombs. However, from a typical citizen's perspective, the "unconventional means" that have been discussed by analysts are the most conventional of means, principally civilian modes of transportation.

ballistic missiles and small nuclear arsenals but lacking the rationality to be deterred by overwhelming US nuclear power.

Nevertheless, it has been recognized for some time that the threat of nuclear retaliation might not be a suitable deterrent against attackers such as terrorists who don't present suitable targets for US nuclear attack, or against some types of states that might consider sponsoring such an attack. And ballistic missile defenses are rather useless against those who deliver their weapons by other means.

This is not a new problem. It has been studied since the 1950s. It is also not a problem that has been ignored. Many individual programs are in place to deal with the potential for such attacks, some as part of larger efforts to counter nuclear proliferation, and others aimed more specifically toward countering terrorist attacks. From what has gone before, we can make the following observations:

1. As we begin the 21st century, an unconventional nuclear attack on US soil remains very difficult to carry out, and remains a very low probability event.
2. It is a low probability event primarily because of the difficulties of producing or otherwise obtaining a nuclear weapon, transporting it without destroying its ability to function, and successfully operating it. However, there is little in place that will prevent a savvy and resourceful malefactor who obtains a nuclear weapon from moving his weapon from source to target.
3. The inevitable progress of technology will improve the ability of terrorists or their sponsors to create a nuclear weapon. In the absence of countervailing measures and trends, one would have to conclude that the probability of attack will increase over time.
4. There is no technology or device currently under development that will make it impossible to move a nuclear weapon undetected. Simple physics tells us that no such "silver bullet" could be built that would not bring global commerce to a halt. Moreover, trends in global commerce push in the opposite direction, i.e. toward easing impediments to the rapid and massive free flow of goods.

We can further observe "by inspection" the following, some of which have been noted in other studies:

1. Considering all the other demands of national security, law enforcement, and domestic emergency response, until September 11, 2001 it was unlikely that significantly more money and effort would be devoted to the problem of countering unconventional nuclear attack, in the absence of an actual attack or an intercepted attempt. In the wake of the September attacks, there will be more devoted to countering terrorist actions. How much of that becomes available to countering nuclear terrorism remains to be seen.
2. The decade or so that has followed the end of the Cold War has seen an increase in the dangers of proliferation and accessibility of nuclear weapons and materials. Whether this is the beginning of a long-term trend, or a temporary "window of opportunity" that will be reversed remains to be seen. Moreover—and perhaps

more significantly—there are opportunities to shape the future. Indeed, the US is well along in some measures to do just that.

3. Much can be done to reduce access to nuclear materials and nuclear weapons as the technology becomes more accessible. The net trend need not be an increase in the probability that terrorists can obtain nuclear weapons. However, in the absence of such countervailing measures it almost certainly will be.
4. Today, access to significant quantities of nuclear materials is not easy, and the technology of nuclear weapons is generally quite sophisticated by today's standards. Increases in the threat will occur slowly over time. Therefore, time can be exploited to put into place a deliberate program to build a defensive system. However, this should not be interpreted as a reason for complacency. The dramatic failure of a nuclear state could change this timeline dramatically.[3]

This leads to the observation that what needs to be put into place is a "system of systems", a combination of measures each of which impedes the ability of malefactors to successfully acquire or build a nuclear weapon, move it to the United States, place it near a target, and detonate it.

This system of systems is based on two basic principles. The first is that it cannot provide an impenetrable defense, i.e. a complete assurance that an attacker could not possibly penetrate it. However, it can aim to reduce the probability of successful attack to as low a level as is practical. Just as there is no "silver bullet", there is no "impenetrable shield". The second principle is that for the attacker there is no acceptable level of attrition. With one weapon, he either gets through to his target or he does not. The role of the defensive system is to reduce to a low level the probability that he gets through. For the attacker this is a roll of the dice, not a question of how much of his damage mechanism he can deliver to the target. And ultimately the attacker's perception of his chances of being successful will help determine his decision whether or not to make the attempt.

In a very general sense, this system will be two dimensional. First, it provides a defense in depth—or layered defense—against any specific threat path an attacker might choose to attempt. Each step that the attack must take along that path will face impediments. The net result should be an actual—and a perceived—very low probability that the attacker will successfully complete all of the steps. Second, the system will have to cover a large number of different threat paths. If it doesn't, an attacker would have the choice of avoiding those paths that are difficult in favor of one that is relatively unimpeded.

[3] A dramatic failure is one more precipitous than the end of the Soviet Union. While the demise of the USSR may have been quite traumatic for its residents, one stable government was replaced by several others. There was no period of chaos. On the other hand, were Pakistan to dissolve into civil war, the security of Pakistani nuclear weapons would be very much in question. Taliban/al-Qaeda would likely be an active party in that civil war.

Although composed of an array of measures, a system of systems is more than simply a collection of measures. What makes it a system is that the measures are correlated in some logical way, and that someone is at least nominally in charge. That does not mean that all of the component elements have to come under the direct control of one organization; rather some person or organization has responsibility to looking across the entire array to understand where coverage is lacking, or where emphasis is needed.

This system should have two primary goals: (1) prevent a successful attack; and (2) establish confidence among the public that they are not in danger, even if an attack is threatened or announced. Obviously the two are related, but they are not the same. Terrorists may conduct acts of violence to cause destruction, or to disrupt society through the act or threat of violence. Their ability to disrupt society is minimized if the public does not perceive the threat as credible.

The general structure of the system should mirror the threat paths, which consist of three basic elements: obtaining a weapon; bringing it to the US; and using it to cause great damage. System elements will generally consist of: (1) controlling the supply side; (2) impeding transportation; and (3) reducing vulnerabilities to attack and freedom of perpetrators to move weapons within the US. From the perspective of inspiring public confidence, the first two are certainly preferable to the third. The public would feel better knowing that terrorists are not going to be able to get nuclear weapons and bring them to the US than they would being told that although a weapon may be here we can take measures to limit the choice of targets and keep casualties down. The first two are also preferred elements for preventing a successful attack, although all three contribute. The more obstacles there are to a successful attack, the more likely the perpetrator is to be dissuaded from attempting it.

Ultimately, deterrence has to play a large role in the system, just as deterrence did in the Cold War nuclear posture. It is always dangerous to speculate about what will deter someone else (particularly a non-rational player), but a few basic observations are in order. Terrorists who are willing to launch a destructive attack on the US are likely to see a big payoff for a successful nuclear attack. However, nuclear weapons and fissile material are very rare commodities on the black market. Obtaining or producing a nuclear weapon, and having confidence that it will work, are very difficult and very costly. If a terrorist organization perceives that the likelihood of success after such high expenditures is low, they may well decide to abandon the effort. Spares are very unlikely to be available. If something goes wrong and the weapon is lost, the entire operation will come a cropper; replacing the weapon will be very difficult. Moreover, if the weapon is captured or discovered, the perpetrators could well suffer the severe consequences of having conducted the attack without reaping any of the benefit of having done so.

Deterrence theory generally recognizes deterrence through denial of success and deterrence through retribution. For terrorist attacks, deterrence through retribution—particularly proportionate retribution—may be very difficult to achieve, thus putting more emphasis on deterrence through low expectation of success. By itself, denial of success carries only the penalties of wasted effort, wasted money, and wasted

opportunities. For some well-supported groups, these may be easily overcome. Therefore denial of success has to be supported by some punishment or retribution. What form this might take would depend on the specifics of the group conducting the attack. At one extreme, a shadowy group of suicide bombers with no fixed base and no obvious support would be very difficult to threaten with retribution. However, such a group would be very unlikely to have the wherewithal to overcome the formidable obstacles to obtaining a nuclear weapon. The fact that measures for retribution that might be applied to nations may not be useful against other groups doesn't mean that no useful measures can be found. Arrest and punishment, disruption of activities and networks, confiscation of assets (and internment of individuals with rare and valuable expertise), and copious applications of "sunlight" are all potentially useful punishment measures to enhance deterrence by denial of success. All of these measures—and more—have been applied in response to the 9/11/2001 attacks, and similar measures were taken in the wake of the Aum Shinrikyo attack, the World Trade Center bombing, and other activities linked to Osama bin Laden. These measures can be supported by forensics and other methods to establish attribution.

The system can be viewed from several different perspectives. The first, as described above, is in terms of basic elements tied to the basic components of the threat paths. The second is in terms of the tools that are employed. These can be correlated, but not always neatly.

System elements (1): controlling the supply side

One basic component of a system to keep terrorists from using a nuclear weapon within the US is keeping them from obtaining one. Supply side controls affect the ability of would-be attackers to obtain a nuclear weapon.

When viewed from a purely technical, users' perspective, the simplest approach is to get one's hands on a completed weapon and the "users manual". The latter would likely consist of some combination of written documentation and experienced technical expertise. The users could be relatively confident that the weapon would work, and they would not face the problems of building one. Complete weapons might be obtained by theft—either directly or from a criminal group willing to steal one for money--by purchase from corrupt officials, or as a "gift" from a sympathetic government. If a complete weapon cannot be obtained, would-be perpetrators might attempt to steal or buy all of the components for an existing weapon type, or at least as many components and they possibly can. They would then require the expertise to assemble the weapon, and possibly to produce components they were not able to steal. If either of these approaches is not possible, terrorists or state sponsors might attempt to obtain fissile material and build a bomb using a proven design they have obtained, or design their own. In the absence of access to weapons-grade fissile material, they would have to obtain reactor fuel, or waste, or some other source of radioactive uranium or plutonium, and then enrich and/or separate it.

In general, the farther down this list the terrorists are forced to begin, the more technical/industrial facilities and expertise they need, and the more technical problems they have to overcome. It is important to impede all paths to obtaining a weapon, and to impede each path in as many places as possible. Moreover, in general, the more things they have to do in order to obtain their weapon the more likely they are to be observed doing it.

The major elements of this part of the system—controlling the supply side—already exist. These are generally nuclear arms control and non-proliferation measures, including international controls on commercial nuclear activities. A Fissile Material Cutoff Treaty (FMCT) is under discussion. These need to be reviewed. In particular, as the US moves toward revising its approach to the basic arms control regime, the implications for terrorist access need to be taken into account. US policies in the international nuclear arena have been undergoing a *de facto* review for about a decade; that review has become more deliberate since the 2001 inauguration. Major elements of this review now clearly include the balance between unilateral defenses and reliance on international arrangements, and the role of US programs to assist the Russians in keeping their nuclear legacy under control. The potential for terrorist use and diversion of nuclear assets adds a dimension that ought to be considered explicitly in this review. As a general proposition, the more the US emphasizes unilateral measures over agreed international regimes, the less ability it has to influence the control and security of weapons and materials in other nations. While there is no fundamental reason that non-proliferation measures cannot be decoupled from other elements of nuclear arms control, they are currently coupled through treaty language, and other nations have thus far evidenced little enthusiasm for decoupling. That being the case, they are likely to remain coupled.

Russia is the most frequently mentioned source for theft or diversion of nuclear weapons or materials, primarily because it has so much and has been undergoing great internal disruptions. Under current circumstances, it seems unlikely that terrorists would obtain official Russian cooperation. However, theft with or without the connivance of a corrupt or disgruntled insider has been discussed as a serious possibility. The US has been involved with the Russian government in programs to improve security of Russian nuclear weapons and nuclear materials. More could be done bilaterally, including expanded cooperation on security measures, relevant economic development assistance[4], agreements to reduce the numbers of nuclear weapons (particularly those that are small and transportable), agreements to improve transparency and accountability, and programs to dismantle excess weapons and irreversibly dispose of their nuclear materials. Efforts to prevent diversion could be really helped by an accounting of how many warheads the Russians have, and their locations. The fewer weapons there are and the better oversight each one has, the less likely it is that there will be diversions—or attempts at diversion—that remain undetected for significant periods of time. The question of how to balance Russian desires for a degree of secrecy and ambiguity as an element of their security with the benefits of certainty and transparency for everyone else's security is a complex one. However, it is a familiar one in arms control circles.

[4] Not necessarily assistance in the form of US payments to Russia.

Other nuclear powers—China, Israel, India, and Pakistan—present similar problems of theft. Each is a unique case that is defined by factors such as the size and technology of its nuclear arsenal, its plans regarding expansion, contraction, or maintenance of the status quo, and its politics. Among these, Pakistan poses the greatest danger that sometime in the future a government will emerge that has a very different attitude toward the US, or that it may dissolve into chaos, or that individuals with access to nuclear weapons may be "turned" by radical anti-US groups[5]. Reducing the potential risk from these countries requires some tailored, but coordinated, approaches to negotiations regarding controls and security. None enjoy the same history of involvement in arms control negotiations that the Russians have.

None of the nations discussed above poses a serious risk of supporting or aiding terrorist groups that might seek to attack the US with nuclear weapons. But with radical changes in government, some might pose such a risk, a risk that already exists with some aspiring nuclear states that the US has branded as "rogue states". Such states call for very different measures, probably less cooperative and more confrontational. The US government needs to give some thought to how it would ascertain and monitor such activities, and what tools it would use to put a stop to them. Some thought might also be given to how the international non-proliferation regime might be used to impose roadblocks.

There is undoubtedly a very broad consensus worldwide against nuclear terrorism. This is not just a matter of principle. The US is not the only country at risk. States that have not been enthusiastic about participating in some other areas of arms control might be brought into cooperation in constructing an international regime that reduces the threat that terrorists could get a nuclear weapon. As a general observation, most scenarios would involve terrorist groups from Eurasia/Africa obtaining weapons in the eastern hemisphere and bringing them across the ocean to the western. Unilateral US measures that make it more difficult for weapons to be brought across the ocean could make European and Asian targets more tempting, thereby providing an incentive for international cooperation.

If terrorists cannot obtain a complete weapon, the next best solution is to obtain the plans and components for a weapon of a type that already exists. They would then be faced with the added problem of assembling the weapon correctly. For this they would almost certainly need expert help. In practice, this approach may be harder than trying to get an entire weapon. It would require multiple thefts rather than a single one, and therefore more chances to get caught. However, if security is less good for components than it is for weapons, it may work out. It has the added advantage that a weapon obtained in parts can be smuggled in parts. If any parts are lost en route, spares might be substituted for them. This approach may be easier to work with insiders than attempts to obtain an entire weapon. It can be done piecemeal, with less visibility and perhaps less

[5] October 25, 2001 the BBC reported that two Pakistani nuclear scientists were arrested for contacts with the Afghan Taliban regime.
http://news.bbc.co.uk/hi/english/world/south_asia/newsid_1619000/1619252.stm

chance of being discovered. Controls may be more difficult to institute, except perhaps for the fissile materials.

System elements (2): impeding and intercepting transportation

Nuclear weapons, components, and materials are most likely to originate in the Eastern Hemisphere, particularly Asia and adjacent European Russia. Reactor grade material exists in most countries, including Mexico and parts of South America that have nuclear power industries, as well as in Canada (where it is likely to be safeguarded better than in Latin America). In addition, it may be prudent not to ignore the possibility that weapons-grade material and/or weapon components could have been hidden away in South Africa, Brazil, or Argentina when those nations' nuclear weapon programs were terminated. But clearly, the main threat is from Eurasia.

Very loosely, transportation can be considered in three categories: (1) transportation within Eurasia, including crossing national borders; (2) transoceanic transportation to the Americas, either directly to destinations within the US or to other nations for transshipment; and (3) movement from Canada, Latin America, or Caribbean nations to the US. As a variation, ports in Africa could be used to facilitate transshipment from Eurasia to the Western Hemisphere.

There exists a large number of potential routes within Eurasia; these are not treated explicitly in this paper. Some of these involve movement across nations, such as Germany, that have effective security, while others (or other parts of the same routes) will be through areas with poor or nonexistent security. US relations with these nations vary from excellent through hostile. These routes should be described in some detail, and analyzed for opportunities for the US to influence and aid security. There are three specific purposes for doing so. The first is to develop a detailed understanding of the threat paths. The second is to identify opportunities to impede the paths—unilaterally, bilaterally, or through multinational arrangements. Third, if we can identify the paths along which terrorists might be able to move contraband to ports of debarkation with the least chance of being interrupted, we may be able to prioritize inspection of arrivals at ports in the US (or other western hemisphere nations with their cooperation). So, for example, a ship arriving in Baltimore from a suspect port of embarkation would receive greater scrutiny than one that sailed from Southampton or Rotterdam.

Radioactivity sensors are generally short range, and therefore not suitable for broad area searches. Major border crossings or other transportation hubs provide "choke points" and therefore an opportunity to channel shipments through positions where they can be brought close to detectors; busy crossings allow for the efficient use of detectors, i.e. they would not be idle much. However, because these crossings are busy, only very small delays due to searching can be tolerated without causing serious disruptions. One approach—as yet only partially proven—is to place nets of radiation sensors along the

road (and rail) networks that lead into and out of transportation nodes. These would detect and isolate suspicious vehicles with a suitably low false alarm rate.

Smaller numbers of sensors--either unattended or hand-held—might be used at secondary and minor border crossings. However, in order to be useful, unattended sensors require a responding force. Since affordable radiation detectors are subject to high false alarm rates, response forces could be overburdened. Guards at small crossings could have more time to search with hand-held detectors than officials at major crossings would. But by doing so they risk being attacked. Remote crossings are very difficult to monitor; they are also difficult places to bring hundreds of kilograms of contraband. An overt program of covert sensor placement rotated among smaller crossings could aid detection and deterrence.

Trains present different problems and different opportunities than do road vehicles. In some nations, officials ride international trains to perform duties such as checking passports. These officials have at least the time from the border crossing to the first stop to check for contraband, and possibly more than that if the stops close to the border are sufficiently small for anyone leaving the train to be checked by other officials.

Transoceanic shipment could be done either by sea or air. The terrorists could bring a weapon for detonation on arrival (i.e. at the seaport or airport of arrival), or attempt to bring a weapon or components into the US. Alternatively, they could bring a weapon or components to some location from which a weapon could then be brought into the US by another route. Such routes include: (1) offloading from a ship to a smaller vessel that either delivers a weapon to a target or lands a weapon or material; (2) by land from Mexico or Canada; (3) by short(er) range air or sea transport from Canada, Mexico, Central America, Caribbean island nations, or possibly northern South America.

Air travel across the Atlantic and Pacific Oceans currently enjoys a high degree of security, thanks in part to terrorist activities in previous decades. It seems unlikely that a complete nuclear weapon could be brought on-board an airliner, charter flight, or cargo flight that complies with FAA regulations regarding the departure of flights that land in the US. However, current measures ought to be reviewed. The only scenario for direct air transport of a bomb to the US that makes any sense appears to be one in which the terrorists attempt to fly a bomb into a major US airport and detonate it there before the airplane is unloaded and its cargo inspected. Opportunities to install detectors to detect attempts to bring smaller amounts of weapons grade materials onto airplanes bound for the US, or to bring them off the aircraft after arrival in the US, ought to be reviewed by the FAA.

Transportation by sea is a more troubling scenario. Roughly 200 times as much weight reaches the US each year by sea as by air. A ship carries much more cargo than does a large airplane, and that cargo is generally stored in larger containers and lots than is air cargo. Moreover, ships often follow much more complex routes than do airplanes. Older design freighters, break-bulk ships, and tankers are large and difficult to search. Modern container ships and “RO-ROs” are designed for quick port turn around. A

container ship could pick up a container carrying a nuclear bomb and arrive in a US city 15 days and 15 port calls later. Most US seaports are themselves within major cities that could be targets for terrorist attacks. Moreover, containers are made to be unloaded from a ship and loaded onto a truck or train. This could be done immediately, or the container could be held in a storage yard for days or even months.

Technology may help with finding contraband once a container has been unloaded in a US port. However, a simple radiation detector is not likely to find even a large quantity of fissile material inside a 40 foot container simply by inspection from the outside. And if the container has a bomb that is set to detonate on the ship or on the dock, such inspection would occur too late.

This part of the problem needs study, particularly in light of increasing globalization and rapid movement of goods. Several "handles" exist. First, except for ships coming from Canada, Mexico, or Caribbean nations, any ship arriving at a US port has a few days of travel from its last non-US port. This provides opportunity for search, given that suitable arrangements can be made. Second, the US government could consider making arrangements with shipping companies that trade convenience for security. In exchange for companies instituting security measures before their cargoes leave for the US, the US will expedite the arrive of their goods in the US. In essence: " if you take time to do security properly, we will spend a minimum of time doing security (and other things) when your shipment arrives." Exactly what these measures are remains to be determined. (Similar considerations could also apply to other forms of contraband including drugs and illegal aliens.) Third, the US could consider adapting measures developed by the FAA for air transport security to sea-transport. These include the FAA "trusted shipper" concept for profiling cargo. Ships bound for US ports would have to satisfy certain security criteria before they departed for the US. If not, they could be turned away. Modern communications technology may facilitate such measures.

Terrorists might not attempt to transport weapons or materials directly to the US from the Eastern Hemisphere. As an alternative, they might land elsewhere in the Americas and use shorter range transportation to make the final leg of the journey. They could come across the Canadian border or the Mexican border in a truck, either embedded in the large amounts of routine traffic associated with NAFTA commerce, or across minor border crossings, or even off-road. At major crossings, arrays of sensors might be used to monitor approaches on the foreign sides (with the cooperation of our NAFTA partners). Other crossings would be harder to monitor in a comprehensive way.

The terrorists might take a cue from drug smugglers (or hire drug smugglers), and enter the US using small airplanes or large boats. The planes could carry suicide bombers who head for urban centers (or similar targets), or bomb-making materials that are landed at remote sites and removed before authorities can track the plane and arrive at the landing zone. Similarly, if boats can sneak into US territorial waters, they can head either to targets or to places where a cargo can be off-loaded. Neither of these methods is likely to be used to smuggle a complete bomb into the US, unless it is a very small sophisticated weapon stolen from Russia. A crude bomb is almost certainly going to be

too large to be handled without a crane or other equipment[6]. However, hundreds of pounds of bomb components could be smuggled in this way. Numerous opportunities exist for moderate size boats to enter the US from Canada with very little chance of inspection by either Canadian or US authorities: for example, across the St. Lawrence River into New York State, across Puget Sound, or across the Great Lakes seaway that stretches from New York to Minnesota[7].

Over the past few years there have been reports of contacts and collusion among Russian organized crime, Colombian rebels (and their associated drug organizations), and Mexican drug smugglers.

For example, one might imagine a route by which a weapon manufactured in Iraq goes to Libya, and then south into very unsettled parts of Africa. From Africa it is smuggled into South America and to a part of Colombia controlled by drug lords who can be bought. The drug lords would then see to smuggling it into the US. While this may be somewhat fanciful, the progress of technology is likely to make it easier. However, each additional party or transaction involved in the shipment increases the risk of detection.

Counter-drug operations provide a good indication of how likely US authorities are to be in finding and stopping small planes and boats. From the US perspective, performance to date does not portend a high likelihood of stopping an attempt to bring in a weapon. However, from a terrorist's perspective, a 20%-50% probability of losing his almost irreplaceable nuclear device might be sufficient to dissuade him from risking the attempt. If the terrorists are smuggling nuclear materials and bomb components and have some spares, they may decide that the anticipated losses are tolerable. However, they might not adopt that view so readily if they perceive that interception of any shipment would lead to an intense investigation.

Close cooperation with authorities in countries that might be used as staging areas for deliveries could help swing the odds in favor of the US. There has been limited success in using this approach to impede the drug traffic. However, other governments might take a different view of being seen as the source of a nuclear attack on the US than they do of being a source of drugs to satisfy a US demand. We should remember that portions of some countries are not really under the control of their recognized governments. In Colombia, rebels control substantial parts of the land. In other nations—including Mexico--government presence is thin in remote areas. This is certainly true of Canada, where vast arctic and subarctic regions have few inhabitants. On the other hand, such remote areas are not the easiest places through which to bring sensitive modern technology.

---

[6] Under some circumstances, a van with a bomb could be driven off a small car ferry.

[7] "On the Great Lakes alone there are more than 4 million U.S.-registered small boats. How is it possible to filter the bad from the good given such numbers?" **Security is a Coast Guard Mission** By Stephen E. Flynn **U.S. Naval Institute Proceedings (October 1, 2001)**

Boats and ships are easier to stop and search than are airplanes. The Coast Guard does this routinely for suspect vessels. For vessels that refuse to stop when ordered, partial destructive measures such as shooting at propulsion or steering systems can be used. Stopping airplanes is more difficult. They obviously cannot pause in mid-flight. In the wake of the September 11 attacks, the US government has instituted a policy of destroying suspect civilian aircraft as a last resort. How well this policy can be implemented—particularly under ambiguous circumstances—remains to be seen.[8]

System elements (3): reducing the consequences-- reducing vulnerabilities to attack and freedom of perpetrators to move weapons within the US

We have considered three basic routes for terrorists to be in the US with a nuclear weapon in their possession: (1) they smuggle in a completed weapon, either stolen, bought, or designed and assembled by themselves; (2) they smuggle in the disassembled components of a weapon and reassemble it here; (3) they smuggle in nuclear materials and other components and attempt to build the bomb here. In any of these cases, they would have to move fissile material—either HEU or Plutonium, either assembled into a bomb or broken down into smaller pieces for transport—within the US.

DOE maintains the NEST team to search small areas, given that they receive some sort of cue. The NEST team searches for an emplaced weapon (or package of material); it does not search for material in transit. NEST would not be generally effective in conducting a broad area search.

Movement is most likely to take place via the road network. Air transport, and to a lesser extent rail, involve going through security. If what is being moved is a complete weapon, it is most likely to be large enough to attract attention if it is brought to an airport or train station[9]. Moreover, being caught trying to go through security with a smaller amount of fissile material would most likely lead to intense scrutiny and disruption of the operation.

The technology exists, partially proven, to deploy networks of sensors to monitor road systems (e.g. the roads leading into a major metropolitan area or some other potential target). This technology includes the ability to compensate for background radiation and to reduce the probability of a false alarm based on background signals to a very low level. However, this system can be distracted by vehicles that carry radioactive sources other than weapons. There is a substantial amount of movement of radioactive materials for a variety of reasons (principally industrial and medical). Were such a

[8] The policy was instituted to prevent a hijacked airliner from being used in an attack like those perpetrated on September 11. A plane would be shot down only if it became clear that it was not responding to routine and emergency air traffic control, and would pose a serious threat. A small airplane that does not seem to be heading toward a specific target (such as a large building) would be a much more ambiguous situation.
[9] A "suitcase bomb" stolen from a Russian source might be small enough to not attract much attention. Other weapons would be substantially larger.

system to be developed and deployed, it would be necessary to take steps to be better able to account for other movements of radioactive materials. Failure to do so could result in serious societal disruptions. Furthermore, HEU weapons are harder to detect than Pu-based designs.

Movements could be made using general aviation operating out of small airfields that have little or no security, or by water along rivers or coastal routes. Unless authorities were "tipped off", such movements would be very unlikely to be detected if the perpetrators were the least bit clever.

Delivery of a weapon to its intended target would most plausibly be attempted using some sort of conventional vehicle—car or truck, train, airplane, or boat. The final delivery route could originate from within the US, Canada, Mexico, or some other relatively close country, or a ship that stops off the coast. (While one can imagine a short range missile or artillery as a launch platform, this approach seems somewhat fanciful. It would entail extra risk and additional problems associated with acquiring the delivery weapons.) Of these modes, rail and road are the most amenable to monitoring. However, the practicalities attendant to the extent of the road and rail networks and the typical volume of traffic lead to the conclusion that routine, broad area monitoring would be prohibitively costly. Limiting monitoring to a few critical areas would reduce the cost and effort, but probably not enough to make it practical. Monitoring systems that are deployable on warning is probably overall a more practical approach.

For about a quarter century the US had a civil defense program to help survival of a nuclear attack. This enjoyed a brief, not very popular revival during the early 1980s. Programs based on evacuation and sheltering have basically proved to be unworkable from a practical perspective. Affordable programs to harden major structures against nuclear attack appear similarly impractical.

Some measures to make it very difficult for bombers to get close to major targets may be practical. However, if a nuclear weapon detonates almost anywhere in the US major damage will result and the credibility of the government will suffer. Cities could be ringed with networks of sensors that dramatically increase the chances of being detected the closer the perpetrators get to the urban centers. However, major US metropolitan areas tend to be large and sprawling with more than one "downtown". Population can be dense 50-100 miles from the geographic center. Practical issues—including jurisdictional ones—attend to the development of practical plans for deciding how close a suspect vehicle should be allowed to approach. Still, there is some value in damage limitation. Some thought might be given to a long-term transition in the design and operation of seaports to significantly reduce the probability that a bomb can be brought in on a ship and detonated close enough to the port and surrounding population centers to cause catastrophic damage. In the abstract, confining any detonation to several miles out to sea has more appeal than creating a similar stand-off from an inland city. However, there may not be any practical way to accomplish this. Similarly, one might

consider stricter rules regarding operation of aircraft within urban areas[10]. But this raises practical questions such as how those rules might be enforced, particularly for cities that have close-in airfields.

Two keys: information technology and international cooperation

As a general proposition, broad area searches for activities that have a low probability of occurrence are very inefficient. Cueing is extremely helpful. Indeed, for most of the individual activities associated with getting a nuclear weapon and bringing it to the US, the prospects of successful detection using broad area search are very remote, particularly if the search is based on trying to detect a radioactive signature. However, each threat path has a very large number of individual steps each of which has some degree of detectability. It would be worthwhile to design and develop a system that gathers relevant intelligence from a variety of sources, analyzes it for indicators of suspicious activities (and their likelihood), and uses that information to cue other surveillance systems. For example, while it may be impossible to search every container ship that enters Baltimore harbor, it may be practical to stop and search several miles out to sea a few that arrive from a particular part of the world during a three day interval[11]. Similar considerations would pertain to running trucks crossing from Canada through radiation detection systems, possibly in combination with other detectors. An intelligent analysis and use of cues might reduce the necessary level of effort to a manageable one. Modern information technology offers both sources of information and techniques to use that information.

Most of the activities that ought to be monitored are likely to occur outside the US. US efforts would benefit greatly from international cooperation. In the case of our close allies, mechanisms for cooperation already exist, and could be optimized to address this problem. Many—if not most--other nations will see this as a shared problem, and will probably be easy to convince to cooperate. The US may want to review the international nuclear control and non-proliferation regime to identify ways in which it might be strengthened to make it more difficult for terrorists to obtain and transport nuclear weapons. If appropriate, additional multi-national treaty obligations might be sought through the UN or another forum. Like the non-proliferation treaty, such obligations could be used to put obstacles in the path of governments that might seek to sponsor terrorist groups or otherwise help them in obtaining nuclear weapons.

According to numerous press accounts, the September 11 bombing, the anthrax scare, and the campaign to uncover and destroy the al Qaeda network have resulted in energizing—and probably expanding—international cooperation in law enforcement, investigation, and intelligence gathering. These cooperative efforts should be reinforced and expanded for the long-term campaign to counter terrorism, including constructing the system to defend against nuclear terrorism.

---

[10] Currently a 25 mile keep-out zone near DC and New York is mandated for general aviation. This clearly did not prevent the 9/11/2001 attacks.

[11] Following 9/11/2001, the Coast Guard increased the prenotification of port visits from 24 hours to 72 hours, and began searching ships before allowing them to enter some ports.

ANALYSIS AND DISCUSSION

Approach and assumptions

The threat of a terrorist attack using weapons of mass destruction (WMD) has received significant, and increasing, attention over roughly a decade. While defending against a nuclear attack has received less attention than defense against a chemical or biological attack, it is far from a neglected subject. Most reports have focussed on the threat of a nuclear attack, and on pointing out that there exist no devices (or individual systems) to prevent such an attack or to protect victims against its consequences.

The basic measures for opposing such attacks are well known: intelligence and counter-terrorism directed against potential perpetrators; measures to impede access to nuclear weapons and nuclear materials; deterrent measures aimed at terrorists or sponsoring states; the NEST team and related search capabilities; forensics and attribution measures; and to a lesser degree domestic consequence mitigation. Most analyses more or less conclude that none of these is currently sufficient to provide protection with a high degree of confidence. While many specific improvements have been suggested, none have been shown to hold any great promise of altering that basic conclusion. Some studies have sought to compare these different approaches[12].

This paper begins first from that well established baseline--there is not likely to be any "silver bullet" that will render the US safe from the threat of a terrorist nuclear attack. Second, it assumes that while the prospect of such an attack is currently remote, there is no reason for complacency, no reason to ignore the problem, particularly when the potential consequences of an attack are considered. Third, because the threat is generally considered less immediate than a chemical or biological attack, it is unlikely that large amounts of funding will be found to develop effective defenses. That point is reinforced by all the analyses that have failed to identify credible candidate defenses. Fourth, again proceeding from existing work, it assumes that many partially effective measures are possible. Some exist, others have been suggested, and still others may be developed.

Rather than comparing individual measures, this paper takes a systems approach: how can a variety of disparate measures be combined into a "system of systems" that, taken as a whole, greatly reduces the likelihood that a nuclear terrorist attack can be

[12] As a recent example, with earlier references, see: Fogarty, Jeff J. *Evaluating Strategies for Countering Nuclear-armed Terrorist Groups* These, Navy Post Graduate School, December 2000.

successfully accomplished? It proceeds from two basic principles—two orthogonal dimensions--in the design of complex defenses.

1. Design and build layered defenses. For any particular threat path, an incoming weapon has to get through a number of barriers, each of which reduces the probability of successfully reaching the target. The overall effectiveness is much greater than that of any one component measure. Discover and protect against all potential threat paths.

Finally, this paper proceeds from the assumption that nuclear weapons will remain scarce and precious commodities. As we look toward the future, some aspects of obtaining nuclear weapons—principally access to the technology--are likely to increase, while there may be offsetting declines in other areas. Some major factors are subject to management and control. These include: security of weapons and fissile materials in Russia and elsewhere; numbers of weapons and quantities of materials in Russia and other nuclear states; the size of nuclear weapons programs in other nuclear states; and the proliferation of nuclear capabilities. If the probability of a successful attack is perceived by potential perpetrators as being sufficiently low, they may be discouraged from expending the effort to try.

This deterrence through denial should be reinforced by establishing further penalties for failure, beyond not accomplishing the mission and losing a very costly weapon. If failure can be linked to discovery, punishments of various types can be inflicted. The risk of failure should be seen as multi-dimensional. In general, potential perpetrators should perceive that they will be significantly worse off if they try and fail than they would be if they don't make the attempt. At the least, they should expect to have wasted efforts and major resources, been discovered and had their ability to operate seriously impeded, and receive significant retribution. Lack of success alone is unlikely to be much of a deterrent to a group that sees time as being on its side.

The subject of what constitutes practical and significant retribution and punishment is not dealt with in this paper. But it is worth careful analytical attention. Just as the US has been shown to be vulnerable to attacks by other than military means (including information and economic measures), terrorist organizations may be vulnerable to much more than ordnance and arrest.

The threat

This report focuses on attempts to attack with nuclear explosives (referred to here, as elsewhere, as nuclear weapons), but it also deals with radiation dispersal devices (RDDs, devices designed to cause contamination by dispersing radioactive material). While RDDs do not produce the major sources of damage of a nuclear weapon—blast and heat—they do produce the health and property hazards associated with contamination with radioactive materials. RDDs share some other characteristics with nuclear weapons, but are far easier to assemble. An RDD can be made from any radioactive material—or any *ad hoc* mixture of radioactive materials that might be obtained--while a nuclear

weapon requires either highly enriched Uranium (HEU) or Plutonium[13]. An RDD does not require the sophisticated technology that is necessary to produce a supercritical mass. Conventional explosives have been demonstrated to be the weapon of choice for many terrorist groups[14]; all that is required to produce an RDD is to obtain a quantity of radioactive materials and mix it into a simple chemical explosive bomb[15]. A botched nuclear weapon design or assembly can detonate without producing a nuclear detonation, and therefore become a *de facto* RDD.

For brevity, this report will refer to any person or group attempting an attack on the US, other than the military of a sovereign nation, as "terrorists". This is more or less the common usage of the term. A short disquisition on the term terrorist is found in the Appendix.

Obtaining a weapon

The first step in designing a system to keep nuclear weapons away from US cities is to understand the possible paths by which they would get there. How would a terrorist or terrorist organization obtain a nuclear weapon?

The most straightforward path would be to get a complete, operating weapon. This could be a gift from a friend, or come about as the result of a theft. The "friend" could be either a minor nuclear power that otherwise lacks the means to deliver its weapons against the US, a nation such as Iraq that has had to conduct a nuclear program in complete secrecy, or a government or quasi-government (e.g. the Taliban) that participated in the theft of a nuclear weapon from a nuclear weapon state. For a nation that might ultimately be tied to such a weapon, there would be extremely serious questions regarding the wisdom of entrusting it to a terrorist organization. Moreover, if that nation had to sneak a weapon into the US in order to attack, it would have little ability to deter a US retaliatory attack, were its involvement to become known. On the other hand, the terrorist organization could be an arm of that government, and the deterrence could be of the form "there are others hidden at locations in US cities".

A terrorist organization that lacks a settled base would present the US with a difficult retaliatory problem. Were a nuclear or similar large-scale retaliation to be contemplated, it would have to take place on the territory of a nation that was not necessarily involved. One can imagine many paths that could put a stolen nuclear weapons into the hands of a well-financed or otherwise well-supported terrorist organization. Russia is the most frequently mentioned source of the weapon. They have many; security is not all that good; and inventory control may be less than complete.

---

[13] The fissile material has to be one or the other and has to have a controlled purity and uniformity.

[14] For example: The Murrah Building in Oklahoma City; the World Trade Center; Khobar Towers; the Beirut barracks; innumerable car bombs in Israel; standard IRA practices in England over several decades; Pan Am 103 and other airline bombings.

[15] Materials vary in their radioactivity and half lives. Isotopes that decay quickly can be cleaned up simply by waiting a few days, while others remain extremely hazardous for thousands of years. Similarly, elements differ significantly in those chemical properties that affect how likely they are to enter people's bodies as the result of exposure, and to be retained.

Organized crime and official corruption are major problems in Russia today. Moreover, Russia is known to have produced small modern nuclear weapons ranging from moderate yield SLBM Reentry vehicles to atomic demolition "suit case bombs"[16].

To be useful to a terrorist, theft of a Russian weapon would almost certainly have to be accompanied by a source of expertise that would allow the thieves/terrorists to move it without destroying it, and to fire its detonation circuitry. However, they would not have to obtain both at the same time. Lacking the expertise, they might steal one (or by a stolen one) were the opportunity to arise, and then seek the relevant expertise later.

Russia is not the only nuclear weapons state. France, the UK, Israel, India, China, and Pakistan all have them. For a variety of reasons, these are all considered to be less likely targets of theft than Russia is, but cannot be excluded. Pakistan has quickly become a state of special concern.

Theft or diversion of a US nuclear weapon from a facility in CONUS will not be considered. While all sorts of fanciful scenarios might be concocted, it is extremely unlikely that any thieves—assuming they could actually get their hands on one and abscond with it—could remain at large long enough to figure out how to bypass the systems that exist to prevent unauthorized detonation.

If thieves cannot get an intact weapon, they might attempt to steal all of the components, or at least those components that are critical and very difficult to build, including the assembly of fissile material. This operation would almost certainly have to be conducted by, or at least with the guidance of, experts. Having some confidence that the device would work would almost certainly require some form of partial testing[17], particularly if some components cannot be obtained and have to be built and integrated into the weapon. That would require an expert who knows what to test for. Building a nuclear weapon is not generally a "mix and match" affair; the components for one design would not necessarily work with another design. For example, the geometric design of the chemical explosives will depend fundamentally on whether the weapon is a gun-type or implosion device, as will the design of the circuitry. Timing requirements for the two design types are very different.

If a gift or theft cannot be arranged, the terrorists would have to design and build their own weapon. Volumes have been written on this subject, and won't be repeated here. The terrorists would need four basic things: (1) a sufficient quantity of HEU or separated Plutonium; (2) the other components of the weapon; (3) a detailed design; and (4) expertise. Unless they are resident in a state that has weapons grade material, they would have to transport the nuclear material across national borders.

---

[16] Public information on "suitcase bombs" is based primarily on dramatic statements by former Soviet general Lebed. Although his statements could not be confirmed, and were recanted somewhat ambiguously, the possibility that these exist is taken seriously.

[17] That is testing of individual components, or of systems of components short of a nuclear detonation. If they steal the fissile material assembly for a proven design, there would be little reason to test it; they would want to test the other components that trigger the nuclear reaction. Testing the nuclear explosive would destroy a valuable asset and risk revealing their activities.

To some degree, these can be traded against each other. For example, the less complete their design, the more expertise they will require.

They would also have to have the expertise to know that the nuclear material they obtained was actually as advertised. The degree of enrichment and chemical purity is important. If they don't get exactly the material called for in their design, they would have to design to the material that they have. Making the necessary adjustments could call for not just a skilled technician, but a knowledgeable engineer or physicist.

Testing would be a major issue. Unless the weapon were built exactly to the plans of a proven design by a real expert (probably one having experience with that design), some testing would be required to know that the device would actually detonate and produce a nuclear yield. This almost certainly couldn't be a full up test, i.e. one that produces a nuclear explosion. A successful nuclear explosion would most likely be detected, and attention would be brought to bear, making plans for covert delivery much more difficult. In addition, it would consume a large amount of valuable nuclear material. Partial tests would have to be conducted by someone who knew what to measure and how to interpret the results.

In designing and building their own device, they would have two basic choices. They could opt for either a simple gun-type device, or an implosion device. The gun-type is by far the simpler design, and requires much less precision. But it can only be built with HEU, and requires more nuclear material than does a plutonium implosion device. Although small gun-type devices are possible, a crude one is likely to weigh about a ton. Some experts speculate that a gun-type device could be built without testing and still have a reasonably high likelihood of producing a nuclear yield. An implosion weapon would almost certainly have to be tested, although significant assistance from an expert could greatly reduce the amount of testing required.

A weapon could be designed and built abroad and smuggled into the US, or alternatively, a terrorist organization could attempt to smuggle materials and components into the US and build the weapon here. These two cases would present very different challenges to the perpetrators and to authorities attempting to interdict the smuggling operation. A hybrid situation would arise if the terrorists attempted to assemble the weapon, or major components of it, in Canada or Mexico and transport it across the US border. Shipment from almost anywhere in the world would involve landing at an air or seaport; access from Canada or Mexico is much more open.

An RDD could, at least in principle, be assembled in the US entirely of materials obtained within the US. One advantage to the terrorists of assembling an RDD rather than a nuclear weapon is its relative simplicity of design. Little specialized expertise would be required, and the process could be accomplished much more quickly. Moreover, the amount and type of radioactive material used would be far less restricted, almost unrestricted. On the down side, most nuclear materials are under relatively tight

security in the US. However, access to some quantity is not overwhelmingly difficult even for amateurs.[18]

The possibility that terrorists might attempt to disperse radioactive material by sabotaging a nuclear power plant or other nuclear facility has been talked about and cannot be dismissed. However, from the perspective of the threat posed and from the perspective of the possible defenses and responses, this differs fundamentally from attempts to acquire and use a nuclear weapon or RDD. It will not be discussed in this paper.[19]

Bringing a weapon to the United States

The paths to obtaining a weapon described in the preceding section involve different degrees of access to engineering and industrial capacity. If the malefactors obtain a complete functional weapon and can defeat any protective devices or interlocks it might be fitted with, they only need to bring it to their target, possibly dissembling it for shipment and reassembling it for use. Similarly, if they obtain all of the components of a complete functional weapon they have only the added step of assembling it (with the application of the necessary expertise). Designing and building a weapon from the proper fissile material requires access to engineering and sophisticated manufacturing. And enriching or separating material would add a requirement for considerable industrial capacity.

How much industrial and engineering capacity would be required (away from prying eyes) will influence the available paths.

The most likely sources of a weapon are in Eurasia; with the exception of the US, all of the world's current active nuclear weapons programs and activities appear to be located there. Russia is the potential source that is most discussed for complete weapons and nuclear materials. Either might also be obtained by theft or diversion in China, India, or Pakistan. Britain, France, and Israel are less likely sources[20]. Iran, Iraq, and DPRK

---

[18] See, for example, Silverstein, Ken, **Harper's Magazine** Nov, 1998
The radioactive boy scout: when a teenager attempts to build a breeder reactor. (case of David Hahn who managed to secure materials and equipment from businesses and information from government officials to develop an atomic energy radiation project for his Boy Scout merit-badge) *(*printed from FindArticles.com, located at http://www.findarticles.com.)

[19] In principle, a terrorist organization could sabotage a nuclear facility and take advantage of the resulting confusion to obtain nuclear materials. This does not, however, appear to be a practical approach. It would call attention to the terrorists.

[20] Some analysts have argued that mixed oxide reactor fuel—MOX—presents a major danger for diversion to making bomb material because it is rich in plutonium and not highly radioactive. They further argue that MOX reactor fuel assemblies are a prime candidate for theft because they are part of the commercial structure, not the military structure, and are therefore not sufficiently secure. Most of the world's MOX is found in the UK, Germany, France, Belgium, Switzerland, and Japan. See The Times (of London) THURSDAY MAY 31 2001 "Nuclear plant is terrorist threat" BY MARK HENDERSON, SCIENCE CORRESPONDENT; The CornerHouse (2000) Briefing 17 - How Not to Reduce Plutonium Stocks: The Danger of MOX-fuelled Nuclear Reactors. This subject is also treated in **The Disposition of Weapons-grade Plutonium as**

(North Korea) are all cited as states having nuclear weapon ambitions and possible political sympathies and contacts with groups that might be suspected of considering attacks on the US. These three are prime suspects to be "state sponsors" of nuclear attacks on the US.

A bomb might be assembled or otherwise prepared for shipment toward the US in almost any country; however, life would be easier for the terrorists if they could operate in a state where they are unlikely to be interfered with. This could be the case in a "friendly" state (i.e. one that might be a sponsor or at least sympathetic), one in which official corruption could be exploited, or one in which government control is mostly absent in significant areas.

Were a secure shipment route to be found, there are many locations in Africa that could be used for assembly and/or preparation for shipment to the US. That route could be by air or sea, or some combination of the two. For example, flights from Iraq or Afghanistan to a friendly country in Africa (e.g., Libya) could be made with little likelihood of US interference.

Another possible, although less likely, source of materials and expertise might be found in the remnants of South Africa's abandoned nuclear weapons program[21].

One way or another—whole or disassembled or as components and materials—the weapon would have to be shipped across either the Atlantic or the Pacific to the western hemisphere. It could go: (1) directly to a destination within the US; (2) to Canada, Mexico, or a Caribbean nation from which a short movement into the US could be staged; (3) to South America for further work and subsequent transshipment to the US, either directly of through a neighboring country; or (4) to some at-sea rendezvous where it would be transferred to a small ship or large boat for entry into the US.

This transoceanic shipment would have to be either by ship or on a large aircraft having the requisite range capabilities. Shipments from, for example, western European countries directly to the US (or to Canada) might maximize exposure to detection. That could be minimized by shipping from an eastern hemisphere country where security could be avoided--by government intervention, by corruption, or by lax security in general—to a Latin American country with similar characteristics.

For a number of reasons, shipment by sea seems more likely than shipment by air, but air transport cannot be ruled out. By weight, roughly 200 times as much is imported

---

[21] The materials appear to have been accounted for by the IAEA.

into the US by ship as by air. For Canada the ratio is somewhat lower.[22] However, there are many more airplane landings than there are ship arrivals. Large objects are more easily sent by sea; large objects sent by air are likely to be conspicuous. Moreover, airline security is much tighter than cargo shipping security, due in part to past terrorist activities. Therefore, shipping an entire bomb or all of its components by air seems very unlikely—although not impossible.[23] However, they might consider sending small components by air through a varied set of routes.

In shipping directly from a European or Asian port to the US, the number of border crossings that are required would depend on the specifics of the path from origin to port. Air transport has the advantage of not requiring that international land borders be crossed in order to reach a port. It has the obvious disadvantage (to the perpetrators) of being subject to much tighter security than is sea transport. The US government imposes security restrictions on flights that depart foreign airports for destinations in the US. Moreover, packages in the 100-1000kg range are much more anomalous at an airport than they are at a seaport. Such large parcels arriving at an airport in the US are likely to receive scrutiny.

Assuming that the terrorists could manage to ship from an airport where security could be subverted or circumvented-- one could imagine the use of a chartered cargo flight that departs from an airport at which officials have been bribed--terrorists might seek to avoid security at the US end by designing a bomb to detonate on an airplane, either just after it has landed, or while it is still in the air over a populated area. This would require a degree of sophistication in the design and operation of the weapon. Moreover, not all international airports are close to populated areas, and not all approach routes go over populated areas. But planned routes could be altered by hijackers. It may still be possible for couriers carrying bomb components or small quantities of nuclear materials to circumvent security at US airports through collusion with organized crime, by infiltrating airport security[24], or by bribery.

Airline security is primarily a consequence of several decades of hijackings and terrorist attacks on airplanes, particularly those that carry passengers. The considerations behind aviation security systems don't apply to ships, where small amounts of explosives are of much less consequence and passengers and cargo are seldom on the same ships. Moreover, the volume of cargo that moves by sea and the general structure of sea cargo handling do not lend themselves to security procedures that are similar to those that have been developed for aviation.

Sailing a weapon into a seaport city and detonating it there is probably the most mentioned means of unconventional nuclear attack on a US city. Most of the goods and materials that are imported into the US arrive via ship. Very few of these ships are US flag carriers. A ship can arrive at a US port directly from almost any seaport in the

[22] Source: Bureau of Transportation statistics. http://www.bts.gov/itt/natf.html
[23] Unless terrorists can really get their hands on a Russian "suitcase bomb".
[24] For example, by arranging to get their members, sympathizers, or paid helpers jobs in security or positions that allow them to escort parcels around security.

world, and can make many stops before arriving at that port. An item of cargo can remain on a ship for several port calls before it arrives at a US port. Neither security nor protection of US interests should be assumed at many ports. Ships typically carry large and bulky cargoes; a one-ton package would not draw much attention based solely on its size.

Coast Guard and other US agencies have the right to board ships as they enter US waters (and under some circumstances in international waters). However, in practice few ships are inspected before they either dock or anchor in a harbor. For example, despite the intense efforts associated with intercepting water-borne drug shipments, it is estimated that more drugs are landed by sea than are prevented from landing. Thorough searches of medium to large displacement ships are very time consuming. Unless ships are anchored and searched well beyond the damage radius of a nuclear weapon, once a ship is anchored (or docked) and awaiting search or unloading, it is already too late. If the terrorist is clever, he will arrange the weapon so that he can detonate it if there is a danger that it will be discovered.

For about two decades cargo shipping has been undergoing a revolution. Container ships for most items and roll-on/roll-off (i.e. "Ro-Ros") ships for transporting vehicles have been replacing traditional "break bulk" ships. These newer ship types are designed to minimize the amount of time that ships spend in port, time which is primarily determined by loading and unloading. Container ships move among ports much more quickly than older freighters not because they sail faster, but because they spend much less time in the ports. Port calls that used to take days can now be accomplished in hours; In some cases a ship can visit more than one port in a day, loading and unloading cargo in each. The concept is to pack cargo into standard size containers (8'X8'X40' and 8'X8'X20') that can be easily removed from a ship by a suitably designed crane and can be placed—either immediately or after some time in storage—onto a railcar or a highway truck. While this transition has faced resistance from several powerful elements of the shipping industry, it has been taking place inexorably.

Shipping containers are sufficiently large to contain a nuclear bomb and a significant amount of shielding. Unlike a large parcel placed on an airplane, a standard container with a bomb in it would look like any other standard container. Moreover, searching containers is very time consuming and labor intensive, and may not even be possible without unloading the ship. A typical ship would be carrying hundreds of them. The largest "Post-Panamax" class ships carry more than 6000 20' container equivalents[25]. Thoroughly searching all containers on any ship entering a port would subvert the basic reason for building such ships—to speed commerce. New concepts are under consideration to load and unload stacks of containers rather than single containers, and to outfit ships with container-carrying barges that would proceed to a dock (or a destination farther into the harbor or upriver from it) after being taken off the ship with a crane[26][27].

[25] http://www.ldeo.columbia.edu/eeg/e9282_lect06/tsld001.htm; http://www.k-line.com/Company/news/000420Post-PanamaxCtrshp.htm; http://216.254.0.2/~peterc/nicaragua/drycanal/containr/shipng02.htm

[26] Giles, D L (1997), "Faster Ships for the Future", Scientific American, October 1997

This system provides several opportunities for terrorists to employ a nuclear weapon. A bomb could be detonated inside a container while it is still on the ship. The amount of damage that would be done would depend on the location of the ship *vis-a-vis* nearby buildings, port structure, or other shipping, and on the yield of the weapon. A weapon that did not fully function and only produced a yield of a few tens of tons deep within a load of containers might well destroy little more than the ship that carried it. Moreover, under those circumstances the terrorists (assuming they were suicide bombers) would likely have no access to their weapon after it was loaded on the ship, and might have to rely on remote detonation functioning correctly after several days at sea[28].

How much damage a weapon can actually do if detonated while on-board a ship will depend on the design of the weapon, how it is loaded into the ship, where the ship is docked or anchored, and the specific geometry of the seaport and adjacent cities. In some cities the trend over the past few decades has been to remove port facilities from prime downtown real estate. A 100kt weapon that explodes in the hull of a ship will probably not have its primary damage effects attenuated much by the presence of the ship and cargo. However, if the weapon malfunctions and only produces a yield of a few tons, the damage may be confined largely to the ship. A weapon that produces no nuclear yield, or a reasonable size RDD, may well have its effects limited to the inside of the ship.

The bomb-carrying container could be unloaded onto a dock (or into a storage yard) for detonation after the ship that carried it in was far out to sea. The weapon is likely to be more destructive, all else being equal, if it is detonated within a port facility rather than onboard a ship in the harbor. This would depend on the specific characteristics of the port in question. Some, like Baltimore, are close to densely populated areas. While many commercial ports are in, or adjacent to, coastal cities, others are inland. Freight moves up the Mississippi River, and through the St. Lawrence/Great Lakes seaway to midwestern cities such as Chicago. Alternatively, if the container is not inspected before it leaves the port area, it could be transported by truck or rail to some other location, either for further work or for detonation. Transfer to a smaller ship bound for an interior port is also possible.

Terrorists could opt for an approach that would be less dramatic and, for them, less risky. Rather than attempt to ship an entire assembled bomb in one container, they could make multiple shipments of components hidden within items that are themselves packed into boxes within shipping containers. These could then be delivered or otherwise retrieved, and transported to a location for assembly.

The terrorists could elect to ship their goods to Canada or Mexico. Official corruption in Mexico is well documented. Even if the Fox administration is serious about reform and pursues a vigorous program to stamp out corruption, corruption is likely to

---

http://www.sciam.com/1097issue/1097giles.html

[27] Sid French and Trevor Rabey, Container Ships for the 21st Century A radical idea, a work in progress

[28] This depends on how the containers are loaded on the ship (i.e. how accessible they are) and whether the terrorists are crew members.

persist for many years, if not decades. Moreover, Mexican airports and seaports have some of the same congestion problems that their US counterparts do. The Canadians can be expected to be more diligent than the Mexicans about finding dangerous contraband, although some consider Canada to be something of a haven for terrorists provided they don't practice their trade on Canadian soil. Canada is, however, a large country that is sparsely populated throughout most of its territory. If successfully landed, the bomb or components could then be transferred to a train, or truck, or even a car that would become part of the enormous volume of legitimate traffic that crosses into the US each day. While there are opportunities to inspect at major border crossings, realities dictate that the likelihood that any specific vehicle will be inspected will be low.[29]

If the smugglers wish to avoid that risk, they could opt to sneak into the US along other routes. The Canadian border is very long and largely unguarded. Crossings include small modern roads that are not patrolled with any regularity. There are undoubtedly dirt roads and jeep trails that are known and used locally. Significant water-borne traffic moves between the two countries—at least in the warm months—across the Bay of Fundy, the St. Lawrence and Niagara Rivers, several of the Great Lakes, and Lake Champlain. Smugglers might also attempt to fly small aircraft (including helicopters) outside the air traffic control system and land at small airfields, remote airfields, or minimally prepared locations.

All of these techniques have been used by illegal migrants and drug smugglers for access from Mexico and, except for ground transport, from Caribbean Island nations. These methods have included using watercraft and aircraft for single trips, i.e. using them once and abandoning them. However, these routes receive extensive monitoring from US authorities. Drug smugglers, in particular, can afford to lose a substantial fraction of their cargo (e.g. 10-50% in some cases). Losses can be compensated for by the large mark-up the drug market will support. Smugglers of scarce nuclear weapons or components are not as likely to accept that potential level of attrition. On the other hand, they may be able to find specific routes that have a very low probability of being interdicted.

Terrorists and smugglers have been known to transfer on the high seas from ships used for long range transport to smaller vessels that would be used in landing. In principle, a nuclear weapon could be smuggled this way. A ship could carry a modest size boat into which a weapon or materials is packed, and launch that boat while at sea. Or it could rendezvous with a smaller craft. Transferring a tonne or so at sea is not a trivial exercise, but is well within the capabilities of freighters that are equipped with small cranes. Unless there were something suspicious about the boat the attracted attention, it could proceed to almost any US port—major or minor—where the bomb could be detonated or unloaded onto a truck. Most US coastal cities have marinas with dozens to thousands of pleasure craft where one more boat could go almost unnoticed. Those that are in close proximity to populated areas could be easy targets. Well-traveled waterways lead into many places including Chicago, Miami, New York, and Washington.

[29] See, for example, "Beyond Border Control", Stephen E. Flynn, Foreign Affairs Vol. 79 No. 6, November/December 2000.

A more complicated route could involve South America. South American ports (including airports) could be used as transshipment points for bombs, components, or materials moving from the eastern hemisphere. One might imagine a route from south Asia to Africa, on to South America and thence to Mexico or Cuba or the Bahamas for smuggling into the US. South America has several aspects that might be exploited. In some countries official corruption or indifference might be exploited to assure unimpeded movement. Some areas are under the *de facto* control of entities other than the government, including organized crime and insurgents. Drug smugglers already have routes and networks developed for bringing contraband north to the US. In many areas antipathy to the US runs deep. Finally, there is the legacy of nuclear programs in Brazil and Argentina. These existed for about a decade beginning in the 1970s[30]. Some exploitable expertise and materials may possibly exist.

Reactors exist in Argentina, Brazil, Mexico, and Cuba. These could become sources for radioactive materials to make an RDD.

Moving a weapon within the US and delivering it to its target

Once inside the US the terrorists would have a great deal of freedom to move their weapon (or components) about, unless they do something to arouse enough suspicion to generate a search warrant or a traffic stop. They would have three basic options for delivering it: (1) transport it to the target, emplace it, and detonate it; (2) bring it to the target in pieces, assemble it *in situ* and detonate it; (3) mount it on some kind of delivery platform and launch it toward the target. The third would be the most complex.

Nuclear weapons would range in weight from perhaps 50 kg to more than a tonne. To have something at the lower end of that range, the terrorists would have to either steal a relatively sophisticated weapon, or design and build a plutonium implosion device. Were they to build an implosion device, they would probably encase it in shielding, which would significantly increase the mass.[31] They are likely to have a weapon that would require a small motor vehicle to move it—a car or light truck, or modest size boat, or a light airplane or helicopter.

These weapons could be carried in a great variety of general purpose vehicles. Once inside the US, they could be moved by small trucks, or embedded in cargo in a large truck. For the larger devices, loading machinery such as light cranes or forklifts would be required to get them into the vehicles. They could be put onto trains or scheduled cargo aircraft, but special arrangements would almost have to be made in order to do so. Cargo aircraft could be chartered. Trains would take them into the middle of cities that are served by train; airplanes would be useful only for attacking those cities

[30] See: http://www.fas.org/nuke/hew/Nwfaq/Nfaq7-4, and numerous other sources.
[31] Plutonium is "brighter" than HEU, i.e. it produces a radiation signature that is easier to detect. HEU produces no neutrons and a much lower gamma signature. The shielding would be useful for attenuating this signature, and for protecting those involved in the production, transport, and delivery.

that have close-in airfields[32]. Train stations and airports would not be the most effective places for detonating RDDs.

Large boats or small ships could carry these weapons, but away from the coasts delivery by water would put important limits on where the weapon could be delivered to, and where it could be assembled and loaded. Some cities—e.g. Washington, New York, Philadelphia, Baltimore, Chicago—could be reached by boats launched from relatively sparsely populated rural locations. But these cities could also be reached by road.

A device could also be assembled *in situ*. Doing so would require many trips into the target city carrying potentially detectable and incriminating components, but it might be viewed as less risky than attempting to transport a large radioactive device.

Devices could be delivered by general aviation aircraft that either land at small general aviation airports close to the target, "emergency" land on highways, crash near the target, or detonate their cargo while still airborne. These could be piloted by risk-takers or by suicide bombers (or by dupes), or operated remotely. These flights could originate within the US, in Canada, in Mexico, on some Caribbean island, or even in Colombia. Organizations that smuggle drugs into the US could be hired to do the job.

As an extreme scenario, a weapon could be mounted on a UAV or missile either somewhere within the US, or across the border in Canada or Mexico. It seems fairly unlikely that a terrorist group could produce a makeshift weapon and a makeshift ballistic missile. The missile would probably have to be large, and the weapon would have to be designed to withstand the launch and flight of the missile. It is conceivable, but not very likely, that a group could obtain both a complete weapon and a missile configured to carry it—either by theft or from a state sponsor—and smuggle both into the US or a nearby area in Canada or Mexico. The terrorists would face similar problems with the missile that they would face with the weapon, including obtaining, smuggling, possibly disassembling and reassembling, and gaining some degree of confidence that they could make it operate. Perhaps the most likely of these unlikely scenarios would be to obtain a Russian nuclear artillery round and a small unguided rocket (e.g. FROG or Katyusha type) to carry it.

Were the group to contemplate delivery using an unpiloted air vehicle (UAV), by far the simplest route would be to use a conventional small airplane and equip it to fly autonomously, or by use of a data link to a site on the ground. This technology is not trivial, but is fairly well known. However, putting a pilot in the airplane would be far safer operationally, although perhaps not for the pilot. A UAV could prove more problematic to control, and might have much more trouble with air traffic control systems.

Weapons that are detonated manually—either at the scene or via a datalink to a remote location—are simpler and more likely to work than those which have to be designed with fuses that work with delivery platforms like missiles.

[32] Unless a suicide bomber detonates the device on-board the airplane while in the air over a target city.

Launching a weapon from Mexico or Canada would avoid two potential sources of detection: smuggling contraband into the US, and moving and storing contraband within the US. Terrorists could also avoid these problems by attempting to deliver a weapon with a vehicle that can bring it within lethal range of an intended target before US authorities have a chance to examine it. The primary candidates are ships bound for US ports from foreign ports of embarkation, and international flights, as discussed above. Trains travelling from Canada (or possibly Mexico) are also possible modes of delivery, but there are relatively few of these, and they are subject to possible border inspections. A ship (or even a submarine, one supposes) could be brought to within a few miles of the US coast and used to launch a small craft carrying a weapon. That small craft could enter a major seaport with somewhat greater freedom of movement (and freedom from scrutiny) than a ship would have. Alternatively, it could enter smaller bodies of water and possibly obtain rapid anonymity among many other boats. It is far from clear, however, that transloading onto a small boat would provide any operational advantage over leaving a weapon onboard a ship and sailing it into a seaport.

Delivery via a commercial transport aircraft would be more problematic for the terrorist. The goal would presumably be to place a bomb on an airliner or charter, or cargo flight bound for a US airport, and have it detonate while the airplane is at its destination airport. If the bomb detonates successfully, this would almost certainly destroy the airport. Airplanes being less substantial than ships, were the weapon to malfunction it would still cause considerable damage to the airport. An RDD would similarly damage the airport. However, some planning would be necessary: an RDD or malfunctioning weapon that detonated just after an airplane touched down might do little more than spread radioactive material across a runway. A fully functional weapon would cause destruction to the area around the airport. However, the trend has been to remove international airports from cities to more sparsely populated areas, although fields like Washington Dulles, JFK and Newark in New York, LA International, San Diego, and San Francisco are close to densely populated areas.

An alternative approach would be to detonate the weapon while the airplane is approaching the airport over a densely populated area. Doing so would almost require that someone on the plane detonate the weapon. There is some risk that an approach path would be assigned that avoids overflying juicy targets.

Air traffic is generally much more closely scrutinized than is ship traffic. A weapon weighing several hundred kilograms to more than a tonne would be difficult to get onto a regularly scheduled flight without close inspection, including cargo-only flights. A charter could be arranged. However, flights bound for the US are subject to aspects of security procedures as determined by the FAA. A flight cannot just show up heading for an US airport; its origin, flight plan, and arrival are controlled. An airplane could be specially purchased for the purpose, and perhaps disguised as the private airplane of a foreign potentate or business magnate. Were the subterfuge to succeed, the dignitary who lent his name to the endeavor would be in the hot seat; that alone ought to deter agreement to the scheme.

Summary

The preceding discussion illustrates two basic points:

1. There are a number of plausible paths for terrorists to deliver nuclear weapons against targets within the US. None of these are easy, and all face major obstacles, although legs of some threat paths appear very difficult to interrupt.
2. The fact that these obstacles exist demonstrates that elements of the system to protect the US against terrorist nuclear attacks already are in place. However, it is neither true that these elements are sufficient to provide confident protection, nor is it true that the architecture of a system really exists.

Constructing a defensive system of systems: Purpose/Philosophy of the system

Considering the consequences of a successful attack, it is tempting to announce a goal of building an impenetrable shield, of providing a system with a 100% probability of stopping any such attack before it can do any damage. For very basic reasons, that is an unachievable goal; announcing it would doom the effort to failure.

The basic nature of the threat mitigates against announcing an impenetrable defense as a goal. As discussed above, there are a large number of possible threat paths, all of which would have to be completely closed. This is a prescription for a prohibitively expensive system. By rough analogy, it would be like attempting to build several different complementary versions of President Reagan's Strategic Defense Initiative. Whereas SDI had to contend with only one threat path, this would have to deal with several simultaneously. Extending the analogy a bit farther, one could expect that this would be a harder sell (to Congress and the public) than was SDI. SDI was directed against thousands of existing Soviet weapons that were assessed to be real tested and deployed systems. This system would have to be sold on the basis that it was there to stop a very small threat that very likely does not, as yet, exist as a threat in being. Moreover, elements of this system could well raise civil liberties questions if one is to insist on very high effectiveness; SDI would have been a military system that was supposed to function in space.

The system discussed in this paper exploits the basic nature of the threat. Potential perpetrators will have very few weapons, most likely only one. Even in the absence of any new defensive measures, getting that weapon and delivering it would be a complex affair. Being caught in the act would carry extremely serious consequences, not just for the attack that would be foiled, but for the ability to attempt future actions and most likely for the future of the organization(s) and/or government(s) involved. Furthermore, time is a critical factor. On the one hand, a slow, cautious, deliberate approach on the part of the perpetrators will maximize the likelihood that the device can be made to function properly, and that errors will not be made that reveal what the perpetrators are doing. A good way to get caught would be to detonate a device that malfunctions in a noticeable way (such as an explosion that does not produce a nuclear

detonation). On the other hand, the longer the process takes—and the more people that are involved--the more opportunity exists for them to be found and stopped. As a further complication, some components deteriorate over time.

This entire scenario is driven by the unique characteristics of nuclear weapons, particularly their destructiveness, scarcity, and unitary nature. Unlike the nuclear exchange scenario of an ICBM attack on a city, an attacker cannot produce success by overwhelming the defense, i.e. shooting 20 weapons to get one through with high probability. Similarly, unlike an attacker who has a quantity of high explosive, or chemical agent, he cannot hedge his bets by building 10 small weapons in place of one large one.

Even for a group that is supported by a state sponsor that is (or has surreptitiously become) a nuclear power, nukes will be rare and precious commodities. High attrition will be very hard to tolerate, which means that a (perceived) low chance of success may be a strong deterrent. This can be illustrated by considering chemical or biological attacks. Those agents are relatively cheap, and at some level can be viewed in terms of volume, not numbers. If a perpetrator faces a 10% chance of a successful chemical attack, he may think that to be acceptable, since the cost of the 90% of the chemical agents that is lost is low and the damage done by the 10% that gets through can be very high. The lost 90% can be replaced. Like drug smuggling, low success rate can be balanced by the low cost of what's lost and the high payoff for the small part that gets through. Now consider nuclear weapons. It is very unlikely that a perpetrator will have 10 weapons, and that he will want to accept losing several in order to get one through. If they are a criminal or terrorist group, they will obtain their weapon(s) by stealing (a Russian) one, or by smuggling small amounts of nuclear materials in order to assemble a home-made one. If they are state-sponsored, the sponsor is unlikely to have very many, and unlikely to let most of them go, particularly if US retaliation is in the cards.

Therefore, if a layered defense reduces the overall chance of success to much less than an expected value of one detonation, the attack may be effectively prevented.

Furthermore, if the bad guys *think*, or calculate that their chances of getting a single detonation are low, they may be effectively deterred. They may decide that the chances of success are too small to be worth the gamble, and look for another means of attacking the US.

One might think of this in the context of cost and likely payoff (from the bad guys' point of view). To pick a number, $50 million may buy one nuclear weapon, that overall they have only a few percent chance of detonating within the US. The same $50 million could buy a lot of chemical agent, some of which would almost certainly get through, with effects that, while not as devastating as one nuclear detonation, would nonetheless be severe and make their point. For that matter, it could buy an awful lot of firearms or explosives.

For the terrorists, the worst possible outcome would be to fail and be caught trying to do it. They would lose their one (or few) nukes, and be held accountable for a nuclear attack. They could expect severe retribution from the US on the grounds that they could well have more such weapons to use against the US or some other target.

This paper discusses the architecture of a system designed to allow a very low probability that a party attempting to use a terrorist nuclear weapon against a US city (or other major target), by any path, will be able to complete all of the steps that are necessary to achieve that end. The purpose of the system is to produce high confidence that any such attack will not succeed, and to deter attacks by producing among potential perpetrators very low confidence that they will succeed and not be found[33]. This approach is based on a layered defense, designed so that the overall leakage rate is such that the number of weapons any perpetrator could expect to get through over a reasonable period of time would be far below one, when he takes into account the number of weapons he could get his hands on. It is also based on maximizing the time required for the terrorists to conduct the necessary sequence of actions, and therefore maximizing the time during which they are exposed to detection and interdiction.

Responses to a defense.

When faced with a capable defense that cannot be circumvented, a rational attacker has three basic choices: (1) overwhelm the defense; (2) accept reduced effectiveness; (3) abandon the attack. He could attempt to overwhelm the defense by using enough weapons to guarantee that his attack will succeed. If he expects to lose 90% of his weapons, he will employ 10 weapons for each one that needs to reach a target. The approach leads to high attrition of weapons (or high weapon expenditure), but it produces a high expectation of success. With the application of enough firepower the attacker can expect to destroy all his targets. A terrorist with one nuclear weapon does not have the option to take this approach. Alternatively, the attacker could opt to proceed knowing that only 10% of his attack will get through and will have only 10% of the effectiveness he planned for. An attacker with a quantity of chemical agent sufficient to kill 100,000 victims might do this. If only 10% of his attack gets through, he will still expect to kill 10,000 victims. Although much smaller, that would still be a horrific attack. Some people—a lot actually—will be killed, and the goal of his attack was to kill a lot of people. A terrorist with one nuclear weapon has neither of these options. Either his weapon gets through or it doesn't, and the odds a 10 to 1 that it will not. Therefore the number of victims he can expect to kill is…ZERO. In that case, a rational player is likely to conclude that the attack is not worth the effort, particularly if he can expect to be penalized for trying. This difference of perspectives is basically the difference between a high expectation of a low, but meaningful level of success, and a low expectation of any success.

[33] We can expect that some of the immediate perpetrators, those that detonate the bomb, could be suicide bombers and would therefore not be deterred by an expectation of getting caught after the act. We aim to inculcate in the leaders of terrorist organizations (or supporting governments) that they and the "cause" will be found out and suffer significantly as a consequence.

Of course, one should not necessarily rely on terrorists making rational decisions. Faced with a low prospect of success, they may opt to go ahead anyway.

The system is based, in part, on deterrence through creating an expectation of denial plus high cost. The US should seek to create a situation in which the would-be attacker's calculus leads him to conclude that his attack is unlikely to succeed, and that the failed attempt will cost him dearly. That cost will include the substantial resources expended on the unsuccessful attack as well as substantial retribution. Moreover, the system in based on having those deterring expectations rest on reality: the attacker is likely to fail, and the cost of failure (or of success) will be high.

Layered defense.

As the discussion of threat paths shows, any attempt to obtain a nuclear weapon, bring it to the US and use it will consist of a fairly large number of consecutive steps, each of which has to be completed successfully. A layered defense simply refers to building impediments to as many of those steps as possible. Each layer reduces the probability that the step that it is aimed at will be completed, and contributes to an overall degradation in the likelihood that the process will be completed. If, for example, there are ten steps that have to be completed, and each one has an 80% probability of success, the probability that the entire process will be completed will be only about 10%. It is therefore useful to build as many impediments to as many steps as possible, even if those impediments are individually marginally useful.

The overall design philosophy can be summarized as:

- Low probability that a weapon can be successfully obtained and delivered
- Deterrence based on this and on high probability of discovery and retribution
- High public confidence in public safety
- Layered defense; multiple significant obstacles
- Force terrorists into a long, complex process

The system is designed to satisfy two primary goals:

1. Primary goal #1: Prevent the weapon from being delivered and detonated.
2. Primary goal #2: Establish confidence among the population that they are not in danger of catastrophic attack.

These are goals, not absolute requirements, and they are interrelated. It is generally accepted that terrorists have two similarly related goals in planning an attack. The first is to cause damage, and the second is to terrorize the population so that normal life is significantly disrupted. Hence, the goal of the defense has to be to prevent the terrorists from achieving theirs.

This paper focuses primarily on the first goal. However, serious attention has to be devoted to accomplishing the second after the first has been seen to. If steps are only taken to accomplish the first goal, we could wind up with a situation in which the likelihood of a nuclear attack is vanishingly small, but the "terrorist threat" to society is still strong. If the government has the ability to prevent a weapon from being delivered and detonated, but the public doesn't believe that, then terrorists will be able to achieve an important goal, even through hoaxes and false alarms.

On the other hand, public release of detailed specification of the defensive system as a means to obtain public confidence risks giving information to the terrorists, and therefore undermining the effectiveness of the system. Moreover, if the government convinces the public that it is safe, and terrorists prove them wrong, the societal consequences may be even worse.

So these two primary goals are intertwined. The second cannot be accomplished unless the first can be accomplished **and** the American public can (mostly) be brought to believe that it is so. The latter is not a trivial step. Announcing to the press that the government is confident that the public is safe is unlikely to be sufficient. Two factors loom large here. The first is the evidence presented by major incidents such as the bombings at the Murrah building and at the World Trade Center. The second is a predisposition on the part of some segments of society to disbelieve what the government tells them. The notion that the government lies unites right wing paranoids and left wingers, and includes a strong strain of cynicism that exists across the political spectrum. Whether one believes that the government is self-serving (a left wing notion), out to get you (a right ring one), bumbling (a more common one), or composed of sleazy, sneaky politicians (maybe an even more common one), one is led to distrust such grand assurances.

If the primary goal cannot be achieved, a secondary goal ought to be to minimize the effects of the weapon detonation. From the perspective of the threatened US population, this goal is clearly a distant second best to preventing the detonation. However it does have important benefits. Furthermore, a credible, advertised capability to accomplish this could help in deterring an attack in the first place, and therefore contribute to the primary goal. This goal can be approached in three general ways.

1. Force the perpetrators to detonate the weapon in a less than optimum location. In military terms, take steps to maximize standoff at detonation.
2. Evacuate or shelter vulnerable population and assets in anticipation of the attack.
3. Treat the injured, decontaminate affected areas, provide life support to those whose homes are destroyed until their homes can be reconstructed, and then proceed with prompt reconstruction. These are basically the steps that are taken after any disaster, natural or man-made.

A tertiary goal ought to be to identify, capture, and punish the perpetrators, and to exact reparations. This goal is less important than the primary and secondary goals since it neither directly prevents damage nor limits it. However, capturing the perpetrators would contribute to preventing subsequent attacks, and a knowledge that they are likely

to be caught either before or after the act may act as a deterrent. Being able to trace the origin of an attack back to a sponsoring state, against which extreme retaliatory measures might be taken, would act to discourage that state from sponsorship.

In designing a system to achieve these goals, it is important to keep sight of associated goal, which is to minimize the impact on normal life of the measures taken to achieve the primary and secondary goals, i.e. to prevent unnecessary societal disruption. To the extent that a continuing implicit threat of nuclear attack results in the government taking measures that disrupt peoples' lives and affect civil liberties and economic activities, the terrorists will have partially achieved one of their goals. Under those circumstances, as long as the US refuses to meet their demands and the threat remains, Americans are paying a price.

Some thoughts on timing

A window opened up when the USSR broke apart, a window of opportunity to obtain nuclear materials and maybe nuclear weapons. Time will close that window, in part because of US-Russian cooperative programs, and US cooperation with selected other FSU states. On a longer scale, the window will close because of aging of trained Soviet personnel, and because assembled weapons will become less reliable over time. Whether the window was widest right after the fall of the USSR, or somewhat later as the economy took a downturn (and other factors came into play) is not immediately obvious. However, as time goes on, programs to restrict access to nuclear weapons, components, and materials and improvements in Russian life ought to reduce the dangers of nuclear theft and enticing away expertise. On the other hand, as time goes on, criminal and espionage networks will have time to mature. Bad guys will have more time to learn to use what they might be able to smuggle out of Russia.

In the same vein, the progress of time will also affect the availability of nuclear weapons and materials through routes that do not directly involve Russia and other former Soviet nations. These will be affected by the future of the international non-proliferation regime, and that of the nuclear power industry. Given that uranium enrichment and plutonium separation are complex and costly enterprises, controls on HEU and Pu are directly related to the difficulties that terrorists and "rogue states" will face in creating nuclear weapons. On the other hand, it seems fair to say that as time goes on the technology for designing and manufacturing weapons—once the nuclear materials are in hand—will become increasingly disseminated and easy to master, particularly if nuclear power and its associated support industries become more widespread.

In general, three types of things related to this threat will happen as time goes on. First, there is a natural progression of events—and some extraordinary ones—that is controlled neither by those who might try to obtain and use nuclear weapons or by those that would like to prevent them from doing so. Second, are the actions that the perpetrators may take. All are time-consuming to some degree, and some will become possible only if events progress in compatible ways. Finally, time can be exploited to

take actions to make it more difficult for the terrorists. Both sides can seek to exploit time against the background of the general evolution of the world. And all actions will take time to accomplish.

There will be two major timelines. First there will be a longer-term or strategic timeline that will determine whether successful attempts to obtain nuclear weapons and deliver them by terrorist means become easier or more difficult. How this evolves will determine whether the US faces an increasing threat, or one that declines. Then there is a tactical timeline that runs more or less from the time a terrorist group makes a decision to obtain and deliver a nuclear weapon to the time that weapon is either detonated or intercepted, or the perpetrators decide to abandon their efforts.

The process of obtaining or building a nuclear weapon, learning how to make it work, and bringing it to a target and detonating it will take some time. How much time will depend on a number of fairly obvious factors. This time can be exploited to determine that there is a problem, track down the perpetrators, and interrupt their actions. The perpetrators also have to deal with deterioration of materials over time. These include: boost gas (tritium) for sophisticated devices, and more mundane things like batteries. The fissile material degrades by nuclear decay too slowly to matter, but it can also decay through corrosive chemical processes that change its mechanical structure (e.g. shape and strength).

Therefore, there are two timelines that have to be run against each other: the timeline for the perpetrators to get and exploit their weapon, and the timeline to detect their activities and react accordingly.

An organization might realize that there are time-consuming steps that they have to take, such as obtaining necessary experience, constructing certain parts, or planning their attack, and do these in anticipation of obtaining the weapon. That would shorten the timeline, but perhaps provide opportunities to detect what they are doing in advance of the actual threat.

There are also longer term timing issues.

Most observers will probably agree on two points. First, that the prospect of a nuclear attack within the US is horrific. And second that it is a very unlikely event. Unless there is some precipitating (series of) event(s), or a drastic change of perspective on the part of the US government, solving this problem is unlikely to receive the massive amounts of funding and attention that would be required to make dramatic progress within a very few years. Whatever system gets put into place will be constructed slowly, i.e. over a decade or more. During this interval, the threat will evolve and other significant events will take place. Some of these events can be influenced as part of the defensive system of systems.

The most significant trends are those in: technology and dissemination of relevant information and expertise; proliferation and availability of complete weapons; and

commerce in and availability of fissile materials. Progress in global trade and the movement of goods by water, air, and land will also impact the problem. The US will have the ability to influence all of these to varying degrees. How well we can do so, and how unambiguous US interests are perceived to be, remain to be seen.

Volumes of information on the design principles of nuclear weapons are freely available. That will not be reversed. How a fission weapon works is no longer a secret to anyone with a modest physics background. The details of US weapon designs are still secret[34]; so, presumably, are those of the other nuclear weapons states. At best that information will be disseminated no further than it already has been. It seems unlikely that over the long term it will not be further compromised. The fact that several states have developed nuclear weapons over the past few decades is reasonable evidence that necessary design information can be had, that the state of engineering education is such that working designs can be produced from knowledge of design principles. As a general proposition, the more states that have that knowledge, the more likely it is that the information will be compromised.

On the "plus side", engineering is always a combination of documented information and experience that resides in individuals. As (some of) the major nuclear powers scale back their nuclear weapons programs, that expertise will age, retire, and fall into disuse. Similarly, if nations follow the example of Brazil, Argentina, and South Africa, and abandon nuclear weapons programs, their expertise will similarly atrophy. Indeed, the US now is concerned that the field is no longer attractive to bright young people needed to sustain the US expertise in the long run. The US has worried that the deteriorating economic conditions that accompanied the end of the Soviet Union would result in Soviet nuclear expertise being offered for sale. That expertise is now a decade older; and within another decade or two most Soviet-trained experts will be gone or irrelevant. However, as the Russian experience has demonstrated, the immediate result of ending or reducing nuclear programs is to make nuclear expertise potentially available to others. Only later does that expertise decline through disuse and lack of replenishment.

How those retiring experts are replaced by a new generation will depend on how the nuclear program is viewed in Russia. Just like here, if it is high priority, it will get new blood (and good blood at that). If the program is withering away, so will the expertise. And that depends--in part, but far from entirely--on the US relations with the Russians.

New expertise will grow in other states that have expanding nuclear programs. The US has some influence over the vibrancy of that growth, and on the ease of proliferation beyond the borders of the states in question. This gets complex. For example, if related areas of physics are de-emphasized in the US and Europe, aspiring nuclear states will have to carry a larger burden of research. Most of those foreign experts learn their science and engineering in the US and Europe. At the risk of violating academic freedom, steps could be taken to make it harder for states that have nuclear

[34] I.e., that information is classified. It is not necessarily classified SECRET.

programs—open or clandestine—to send their young people abroad to study relevant areas.

If a substantial part of the world community is serious about preventing the spread of nuclear weapons and materials, it should be possible to evolve a more robust system of reductions and controls that gradually tightens access and makes it much more difficult for bad guys to steal weapons or divert weapon-grade fissile material. Time should be on the side of making access more difficult.

Proliferators could respond by developing the capabilities to produce their own weapons-grade material, either from available uranium or spent reactor fuel, or by being able to combine different grade materials from different sources into stockpiles having uniform characteristics.

Obtaining weapons grade material through enrichment or reprocessing now requires complex industrial facilities with large signatures. These are clearly beyond the means of terrorist organizations, particularly those that operate in remote clandestine locations. History has shown that such facilities are not beyond the reach of nations of modest means, but they are hard to hide. However, alternative processes could be developed that are pursued in facilities that are much smaller in scope and therefore easier to hide. While separation and enrichment is not likely to turn into a cottage industry, evolving technology could result in facilities that are much easier to conceal and perhaps much less costly to build. The relevant physics is known, and much of the technology has been developed to some extent[35]. It is, however, far from "off the shelf". As time goes on, determined engineers might develop alternative enrichment processes. The more time they have, the more likely they are to be successful. On the other hand, the more time they take, the more likely they are to be found out. The time that the process would take could be exploited to conduct research into methods for discovering such processing facilities.

Very different international political futures are possible. These may vary greatly in their implications for the risks of nuclear proliferation. It might be worthwhile to create some scenarios and consider how the US might influence events in ways that minimize the risks of proliferation. More nations may decide to develop nuclear weapons; or alternatively the non-proliferation regime may tighten. The number of nations with radical regimes, or regimes otherwise opposed to the US, may increase; existing radical regimes may increase the number of nations with which they have normalized (or even friendly) relations. As an example, international pressure is building to end the isolation of Iraq that was put in place following the Gulf War. This is likely to happen with or without US acquiescence if steps thus far taken by Russia, France, and other nations are reasonable indicators. Another possibility is the emergence of more, and stronger quasi-state players that exist on the fringes of the international community. Such regimes could be quite radical in different ways. Some may have radical political goals, while others may be purely mercenary or have large-scale criminal connections.

---

[35] See, for example, Sublette, Carey, *Nuclear Weapons Frequently Asked Questions*, posted at http://www.envirolink.org/issues/nuketesting/hew/; http://www.fas.org/nuke/hew/

The Taliban in Afghanistan is an example. Currently, large parts of Colombia are under the administrative control of non-government entities. The US has been concerned about "rogue states" such as Iraq or North Korea, or Cuba that harbor anti-US sentiments and violent potential. Because they are states with governments, capitals, infrastructures, economies, and recognized organs of control the threat of conventional military actions against them remains viable. However, one can imagine much more amorphous entities that control significant territory and population, and have access to financial and technological resources.

Terrorist organizations could take advantage of passing years to build and solidify smuggling routes and associated networks that could be used in obtaining, moving, and perhaps employing nuclear weapons. The passage of time might also be exploited to discover and infiltrate these networks.

Progress in sea, air, and land transportation attendant to the globalization of manufacture will affect opportunities to smuggle weapons and components, as well as opportunities to detect them. Economic realities are likely to dictate that greater volumes be moved through increasing numbers of locations, and that schedules become shorter and more predictable. Using traditional methods of border control, this would inevitably lead to greater volumes to inspect and less time to inspect them. Even modest delays would become extremely disruptive of commerce; measures that cause delays would be vigorously opposed by industrial interests. This will evolve over years. The intervening period could be exploited to design features into the transportation system that inhibit smuggling while imposing minimal delays. That won't be easy to do, but it would have important applications beyond just the inhibiting nuclear smuggling.

Similar considerations attend the movement of information: scientific and technological information that may be weapons-related; funds in the form of electronic transfers; information related to the availability and shipment of items related to manufacturing weapons; detailed information used in planning routes to move weapons and locations for attack; intelligence that might be useful to help terrorists evade detection and interception. Modern communications technology permits widely dispersed groups to coordinate and plan. The internet provides a handy C3 network that can carry plans, commands, and large volumes of information in near-real time.

There are defensive measures that can be evolved over a period of years, given that decisions are made reasonably expeditiously to start them. These could include:

1. Arms control measures that reduce the number of Russian nuclear weapons
2. Measures to improve security and accountability of Russian weapons
3. Measures to reduce the amount of nuclear materials in other FSU countries and increase the security of that material
4. Strengthen international agreements and structures to inhibit proliferation
5. International agreements to bring more nuclear material and weapons under safeguards, controls, and accounting regimes
6. International arrangements to inhibit illicit movements of nuclear materials within and among states

7. Improved surveillance of suspect groups, including arrangement for international cooperation
8. Improved detection technology
9. Development and institution of measures the inhibit the movement of nuclear contraband through airports and seaports
10. Better control of movements of radioactive materials within the US; better understanding of the radioactive "background" against which illegal shipments would be detected.

Design and configuration of the system

The system will have a very large number of individual elements. This can be inferred by simply considering all the different threat paths and their possible elements as addressed earlier. In most cases, multiple approaches can be envisioned for countering each threat path elements. It is not the intent of this paper to specify these elements in detail. Rather, this section provides an overall framework within which they can be arranged.

The simplest aggregation has three basic elements: (1) control the supply side; (2) impede and intercept attempts at transportation and delivery; and (3) reduce the potential consequences of an attack. This breakdown provides a convenient way to think about the system. However, it is not entirely "neat"; these categories overlap. For example, the supply side (i.e. the acquisition of nuclear weapons) will most likely involve transportation. And impeding transportation to or within the US can reduce attack consequences if it causes the weapon to be detonated far away from major targets, or stimulated the perpetrator to abandon his efforts.

In addition, there are other areas that need to be considered that fall across all of these categories. One is deterrence, which is both a tool and a goal. We would prefer that the system deter (or dissuade) potential attackers from making an attempt. Another is intelligence, or gathering and using information; and a third is interdiction and apprehension. These are basic parts of most aspects of the system.

Intelligence is a vital part of the system; intercepting an attack attempt will depend critically on knowing what to look for, where to look, and when to look.

While sensor systems—particularly radiation detectors—would be important contributors, it should be obvious from much of the earlier discussion that simply setting up rings of detectors around possible points of entry into the US would be neither practical nor sufficient. There are a large number of possible entry paths, and opportunities for a clever and determined terrorist to drive down detection rates.

Detection will be increased by constructing as many different sources of information as is practical, and integrating their outputs. This includes both geographic extent, i.e. seeking information from foreign sources, transshipment routes, entry points, domestic sources, and domestic activities, and a diversity of information sources—including but not limited to employing different types of sensors to look for different signatures of weapons, components, and related activities. More sources of information means more detection opportunities. It also allows for integration so that some sources can cue others that can then be used more efficiently. Cueing sensors with the results of other forms of information gathering could greatly improve the chances of detection, as would the use of other well known techniques such as arranging for multiple, coordinated

detection opportunities, and employing multiphenomenology (i.e. the use of different types of detection that looks for different signatures).

Other ways to divide the same pie are as follows.

Increase difficulty of obtaining weapons, components, and materials
Impede, intercept, and apprehend outside US
Impede, intercept, apprehend domestically
Harden targets, enforce meaningful standoff
Consequence mitigation

Arms control, non-proliferation, diplomacy
deterrence
Preemption
Active defense
Passive defense
Retaliation
Consequence mitigation

Diplomacy
Military activities
Intelligence
Border security
Law enforcement
Consequence mitigation

Of these three charts, the second corresponds to a typical DoD approach to defensive problems; the last conforms in general to agency responsibilities. Each of these formalisms revolves around measures designed to severely impede—or effectively preclude—the ability of potential perpetrators to acquire a weapon or its components, transport it to the US, bring it to its target, and prepare it for detonation without being apprehended before they can detonate it. The most important thing is to be able to prevent the attack, preferably by deterring it. Consequence mitigation, retribution, and arrest and punishment of the perpetrators are distinctly second order.

Controlling the supply side: measures that increase the difficulty of obtaining nuclear weapons, nuclear materials, and weapons components

This aspect consists generally of imposing impediments to potential terrorists obtaining nuclear weapons and all of the things that they would need in order to produce their own: weapons components; fissile materials and other materials that would be essential to bomb construction; multi-use systems, components, and subcomponents that could be used in fashioning a bomb; technology and expertise for bomb design, manufacture, assembly, transport, and use; technology, expertise, and critical equipment for enrichment and separation of fissile uranium and plutonium. Measures that increase transparency and visibility into activities that might lead to the production and movement of terrorist nuclear devices are also useful. If perpetrators cannot be prevented from getting a weapon, knowing that they have it and where it is would be very important.

Measures to control the supply side already exist. Indeed, it has been a focus of US policy since the earliest days of the nuclear era. It consists of four general areas: (1) nuclear arms control agreements with the Soviet Union and its successor states; (2) the international nuclear non-proliferation regime; (3) cooperative measures with Russia and other former Soviet states to enhance security of nuclear weapons and materials and reduce stockpiles; and (4) unilateral and multi-national export control measures designed to reduce access to a wide range of things that could be useful in building nuclear weapons.

Arms control may have a dual role to play here. First is the direct role of limiting nuclear weapons, nuclear materials, and proliferation in general. Arms control and reduction measures directly limit the number of weapons and amount of nuclear materials produced in Russia (and in the US), and indirectly limit these in France, Britain, and China.[36] Second, arms control often brings with it an accounting system and verification procedures, i.e. agreement to certain measures by which parties allow sovereignty infringements in order to verify that they are in compliance with their undertakings. If properly arranged, these accounting and verification procedures might be used to make theft/diversion more difficult. Better inventory control means a greater likelihood that discrepancies will be discovered rapidly. Verification procedures usually involve having and disseminating more information about what is being controlled.

International obligations under the Nuclear Nonproliferation Treaty (NPT) and the associated safeguards regime administered by the International Atomic Energy Agency provide important impediments to the diversion of nuclear materials, but are far from 100% effective. That proliferation has not been prevented is illustrated by nuclear

[36] China, France and the UK are not parties to SALT and START—the latter two adamantly so. However, negotiated limits on Soviet—and then Russian—force levels have been a factor in capping the arsenals that these two NATO allies have decided they needed. The ability of the US to provide some degree of "extended deterrence" through its forces as shaped by SALT, START, and agreements on shorter range systems has also been a factor in their decisions. The effects on China's force decisions are less clear, but probably significant.

weapons programs in India, Israel, Pakistan, South Africa, North Korea, Iraq, Argentina, and Brazil. Nevertheless, its existence places roadblocks in the path of terrorists or states that might sponsor terrorists. Indeed, not all of these programs have been successful, and some have been abandoned.

In a general sense, the international non-proliferation regime provides a set of supply side initial conditions within which attempts at diversion would take place, the context within which US measures against terrorists would take place. It is not a tool that the US can use directly. However, it would probably be in the US interest to suggest measures that would tighten the regime in ways that would make diversion to terrorists more difficult, and to attempt to get them adopted. Most of the world's nations would have an interest in such measures, at least in principle.

Any save the most cynical observer would have to conclude that these measures have been largely and widely successful. Major nuclear arsenals are nowhere near as large as they were once projected to be, and are indeed much lower than they were not long ago and are most likely headed downward. While the number of nuclear states has grown, that growth has been modest. Nuclear power has become a major factor in the world's economic and energy equations without generating the proliferation and pollution problems that were predicted 30-40 years ago.

But major problems remain. Some of these result from the inherent limitations of the systems and measures that have been put into place. Others have arisen because of conditions that have emerged—evolved is perhaps more accurate—over time.

The basic context for these changes is provided by progress in science, technology, and global commerce. These are all intertwined. Understanding that was available to only a very few individuals in the 1950s and 1960s is now much more accessible. This is perhaps partially due to "intelligence" gathering, but mostly due to advances in science and engineering, dissemination of the results, and education in both areas. That genie will not be stuffed back into the bottle. Evolving technology in a number of areas has made it easier to perform tasks that were once very difficult. Some of this is the result of national nuclear weapons programs and advances in the nuclear power industry, but the rest comes from areas that are less directly related. Globalization of commerce has resulted in the export and proliferation of high technology manufacturing and engineering, in complex corporate and trading structures, and in global movements of products, processes, and information.

These trends all make the control through secrecy, export restrictions, and border controls much more difficult to practice.

Major successes have produced some perverse problems. Nuclear reductions achieved through the START process and the end of the cold war have resulted in significant nuclear capacity and expertise becoming redundant, primarily in the US and the nations of the former Soviet Union. Neither excess capacity nor expertise has posed a proliferation concern within the US, but Russia and other former Soviet states have been

quite another matter. To some extent this is a self-limiting problem. Individual expertise has a "shelf life" of a decade or two, and unemployment in the nuclear weapons field does much to discourage young people from studying and entering the field. Plants can be dismantled, and deteriorate when not in use. Fissile materials, however, remain a problem for much longer. Economic problems, particularly in Russia, have aggravated the threat of diversion of nuclear weapons and materials.

The US has initiated vigorous cooperative threat reduction (CTR) programs to improve security and accountability of stored materials in Russia and elsewhere, and to convert them to less threatening forms. These programs remain vital to controlling the supply side. It would appear to be prudent that as the Bush and Putin administrations reformulate US-Russian relations that the future of CTR be taken into account. CTR is likely to be directly affected by other nuclear-related matters, such as weapons reductions and ballistic missile defenses. It may possibly be indirectly related to other bilateral issues. In general, if US-Russia relations cool, the likelihood of continued US access to—and ability to influence security at--Russian nuclear facilities may well decline.

A medium to long term trend in US/Russian arms control has been to reduce the number of nuclear weapons and the amount of HEU and weapons grade plutonium, and to increase the security of what remains. In the shorter term, however, the combination of reduced Russian arsenals and political/economic turmoil within Russia have created conditions that have increased the possibility that Russian weapons and materials could be diverted. These two countervailing trends are likely to continue. Anticipated deep reductions in Russian nuclear weapons have the potential to add to the problem, while continued progress in US-Russian bilateral programs is expected to continue to turn more HEU and plutonium into forms that are not directly useable in weapons, and to increase security at Russian facilities. How this progresses will depend in large part on how the US manages its relations with the Russians over the next few years.

Since the largest potential supply for contraband nuclear weapons, materials, and expertise is Russia, continued—and hopefully improved—US access to and cooperation with Russia will be very important to controlling the supply side.

Other supply-related factors have emerged. One is China's propensity to use trade in dangerous military technology and equipment for economic and political purposes. It is not at all clear that China views nuclear weapons in the same way that the US, Russia, France, and Britain do. This is somewhat tied to the emergence of two new nuclear powers, Pakistan and India. Their ability to protect their nuclear weapons, materials, technology, and facilities needs to be examined. Security and safeguards in the US and Russia took decades to develop. While the US has tended to focus on the long-standing rivalry between India and Pakistan, it is India and China that are natural rivals for power and influence in Asia. To further its ends, China has moved closer to Pakistan, while India has been negotiating arms deals with Russia. Pakistan admits to being militarily inferior to India, and has been caught sponsoring terrorism within India.

More attention ought to be given to policies and programs to reduce the possibilities for terrorist acquisition of nuclear weapons or materials in south Asia.

Another factor of concern is the emergence of "states of concern", i.e. radical governments (or pseudo-governments such as the Taliban) that are generally antagonistic toward the US, lack resources for a conventional military confrontation, have connections with terrorist organizations (or have sponsored terrorist-like activities), and have access to modern technological expertise and to significant funding. These states are generally the connection between the sources of supply and the potential perpetrators. They are sources for resources that are generally beyond the means of terrorist groups, and potential motivators for terrorists to attack the US. In 1970, the prospect that a radical group with terrorist tendencies could smuggle a nuclear weapon out of the Soviet Union—or produce one in a basement somewhere—and attack the US seemed remote. Today we can worry about states supplying money, technical resources, room to work, and incentives to attack.

These states tend to be largely beyond the reach of the supply side measures that now exist. They are outside the arms control framework and mostly outside the meaningful reach of the non-proliferation regime. Almost by definition, relations with the US are distant, making it difficult for the US to bring diplomatic measures to bear on their behavior.

A major challenge for the immediate future is to find ways to control the behavior of these states as regards nuclear matters.

Sources of information from the supply side—foreign sources of information

A basic source of information derives from nonproliferation and other arms control agreements and the associated implementation regimes. These provide inventory specification and monitoring, and permit certain information gathering activities as part of compliance verification. These activities can be multinational, such as those conducted by the IAEA, or unilateral, like those that the US and Russia grant each other under START. These measures are incomplete, but they provide valuable information. For example, IAEA materials accounting procedures provide a basis for determining whether some safeguarded material may be missing. The accompanying safeguards have some ability to directly observe and detect attempts at diversion. Other agreements give the US rights to observe Russian nuclear weapon facilities including deployed units, storage, and facilities involved in the manufacture and/or dismantling of nuclear weapons.

At best, opportunities exist to directly observe attempts at theft or diversion. In other cases, shortages or inconsistencies can be identified, and used as a warning that something may be afoot. Depending on the frequency of observation, a period of time during which a diversion might have occurred can be identified.

A recent analysis conducted by DTRA/ASCO[37] found that nuclear materials could be marked by doping with small amounts of radioactive isotopes to enhance detectability and traceability. Being able to trace intercepted material to a specific plant is an incentive for plant management and personnel to be serious about security. It also places those involved in diverting the material at greater risk of being discovered and held responsible, and makes continued diversion from that source problematic.

Other sources of information on relevant activities in other nations also exist. These include both covert activities carried out by US intelligence agencies, and cooperative activities with foreign government entities, such as cooperation among law enforcement agencies regarding nuclear smuggling (and other forms of smuggling), and sharing information about groups mutually viewed as terrorist or otherwise undesirable. At best, such information puts US agencies on alert regarding the activities of groups that may be seeking nuclear materials, or warns that materials have been diverted and may be moving toward the US. Such information is often ambiguous. For example, there is still controversy regarding what, if anything, the record of arrests for nuclear smuggling actually tell us. This arises, in large part, because of an inability to know what, if anything, foiled smuggling attempts tell about those that may have been successful. Nevertheless, it is information that can be used.

Gathering information on nuclear terrorism and nuclear smuggling is hardly an area in which the US stands alone. To varying degrees, most of the world's governments have an interest in containing these activities. International structures and organizations can also be exploited for this common goal—for example, IAEA, UN, NATO, and INTERPOL. Although the US is usually considered the most likely target of nuclear terrorism, particularly by US analysts, other major countries are also at risk. Russia faces major security problems, including open conflict, and has been the target of major terrorist attacks and radiological threats. Viewed objectively, Russia appears to be at greater risk of nuclear terrorism than is the US. There is more animosity and violence directed against Russia. Since Russia is the major potential source for contraband nuclear weapons and materials, attacking Russia would involve much simpler threat paths than attacking the US, including gaining control of a weapon and detonating it *in situ*. Israel has the world's greatest tempo of terrorist attacks. Terrorist organizations operating in and against Israel have connections to radical regimes that view Israel as a nuclear threat and apparently harbor nuclear ambitions of their own. The industrialized nations of Europe and east Asia have good reasons to not be complacent. Other nations have strong reasons to want to avoid being seen as unwitting elements of a nuclear terrorist attack, for example suppliers of critical components, or places from which terrorists operated or through which they moved their weapons. These shared interests present the US with sources of information and other help in foiling attack attempts.

Sources close to home. Plausible paths for bringing weapons or material into the US, or for launching attacks, involve neighboring countries, particularly (although not exclusively) Mexico or Canada. US efforts could be helped by information on suspicious

[37] Gilfoyle, Dr. Gerard P. *Detecting and Deterring Nuclear Smuggling.* DTRA/ASCO.

activities in these countries. For the most part, information gathering would be the result of cooperative efforts. Such cooperative efforts are all the more important because surreptitious shipment or movement into the US is much easier across the Mexican and Canadian borders than it is by ship or airplane from farther away. This is also true, but to a lesser extent, for movement from Caribbean, Central American, and northern South American countries.

Impeding movement and transportation

Whatever weapons, components or materials are obtained or produced in other countries are not a direct threat to the US until they are brought here. Transshipment provides opportunities for detection and interdiction.

With very few exceptions, all transport will be by some combination of road, rail, air, and water. (The exceptions are movements on foot or using pack animals. These are very unlikely, and, if they occur, could only be small parts of very complex threat paths.) These all present opportunities for detection and monitoring, primarily at ports, hubs, and border crossings. However, smugglers can be expected to attempt to select ports, hubs, and border crossings where they have the greatest expectations of avoiding scrutiny, or if possible to avoid such hubs entirely. Airplanes can operate from and to primitive fields in remote locations, and boats can load at simple docks or event on beaches. Such operations do place constraints on what can be loaded and unloaded, and impose other risks to contraband and smugglers.

Conceptually, it would be desirable to identify and impose measures that make it more difficult for smugglers to attempt to use routes that are harder to monitor, and take complementary measures to prioritize monitoring systems such that those routes and modes which would otherwise be the most attractive to smugglers receive the greatest attention for instituting monitoring. These efforts could be augmented by judicious use of release and concealment of information regarding monitoring efforts. It would be worthwhile to lead smugglers to believe that the extent and capabilities for monitoring in certain areas may be greater than they actually are, and at the same time to conceal information on the true extent of capabilities in other areas. The former would aid deterrence, and the latter would aid detection. The uncertainties created by these two types of measure together should also aid deterrence, and complicate smugglers' planning.

Road and rail transport present some opportunities for monitoring en route. Under very limited conditions, ships can be searched at sea, and airplanes can be forced to land and be searched.

Detection

The most obvious signature of a nuclear weapon or nuclear material is its radiation. However, the radiation signature is not always easy to detect. Weapons grade plutonium has a much larger signature than does HEU, but both can be concealed by enough shielding. Moreover, a crude terrorist device is more likely to contain HEU than Pu. Such a device is likely to contain tens to hundreds of kilograms of fissile material, but the material could be shipped in smaller pieces for later (re)assembly. Relatively small pieces of HEU encased in shielding could be very difficult to detect.

DOE's NEST team is equipped with state-of-the-art detectors for intensive search of suspected locations. The detectors are costly and the search is time consuming and labor-intensive. As currently equipped and configured, the NEST team is not a practical model for routine search of large numbers of transshipment hubs.

Designing a detection system involves a trade-off between two conflicting goals: maximizing the probability of detection, and minimizing the false alarm rate. Both detection and false alarm generally rise as detectors become more sensitive. Improved ability to determine the natural and instrumental backgrounds and to distinguish real events from background events and noise suppress false alarms, but such capabilities generally come at high cost[38]. False alarms can be tolerable nuisances under some circumstances. However, when looking for very significant rare events within a high volume of traffic, false alarms can be devastating. Re-examining a few percent of the passengers passing through airport security can introduce crippling delays into the air transport system. It is not hard to imagine what would happen if 1% of the traffic on a major highway were stopped every rush hour and searched for nuclear contraband.

One approach that holds some promise is the construction of networks of inexpensive sensors. A report from any individual sensor would not be sufficient to trigger a response, but several properly correlated reports would constitute an event with a very low probability of being false. Several different sources of information could be combined. Such a system—the Wide Area Tracking System, or WATS--was developed and prototyped by Lawrence Livermore National Laboratory to monitor road networks. Low cost radiation detectors were collocated with simple range finders. An event was recorded only if a radiation event occurred simultaneously with a determination by the range finder that a vehicle was present. The system then projected the likely progress of the suspect vehicle through the road network and looked for subsequent events at times and locations consistent with those projections. The project was never completed, but it was taken sufficiently far to demonstrate that the approach could indeed track a target with great precision. Moreover, the project team identified a number of practical problems that would have had to be overcome before the system could become a useful reality.

[38] Background events are events to which the detector responds that are due to sources other than those the detector is trying to find. For example, radioactive events can—and do—occur because of radiation emitted by isotopes that occur naturally in the environment, including uranium isotopes. Noise refers to events that are not real, but result from random electrical fluctuations within the detector and its associated circuitry.

WATS was conceived as a system to protect US cities or overseas military installations against attempts to attack them with nuclear weapons introduced via a surrounding road network. The concept is also applicable to monitoring approaches to transportation hubs, perhaps as a way to identify a very small subset of approaching vehicles (or people) for closer scrutiny. As designed, the processor could accept data from a wide variety of sensors, and could be cued by less quantitative sources. Because radiation signatures can be hidden or obscured, the identification and inclusion of other target signatures would be very valuable.

Networks of sensors using radiation detectors and/or other short range sensors can only work if the locations of the targets are very constrained, and are constrained to being very close to the detectors. This approach is suited to monitoring roads, as WATS was designed to do. Monitoring broad areas, such as sections of ocean, would not be feasible.

Monitoring

Conceptually, the network over which contraband would be moved consists of points and interconnections. The points are sources (points of origin), destinations, and transshipment hubs. These are connected by roads, rail lines, airplanes, and ships. The transshipment hubs present monitoring opportunities, since cargoes move through them, and in some cases are taken off one mode of transit and put on another (e.g. taken off a truck at an airport and put onto an airplane). The roads, and to a lesser extent the rail lines, leading into and out of the hubs also present monitoring opportunities, as do some interconnecting roads and rail lines. Generally, ships and airplanes en route are relatively very difficult to monitor.

Networks of sensors could be used along the roads leading in to and out of the hubs, sources, and destinations. These could be sophisticated networks such as WATS, or much simpler ones. How sophisticated a network needs to be will depend on a number of local factors, including prevailing traffic conditions, how many options a malefactor would have for moving contraband, and the consequences of stopping a vehicle for more detailed inspection. For example, stopping 1% of the vehicles leaving the area of a remote nuclear facility would have an insignificant impact on commerce and local citizens' daily activities, but stopping and searching 1% of the vehicles on the Santa Monica freeway in Los Angeles—or 1% of the trucks entering across a major US/Canadian border crossing—would have much more drastic consequences. The network system also has to be designed to connect with a response team in a useful way. While it may be useful to know that a truck suspected of carrying nuclear contraband passed through a monitored section of highway some time in the last 8 hours, that is not nearly as useful as being able to identify that truck and dispatch a response team to follow it or stop it.

Portal and perimeter sensors already exist at potential source sites. In some cases these may be deemed sufficient to detect and stop any attempt at diversion. In other cases, it may be prudent to interface these systems with others farther out along roads leading away from the sites.

In principle, roads can be monitored by netted sensors or by other means. However, this is likely to be an unmanageably large task where road networks are dense, and impractical (for political reasons) in countries where road networks are sparse. It may be more practical to consider monitoring roads leading to major hubs, i.e. airports, seaports, and border crossings. Trains could be searched or otherwise monitored entering or leaving stations, or en route. Doing so, however, may prove impractical unless cueing can be used to narrow the search to very few trains.

Monitoring road networks leading to hubs could be used to intercept vehicles carrying weapons or nuclear materials, or to identify them for closer scrutiny at the hub. Some fraction of vehicles transiting at border crossings are currently given closer scrutiny for a variety of reasons. Many international airports have instituted significant security procedures, particularly for flights headed to the US. Security measures also exist at seaports. In some instances—particularly if a group intends to fly or ship a bomb to the US and detonate it on arrival—the last opportunity to intercept it will be before it leaves a foreign airport or seaport. It seems reasonable that many foreign governments would want to cooperate with the US in a program to intercept nuclear contraband on its way to ports of embarkation on their territory, and would therefore support and participate in measures to enhance port security and/or monitor road networks leading to the ports. However, there may be concerns that limit their involvement. One is that a nuclear bomb bound for the US not be detonated on their territory—particularly in populated areas around major ports—when it is intercepted. Another is concern for disruption of routine local activities. Yet another is the imposition of impediments to the free flow of commerce that disadvantages local companies, or gives shippers strong incentives to move their activities to other ports. These are practical problems that would have to be solved along with the technical and operational problems. A shared concern may not of itself be sufficient to produce full cooperation; it is, however, a good place to start.

There may be something to be gained in this regard by working with the European Union (EU). The EU has a significant ability to impose standards of commerce on its member states, and companies that do business on their territories, and has a fair degree of influence on states that seek to join the EU and nations such as Russia that seek to create commercial relationships.

Security has been a major issue at airports for more than two decades, primarily because of terrorist activities directed at air transport. Parcels as large and dense as those that could contain a terrorist nuclear weapon are likely to receive special scrutiny, even at the busiest airports, although this can be somewhat circumvented by the use of chartered aircraft rather than regularly scheduled flights, and by exploiting corrupt workers and officials or terrorist agents “planted” in strategic jobs. Smaller amounts of fissile material may be easier to smuggle on-board. As the airport security system has evolved, important lessons have been learned that could be exploited to make it harder to smuggle nuclear materials. However, one of these lessons is that air transport, like other major forms of transport, runs on tight cost and time margins. Any suggestions for security

measures that hold the potential to delay operations or to increase the costs to airports and air carriers are likely to run into concerted opposition.

Air transport has evolved a security-oriented operational framework that provides opportunities to increase monitoring for nuclear materials.

Security at seaports is a much different proposition. Compared to air travel, ships move much more freight and far fewer passengers. The trend in ship design has been toward ships that spend much less time in port—primarily container ships and roll-on/roll-off (RO/RO) ships. Whereas transport airplanes tend to carry relatively small packages that are sized to their contents, container ships are built to take large containers of standard size that the customer can fill as he sees fit. A nuclear weapon or a shipment of fissile material could be packed into a container with a great deal of shielding, and would present no external clues as to its identity. A typical container ship may spend only a few hours in port, on the same order as the time a typical airliner spends on the ground at an airport. While in a US port, that ship can deliver a container that was loaded onto it weeks earlier at a port it called at two dozen stops earlier. That container could even have been loaded onto it from another ship.

In 1999 President Clinton established an Interagency Commission on Crime and Security in U.S. Seaports. The commission issued an extensive report in the fall of 2000, in which they observed that the shipping industry has benefited from security advances made in the air transport industry, but had lagged behind. The report states "Because appropriate technology for examining containers and shipments is limited at sea-ports, shipments may go unexamined."[39] "For the most part, seaport technology has lagged substantially behind that available in the nation's airports and on the Southwest border of the United States…..Both the technology that is in use and the rudimentary forms of security vary from port to port."[40]

The process of detecting nuclear contraband being loaded onto ships appears to be extremely difficult, without either enormous expenditures on labor and equipment or severe delays in commerce, or both. Moreover, those inspections would have to occur in foreign ports, beyond the direct reach of US authority. The US has established and stimulated satisfactory airline security measures in foreign airports by putting requirements on airlines that are flying to US destinations: departures must meet US security rules. Similar rules would appear to be difficult to impose on containers shipped from foreign ports, since a container could be loaded on a ship bound immediately for a non-US port, and reach the US many days later. The US has another lever to pull with airlines: competition. US carriers form a major part of the total international airline fleet, and the US market is a very large one. Foreign carriers have a great deal of incentive to do what is necessary to operate to US destinations. Very little commercial shipping, however, is US flag.

[39] "Report of the Interagency Commission on Crime and Security in U.S. Seaports, Fall 2000" p.112
[40] ibid. p.113

One way to approach the problem is to attempt to shift some of the burden onto the companies that ship goods in containers. The FAA has implemented a similar program for air shippers. How this might be done remains to be explored. However, in general, companies that meet certain requirements for packing, inspecting, and sealing containers would be granted expedited landing and offloading once their goods arrive in the US. Certification would mean being exempted from inspections that other containers would be subject to, inspections that would slow the transition from dock to rail or road. Procedures would have to be worked out whereby US authorities could reaffirm compliance using inspections or other procedures that cannot be confidently predicted in advance. This approach could not prevent a terrorist organization from shipping a bomb in a non-certified container, and detonating that bomb while it is awaiting inspection. Moreover, a very substantial fraction of the shipping companies would have to participate in order for this approach to work.[41]

The difficulties of inspecting cargo would seem to put emphasis back on monitoring access to seaports. However, since shipping routes can be more complex than air freight routes, access monitoring would have to be very widespread indeed. Moreover, the size of cargoes being brought to seaports in trucks and rail cars would make radiation monitoring very difficult, since ample space and weight would be available for shielding.

Systems exist in development and early deployment that provide information about the contents of trucks and shipping containers[42]. These generally provide some form of outline imaging, and/or density information. Such information can be used possibly to detect the presence of shielding materials, or suspicious shapes. Plutonium and Uranium have very high densities, but shielding them can impede the extraction of density information. On the other hand, the presence of objects that cannot be identified may be cause for closer inspections, particularly when combined with other information, such as an intelligence cue. This approach is used in drug interdiction, where the presence of strange objects or unexplained empty spaces in trucks is used as a basis for further searches. These technologies have seen significant advances over just a few years. One of these areas of advance has been in search rates. As the time to search each container decreases, the number that can be searched with minimal disruption to commerce will increase. Moreover, as experience is gained using these systems and the information they provide, it may be possible to construct signatures based on several measurements that provide reliable indicators of nuclear contraband.

---

[41] more precisely, companies that collectively account for a substantial fraction of the containers shipped to the US.

[42] See, for example, ***U.S. Customs and Border Patrol agents stem the tide of smuggling with high-tech tools***

By Donna Rogers
***Law Enforcement Technology*, April 2000, p. 68**

This article can also be found at http://www.nlectc.org/inthenews/contraband_cops.html

Seaports and international airports are the most common points of entry into the US, but not the only ones. Large amounts of traffic moves by land across the borders with Mexico and Canada. The Mexican border is heavily patrolled, but that doesn't prevent the entry each year of large numbers of illegal immigrants and substantial amounts of drugs and other contraband. The Canadian border is largely unguarded, except at major road and rail crossings; this includes a long, mostly wilderness border between Canada and Alaska.

Canada is the US's largest trading partner, and under NAFTA trade with Mexico is increasing and becoming more integrated into the US economy. Major industries—particularly automobile assembly in the northern mid-west—are integrated with Canadian suppliers, and depend on timely movements of goods across the border. This presents the same problem of security at seaports: how to increase security without impeding commerce unduly. However, the opportunities may be better to work with companies to arrange for expediting shipments across the border in return for putting more of the burden of security on the companies. In the case of Canada, the US has the advantages of working with one of our closest allies, and of dealing with companies with which the US government should be able to exert a great deal of influence. Similar arrangements are possible with Mexico, but are as yet much less well advanced. Corruption and criminal activity are known to be widespread in Mexico, but the Fox administration has vowed to fix that. We'll see…..

Much of the traffic across the borders with Canada and Mexico consists of personal vehicles and smaller vans and trucks. This traffic is more amenable to radiation monitoring on both sides of the border, including integrated sensor systems along road networks.

However, there are many opportunities for entry into the US through routes that do not go through seaports, international airports, or major land border crossings. The movement of illegal drugs into the US provides a good primer on other smuggling routes. Drugs come by sea to small ports and undeveloped shore areas. Carrying vessels range from small ocean-going ships to yachts, and to small boats that either make short trips from Caribbean islands or Mexico, or are launched at sea from larger vessels. Some of these are unloaded and then abandoned. Small airplanes arrive from Mexico or the Caribbean and land at small local airfields or makeshift airstrips, or are crash landed in remote places like the Florida everglades. Larger aircraft fly from central America or South America. Similar modes of transit could be employed for trips from Canada.

These alternative routes could present major monitoring difficulties. This is amply demonstrated by drug smuggling. One could imagine smugglers and terrorists planning circuitous routes that bypass major transshipment hubs. However, employing such routes also present difficulties to the smugglers. They would have to handle delicate and dangerous materials under primitive conditions where necessary cargo handling equipment might be scarce. Their chances of losing their cargo to air or sea disasters—or to pirates—would be much higher than if they used major transportation means.

Less dramatic means of surreptitious entry from Canada and Mexico are also possible. The Canadian border, in particular, contains back roads that are often unmonitored. Moreover, boats can cross the Great Lakes/St. Lawrence Seaway where it forms the border from New York to Minnesota, and there are other lakes that are in both countries, principally Lake Champlain in New York and Vermont, and Lake Memphramagog in Vermont. Law enforcement agencies have been using long range night vision cameras to detect illegal aliens coming across remote sections of the Mexican border.[43] Cameras are used increasingly in metropolitan areas for purposes such as traffic monitoring and detecting red light violators. Similar systems at minor border crossings could obtain pictures of vehicles that cross there, including license tags. Depending on how many local people use crossings legitimately, this approach might produce a burden of "hits" that is too large to follow up on in any meaningful way.

Domestic actions: impeding and intercepting terrorist activities within the US; enforcing stand-off from potential targets; active defenses; consequence mitigation

Attacks launched from outside the US

Several of the transportation paths described above would lead to a terrorist group delivering a bomb directly to a target in the US from a foreign port of embarkation. These include: a ship sailing into a US seaport; an airplane landing at a major airport (or detonating the bomb over a city while approaching the airport); a small ship or large boat travelling into a city that is accessible by water such as New York, Philadelphia, Baltimore, Washington, Boston, Miami, Chicago, or St. Louis; a small to medium sized plane crashing at or near a major city. Once the weapon is en route, there would be little opportunity to prevent the attack, except perhaps in some fanciful scenarios in which the identity of the threat vehicle is learned and it is stopped or diverted (or destroyed) before it gets close to the US.

Once the situation has reached this point, there is little the US could do to avoid damage. Small planes and ships launched from Canada, Mexico, or other nations in the Caribbean, Central America, or parts of South America have been used by drug smugglers, and therefore provide a model and experience for this type of attack. Smugglers are often successful in landing their goods, although their success rate appears to be dropping as US authorities become more adept at tracking and interception. The more successful the US is in reducing the ability of these small craft to avoid interception and reach their targets, the less likely terrorists are to attempt these routes. Perpetrator success rates that are acceptable to drug smugglers—which could range from 80% to 50% or maybe even lower—would be much less acceptable to nuclear terrorists. Drug lords can make up their losses through raising prices, and can easily replace whatever is lost. As was discussed earlier, a 50% chance of losing his only nuclear weapon may

[43] Ibid.

appear to an attacker as too big a risk to chance. However, viewed from the defender's perspective, an even chance of the bomb getting through may appear uncomfortably high.

In the long term, seaports can be somewhat hardened to attack by moving the cargo facilities farther away from populated areas, particularly as new facilities are built to handle modern ships and old facilities are abandoned. However, geography limits where the facilities can be, as does the need to have access to surface transportation and other services. So does cost. To some extent, some of the population is likely to follow the jobs at the port. Moreover, unless ships are forced to unload containers at austere transshipment facilities far out in the harbor, any detonation will cause great loss to property and life within the port. Some oil facilities operate this way, i.e. extend pipes to anchorages away from the coast.

This has been the pattern for the construction of airports, but for different reasons. Once airports were built close in to the cities they served. Then the pace of aviation increased dramatically, along with noise, congestion, and pollution, and new airports were built "out of town". However, in the next phase of development many, the towns have expanded to engulf the new airports. The airports themselves are juicy targets with large capital investments and thousands of people passing through at most hours. Moreover, approach patterns often are over heavily populated areas. This could be changed at great inconvenience to passengers, operators, and suburban/rural residents.

Attempts to get people to make significant changes in their lifestyles in the face of the massive nuclear threat of the cold war failed. They are unlikely to work for a much smaller threat.

Weapons smuggled into the US or assembled within the US from smuggled components

Terrorists can attempt to take advantage of basic characteristics of US society to hide activities conducted within the US: the relatively open nature of US society; extensive guarantees of civil liberties; crowded, often polyglot, cities where they can attempt to hide within the crowd; and very sparsely populated areas where they could also attempt to hide in the countryside. In addition, other than a nuclear bomb or its most sensitive components, almost anything they might need for their mission can be easily obtained, usually legally. They are likely to be able to find some measure of support and security among groups who empathize with them for ideological, ethnic, or religious reasons, or for money, or because they can be fooled or manipulated. While this empathy may not extend to the conduct of acts of mass terrorism, the support groups may be kept largely ignorant of the details of the terrorists' activities.

Nevertheless, some of their activities are likely to produce detectable and recognizable signatures. Law enforcement agencies have had some noteworthy successes in apprehending terrorist groups both before and after the fact (as well as some noteworthy failures). As they become more adept at recognizing signatures and

combining them with information from domestic and foreign intelligence agencies, their ability to find terrorists working on a major attack should improve.

The most obvious physical signature of a nuclear bomb or its fissile components is radioactivity. As discussed earlier, this signature is not always easy to detect, can only be detected at short range, can be shielded, and is often hard to distinguish from background with high confidence. Detection is only possible if the target can be localized, i.e. if the search area can be severely constrained based on other information. The NEST team approach depends on looking for a target within a very small area.

The WATS system concept was based on a similar assumption, that the target would be constrained to movements along roads. While the safest approach would be to monitor the entire US road network, analysis conducted for the WATS program recognized that such an approach would be unaffordable, with today's technology and into the foreseeable future. Permanent sensor installations in strategically selected areas would be a second best solution. These areas would be major metropolitan areas and other significant targets, as well as possible points of entry, and major roads leading among them. This is also impractical given current technology. Major advances in technology, perhaps coupled with a heightened threat, might make this option plausible. For the next decade, the affordable option was judged to be a small number of systems that could be quickly deployed in a wide net around threatened areas.

While netted sensor systems such as WATS can do a good job of reducing the false alarm rate due to natural background and random noise—given correct design of the software for integrating the individual sensor reports—they can be undermined by other movements of radioactive materials along roads. Distinguishing among different radiation sources requires a spectrum analysis capability that would add markedly to the sensor costs.

Netted sensor systems only makes sense if the false alarm rate can be made acceptably low, i.e. sufficiently low that the drastic measures associated with intercepting a vehicle believed to be carrying a nuclear bomb are taken against an innocent vehicle only extremely rarely[44]. This would clearly be undermined if a terrorist bomb cannot be distinguished from a legitimate shipment of radioactive materials.

Radioactive materials have a number of industrial and scientific uses. These range from bulk amounts associated with the nuclear power industry to radioisotopes used in trace amounts in medicine, and even smaller amounts used in scientific research. Whether terrorists obtain materials domestically or smuggle them into the country, they will be transporting them within a large traffic flow that includes other radioactive shipments. Storage and transportation take place under regulations imposed by the Nuclear Regulatory Commission (NRC), the Department of Energy (DOE), and the Environmental Protection Agency (EPA), and state and local agencies

[44] The exception would be extraordinary situation in which it is known that a bomb is on its way into a city, and the only issue is to identify which vehicle is carrying it.

In general, the more that is known about the legitimate commerce in radioactive materials, the easier it will be to detect and track illegal movements, and possibly to detect diversions. Ideally (from the perspective of detecting terrorist activities), requiring advance notification of all legitimate movements of nuclear materials (above some threshold size or activity) would facilitate the use of netted sensors. At the least, if the netted sensor approach is pursued, analyses should be conducted to obtain a characterization of commercial nuclear shipments. To complicate matters still more, it is known that there are inadvertent movements of radioactive materials, for example scrap that has been contaminated at industrial facilities may be shipped without either shippers or receivers knowing that it is contaminated. For example, according to the Illinois Department of Nuclear Safety[45]:

> "Department staff respond on average once a week to scrap yard, landfill and waste incinerator radiation monitor trips. In most cases, the radioactive materials detected are naturally occurring, such as radium in pipe scale, or are residuals from medical uses of radioactive materials."

Shipments/transportation of nuclear materials form a background within which illicit movements would be conducted. In looking for attempts to smuggle nuclear materials, systems would have to contend with false alarms that arise from legitimate shipments. In the abstract, having precise knowledge of what is being moved throughout the country could facilitate picking out illicit movements of material. However, for that to be of use it would be necessary to be able to detect all movements, at least in selected areas. The existence of a database of movements of radioactive materials could help to reduce those false alarms.

Credible sensor networks could contribute to enforcing standoff from major targets. Publicizing the existence of such systems, if done correctly, might also contribute to deterrence. If the targets are points, such as the White House or Hoover dam or the New York Stock Exchange, the standoff is relatively easy to define after some assumptions are made about the possible yield of a terrorist weapon. However, that definition gets more difficult if the target to be protected is a city, since population densities don't usually decline abruptly as one travels from the core of the metropolitan area, and because cities tend to grow over time. Moreover, attempts to plan for enforcing standoff are likely to run into major political obstacles, both from those jurisdictions that could claim that they are being consigned to the "OK to nuke" category, and from those that would be tasked with stopping a nuclear weapon that could detonate when the vehicle it is in is stopped. Given the lethal range of nuclear weapons, it seems unlikely that any physical impediments to movement can be found that would provide sufficient standoff while not causing unacceptable disruption of normal life.

Almost by definition, surprise would be a basic element of a terrorist nuclear attack. Under those circumstances, there seems to be little that military units could do to foil the attack once it was launched. If it were known that a bomb was on its way in a vehicle, Army or National Guard units might be called out to provide traffic control and inspection, and crowd control. Similarly, Guard units might have a role in aiding police

[45] Excerpted from IDNS website: http://www.state.il.us/idns/projects/incident/matincident.htm

to intercept a vehicle that was identified through a netted sensor system. The added manpower, firepower, and aviation might be useful in that case.

Once terrorists have come into the US with a bomb or bomb components, the best way to stop them is likely to be good intelligence, investigation, and law enforcement.

Consequence Mitigation

The 1945 nuclear attack on Hiroshima taught several lessons, among them:

1. Nuclear blasts cause incredible devastation
2. Given decades, cities can recover from even a nuclear attack
3. The attack also destroyed the city's resources to help its victims

Had a more widespread system for consequence mitigation been available to Hiroshima, many more people would have survived, but the numbers of dead and dying would still have been very large. In the US we accept casualties up to perhaps 100 as the unfortunate but unavoidable consequence of natural disasters. We have also come to accept yearly traffic fatalities and gun deaths on the order of 35,000 (each category). All of these accrue fatalities gradually over a year; a nuclear blast could kill more than the number of Americans who died in WW II, and do so before the news media could tell the rest of us that it was happening.

Consequence mitigation efforts could make the aftermath of an attack a great deal less difficult for a large number of survivors, and therefore measures need to be planned. But the loss of life and property will still be staggering.

On the other hand, if there is an attack with an RDD, or a nuclear bomb that produces either only a small yield or no yield at all (and spreads radiation), prompt effective mitigation efforts could be very useful. Treatment and decontamination could pay major dividends. Contamination is likely to render homes uninhabitable and businesses unfit to reopen. In this respect, the attack would be on a par with many natural disasters or conventional bombings.

APPENDIX

A very short disquisition on
"terrorism" and WMD

This report, like most, will eventually use the term "terrorist" to describe a perpetrator of violence, for purposes inimical to our interests, who is not part of a recognized military force and not a "garden variety" criminal. States have militaries (come out and fight like a man), as do entities that seek to be states and are well along in their quests. Terrorist have political aims, but haven't reached some plateau of acceptance. The latter separates them from militaries. The former separates them from ordinary criminals, whom we view as acting for financial gain or out or personal emotion or perhaps inexplicable mishegas.

Terror is both a goal and a tool. This duality has bedeviled attempts to craft definitions that are generally acceptable. Moreover, what is terror to one observer is insurrection or freedom fighting to another. The first observer might see the acts in question as being directed against innocents, while the second would see them directed against "the enemy", either directly or indirectly.

Terror is the goal of the immediate violent act. The goal is to scare people who are not the immediate victims of the act. Terror, the act of scaring people, is a tool to get those people to grant a concession, or to put pressure on those that can (e.g. their government). Sometimes, the goal of producing terror coincides with another goal such as killing an individual (or group of individuals) for whatever reason.

Defining a person or a group as a terrorist (or terrorists) aids in the process of dealing with them. In the US it also aids the bureaucratic process of deciding who should deal with them. However, it does little to help in dealing with the act itself. In the case of an attack using nuclear means, the act has to be the primary concern. We are really concerned with two primary goals:

1. Limit the damage that can be done to US citizens and US assets by someone(s) attempting to employ a nuclear device;
2. Limit the ability of such a would-be perpetrator to cause fear among US citizens.

One might legitimately ask whether these two goals are not identical. They differ in that a demonstration, or partial demonstration, or seemingly credible threat might be sufficient, given the extreme destructive capacity of nuclear means, to cause widespread panic. In some ways, this psychological threat might be harder to deal with than the physical threat posed by actually attempting to attack a major target.

In the absence of countermeasures, what might be the public reaction to an announcement that there is a nuclear bomb in-place in a subway or utility tunnel

somewhere under Manhattan, and that it is set to detonate in two hours? Or how might the public react to a detonation that is carried out in some remote area?