HUDSON
INSTITUTE

DETERING NON-TRADITIONAL NUCLEAR ACTORS

Final Report

September 2009

Prepared for: Director, Office of Net Assessment
Office of the Secretary of Defense

(b) (7)(C)

Principal Authors

The views, opinions, and/or findings contained in this report are those of the author(s) and should not be construed as an official Depart of Defense position, policy or decision.

Deterring Non-Traditional Nuclear Actors

August 11, 2009

INTRODUCTION

A persistent uncertainty that earlier OSD/Net Assessment nuclear exercises revealed is how to think about deterring a range of new actors whose reasons for seeking to possess—and perhaps use—nuclear weapons come from radical religious or secular ideologies, deeply-held national and/or cultural beliefs, history, as well as criminal activity. A parallel question asks who may or may not be influenced by traditional ideas of deterrence. And, how can rogue regimes be deterred? Iran and North Korea were mentioned repeatedly during the exercise, as examples of states that may develop nuclear weapons as part of strategies for war-fighting and terrorism. Non-state nuclear actors—e.g., terrorists, separatists, criminals—are particularly difficult to deter because they are unlikely to possess an "address" or set of easily vulnerable assets that can be put at risk and because they may have a risk calculus that is different from that of stable states.

This workshop sought to address a number of issues:

- Who are these actors, and what is it we seek to deter?

- What forces, ideas, and visions of the future constitute their motives and intentions? What are the ideological bases of these actors' behavior? What cultural and religious influences inform their understandings of the challenges, opportunities, and choices that accompany possession of nuclear weapons?

- What kind of strategies do they envision for using nuclear weapons?

- What do these actors value, and would it be possible to deter them by threatening what they value?

- What kinds of instruments might be used in deterrence, and is there any correlation between the character of the instrument (e.g., nuclear weapons) and the strength of the deterrent?

- Do general principles apply to deterring non-traditional, ideological possessors of nuclear weapons, or is each case separate?

- What options—if any—exist if deterrence is not possible or very unlikely?

- Where are the gaps in our knowledge, and how do we fill them?

EXECUTIVE SUMMARY

Workshop participants stated that traditional deterrence theory is an inappropriate model for understanding emerging nuclear threats. Since the end of the Cold War, a potential enemy's culture and religion appear to have become at least as important as the calculated self-interest that once offered a measure of solidity and predictability to the principles on which the superpowers based deterrence. As Saddam's two confrontations with the U.S. demonstrated, the assumption that every opponent would always act in their apparent self-interest deserves to be questioned. Participants agreed that while the principles of Cold War deterrence retain some applicability, they are neither fixed nor shared. General agreement exists that deterrence must be reconsidered if the management of nuclear confrontation with non-traditional opponents is to be improved. However categorization of the motives and means of new nuclear-armed actors is as difficult as a simple division of all nuclear-armed states, groups, or actors into 'rational' and 'irrational.' As the number of actors grows, the range of goals and strategies to achieve them will also broaden. Our challenge is to understand how others think if we are to succeed in deterring them.

Significantly improved national intelligence is essential to sound deterrence policy. Effective deterrence depends on understanding an enemy's capabilities, assets, organizational structure, goals and motivation. Most participants agreed that U.S. intelligence agencies today are not well-prepared to collect and reliably analyze such information where emerging threats are concerned particularly. Some participants argued that since restructuring of the intelligence community would take at least 15-20 years efforts should focus on developing short-term capabilities. This could be accomplished by creating small teams both inside and outside the government which would help gather and process intelligence; submit assumptions about threats to critical scrutiny; and "red team: the conventional wisdom. Others pointed to useful U.S. and British assessments of Hitler that were produced amid World War II and disagreed that 15-20 years is required significantly to improve intelligence. They argued that the intelligence community currently lacks sufficient information to offer U.S. policy makers reliable judgments about other leaders' likely behavior; that our intelligence community's biggest challenge is to understand how other actors make key decisions, and develop useful insight into how senior policy-makers think.

Rather than assume that opponents' decision-making mirrors our own, a systematic method of categorizing nuclear-armed enemies is required. Though participants differed on how to establish the guidelines of such a system they agreed on what information is critical. This includes: the decision-making structure of a potentially hostile entity, geographic location, type and structure of patronage, motivation, mode of operation, access to information and its coercive capabilities.

Participants emphasized the importance of signaling in any policy of deterrence. The key question is: Are there are any signals that the U.S can send a potential attacker which would prevent or delay him from using nuclear weapons? Most participants agreed that the United States must improve its signaling capabilities. We need to know whom to contact, how to reach key individuals or groups, and what to say. Participants also emphasized the need to distinguish between short-term and long-term signaling and to build institutional capacities to accomplish both.

The old model of deterrence also hinders needed examination of an issue most participants saw as critical: the ideologies and motivations which drive non-traditional actors and their ability to "process" deterrence information in conventional ways. Improved understanding of how future potential enemies define their interests and seek to achieve them is likely to produce unfamiliar results and may surprise us about how to influence their behavior.

The workshop ended with both long- and short-term recommendations. General agreement existed that traditional deterrence needs to be re-examined, and that the intelligence agencies' ability to gather and analyze intelligence over the next few decades must be re-structured before they can function effectively. A stop-gap measure would be to establish a pilot program to determine the effectiveness of "mini cells." These would produce intelligence essential to a better understanding of non-traditional actors' motivations, intentions, organization, and the other categories mentioned above. Devising a systematic method of categorizing nuclear-armed enemies would provide valuable information about their capabilities, capacities, motivations, goals as well as ideologies and goals. The intelligence community's improved access to critical sources of information as well as its increased interpretive ability are critical to such categorizing. It is needed to help craft future deterrence policy as well as determine the most effective signaling policy.

CURRENT CONDITIONS

Old Deterrence Theory

All participants agreed that deterrence literature developed during the Cold War was poor, and *largely useless* in the new nuclear landscape. In the early years of the Cold War, research institutions such as RAND attempted to form theories of deterrence which focused on cultural characteristics of Soviet Russia. Participants argued that economic reasoning and rational theoretical models became dominant, quickly crowding out culture as an important element of understanding or predicting Soviet responses.

The economic/rational theory models triumphed. Over time, all deterrence theory, whether applied to states or non-state actors grew out of these abstract models. As traditional deterrence theory took root explanations that sought understanding in culture, history, ideology, and the effort to know more about the opponent fell by the wayside. Moreover, participants agreed that the old understanding of deterrence failed in its reliance on unproven assumptions. Of these the first and most dangerous is that the opponent will act according to what we understand as rational. Such an assumption is particularly ineffective in deterring irrational actors, or actors whose ideological framework is at substantial odds with ours. Since nuclear weapons were never used in the Cold War, many have concluded that shared rationality "worked" in deterring the use of nuclear weapons. However, some participants pointed out that we did not know much more about the Soviet Union than we do about many of the non-traditional actors we face today. Nuclear peace throughout the Cold War could be attributed, they contended, to luck just as much as any specific policy taken by the U.S. or the Soviet Union. Another participant argued that the theory of deterrence evolved during the Cold War into simplified assumptions about all actors' objectives and how they meant to achieve them. In the end everyone was assumed to be deterred by the same threat of an assured and destructive second strike.

Another assumption was that, because deterrence "worked" in the Cold War, its principles are immutable. As one participant noted, we "place hope in our deterring capability and then rely on luck

for it to function." Participants criticized taking deterrence for granted, and assuming that a certain set of military capabilities creates deterrence by their simple existence. According to participants the strength of these assumptions grew out of their ease: failing to question basic principles was simple and uncomplicated. Participants argued that the intellectual problem of what actually constitutes deterrence is substantially lightened by seeking answers that intelligence can easily supply. Participants agreed that the prospects for proliferation increase U.S. national security's reliance on luck[1] to prevent conflagration, a reliance that not all nuclear powers share. Islamabad, for example, does not see its weapons as deterring—as the theory would assume—but rather helping to change an undesirable status quo by *permitting* conflict.

Insufficient Intelligence

In seeking theories of deterrence that apply to the future, participants agreed that we must understand our opponents better. The geographical, cultural, and ideological spectrum of potential threats is enormous and represents a significant challenge for intelligence agencies. Respondents agreed that the many different U.S. intelligence services possess neither the organization nor the knowledge base to collect, analyze, and produce critical information that makes a difference to successful deterrence.

One participant noted a recent discussion with a senior American intelligence official. After asking him a series of questions about intelligence collection for deterrence, the official admitted that U.S. intelligence agencies are not structured to provide such information. "I was told that it would take 15-20 years to create the arrangements, educate the analysts, and then actually do it." This participant stressed that he was not seeking ways to criticize U.S. intelligence, but that our organizations are not set up to provide intelligence about leaders of unstable countries, groups, or key rulers, for example Kim Jong Il.

To improve deterrence, we must know more. This requires that our intelligence agencies ask the right questions: What do our opponents value? If not their lives, what else can we hold at risk? What goals do they seek and what mechanism or worldview allows the accomplishment of those goals? What assets allow them to proceed? What is their organizational structure and where are its

---

[1] Another participant questioned the role of luck in Cold War deterrence. He argued that both sides' nuclear arsenals were so large that deterrence was "over-determined," and likely did not rest on highly specific calculations about the consequences of going to war. Both sides, this participant noted, also had several decades during which they were able to establish "rules of the road" that diminished the chances of direct confrontation.

vulnerabilities? Another participant questioned why these questions should require 20 years for an intelligence organization to be able to answer.

TYPOLOGY

Structure and Factors

A major topic of discussion was how to categorize the nuclear opponents which the U.S. is likely to face in the future. Participants argued that a system of categorization could not, and should not, attempt to cover every possible state, group, or individual who could pose a threat to America. However, participants agreed that a typology could produce useful options in helping to craft effective deterrent policy that anticipates future threats. Participants proposed several methods for constructing such a typology.

One oft-mentioned idea was a spectrum along which opponents would be categorized and graphed according to a set of axes. For example, participants suggested that one axis would include the range of threats from states, groups, organizations, and individuals. Another axis would cover motives for using weapons of mass destruction, from apocalyptic ideologies to criminal groups with perceived economics-based rationales. Participants did not agree on this approach. Critics argued that its rigidity failed to explain important contradictions and sub-groupings, for example states that acted like individuals or groups whose actions paralleled those of states.

Although unanimity on a typology eluded the group, participants did agree on some characterizations of nuclear actors. These include several which one participant summarized citing a study that looked at 200 case studies of deterrence from 2000 B.C. to today. These factors include:

- *Decisions-Making Structures*: How are decisions made within the organization? Is power concentrated in the hands of one individual, a ruling council, elected officials, or some other system? This question addresses the problem of states that act like individuals or vice versa. For example, many believe that Kim Jong Il controls all decision-making in North Korea. Conversely, some believe that Al Qaeda reaches decisions based on consensus among its top leaders. Each structure poses challenges in deterrence: the policy of a sole dictatorship can be shaped if the dictator himself—

especially an isolated ruler whose access to accurate information is restricted—can be influenced. An oligarchy or semi-oligarchic dictatorship in which decision-making power is dispersed offers different challenges and opportunities.

- *Geographic Location*: Although participants did not reach full agreement about the importance of geography, several argued that a non-state actor's physical location will significantly affect options for deterrence. Such threats are subject to the coercive apparatus of the state, including laws, security forces, and the other powers that accompany state sovereignty. This also presents difficulties however, particularly for democracies, when policy responses can be constrained by public scrutiny.

- *Patronage*: Nuclear actors who receive support from states or groups offer complex challenges. The patron can offer nuclear actors wide-ranging resources including funding, raw materials, and technical knowledge, as well as both physical and political shelter. The presence of a patron complicates effective deterrence. Complications include increased demands on intelligence services, possible limitation of policy options particularly hard strike options, and decreased influence of political pressure and sanctions. A patronage relationship can exist between a range of actors including states that support rogue groups, states that support other states, and possibly groups that prop up weak states. While patronage relationships complicate the challenge of knowing whom to threaten, the existence of a patron offers an opportunity as a more accessible target than a non-state actor.

- *Ability of Deterrent State to Mix Tools*: The ability to exploit a broad range of methods, including dissuasion, co-option, and force improves the chances of successful deterrence.

- *Motivation*: All participants acknowledged a powerful link between successful deterrence and the strength and character of a potential opponent's motivation. While there is no clear scale of motivations from "easiest to deter" to "most difficult to deter," participants identified common ground on specific cases. Participants agreed that actors such as criminal groups, which operate for profit, are relatively open to give-and-take negotiations or threats. Actors whose motivations stem from a

completely different world view, or who are irrational are less likely to be deterred by such blandishments.

- *Modus Operandi*: The opponent's mode of operation is important in determining deterrence options. How quickly does the opponent believe he must accomplish his goals? Is an enemy willing to accept tactical retreat or a setback? Does the enemy insist on an "all or nothing" approach? Will he proceed despite—or perhaps because of—the likelihood of failure and death? Will he abandon his effort if it becomes clear his goals are unachievable? Is it possible to negotiate or at least communicate with these actors?

- *Access to Information*: In crafting an effective deterrent, it is vital to understand what access an actor has to information, and what biases and distortions are part of the information he depends upon for decisions. The Cold War idea of deterrence often assumed the enemy's access to accurate information. This assumption is dubious in authoritarian governments and dictatorships where the leader surrounds himself with "lies upon lies." Participants cited examples, including Saddam Hussein, Adolf Hitler, and Kim Jong Il, where entire governments subscribed to "denial and nonsense." Understanding how and what information is manipulated as well as the consequence of the distortions is vital in grasping an enemy's beliefs and how to approach them.

DETERRENCE COMMUNICATION

Signals

One topic emphasized repeatedly was the large role that signals play in deterrence. As participants explained, the United States' ability to send persuasive signals, to understand how to transmit those signals, and to interpret subsequent responses was crucial to effective deterrence Without this ability, deterrence is nothing more—as one participant put it—than a "policy based on faith." One participant noted the twin challenges of signaling: first, ensuring

that the signal will reach the intended target and second, that it will be understood. We may be transmitting, but this neither guarantees receipt nor correct interpretation.

As an example of successful signals, participants discussed America's wars with the Barbary Pirates led by Yusuf Pasha of Tripoli. President Jefferson was aided by the services and knowledge of Tobias Lear, whose years of residence in North Africa gave him significant understanding of Tripoli's ruler including his vulnerability to a U.S.-inspired effort to replace him with his brother, Hamet. In this case, effective signaling and knowledge of the opponent—including the ability to "read" his signals—saved the U.S. from more costly and violent direct action.

Signaling covers the gamut of strategic communications from direct contact with nuclear actors to indirect signals in seemingly unrelated situations. As one participant explained, "everything you do or don't do has an influence on all kinds of bad actors." Again, effective signaling depends on good intelligence, on knowing how to answer any of the following important questions:

- *How to contact?* Contacting opponents often poses a difficult logistical challenge. With non-state actors, there is often no "address." The enemy is likely to regard phone numbers, e-mail addresses, and other forms of direct communication as closely guarded secrets. How do we contact these actors? Significant intelligence work is required to discover methods of direct communication, as well as to uncover backdoor routes through family members, known associates, embassies, and public announcements.

- *Whom to contact?* The question of whom to contact within a state or organization speaks directly to identifying decision-making structures within states and groups that U.S. leadership seeks to deter. For any given threat, who gives the orders? Whose finger is on the trigger? If the leader cannot be contacted directly, who in the organization has access to, or influence over, that person? Finally, if there are factions or divisions within the state or organization, can we contact some of these groups? Can they be coerced or co-opted to cancel an operation?

- *What's the message?* Each case in which deterrence is judged necessary corresponds to a unique and appropriate message. Contributing substantial knowledge in crafting the proper message is a critical task for intelligence agencies.

Immediate vs. Continuing Signals

Participants also distinguished between signals that deter imminent threats, and those meant to preserve a continuing policy of deterrence. The purpose of the former is to defend against an immediate danger. Continuing deterrence requires that signals be conveyed over time to present an image that keeps others from becoming nuclear actors or from threatening the United States with nuclear weapons. Long-term, or continuing signals, include actions such as policy speeches, declared responses, and the firmness of leadership in the face of threats. Immediate and long-term signals are linked, and, if executed correctly, support one another. If either is carried out poorly, however, the overall effectiveness of signaling and deterrence if weakened. If deterrence of an imminent threat fails and the U.S. is attacked, other actors are likely to be encouraged. However, if the U.S. is consistently successful in deterring attack, other nuclear actors are likely to reconsider their calculations. Similarly, if the U.S. appears weak or cannot establish credible long-term signals, the effectiveness of signals against imminent threats will be diluted.

Participants expressed concern about current U.S. signaling capability. They argued that the U.S.' ability to signal against imminent threats is effective. Though terrorists struck at America on September 11, 2001, many participants believed that Washington's swift action in Afghanistan and against terrorism represented a strong immediate response. But, argued some, the U.S. ability to project effective signals against terror over time did not possess the same element of persuasion. Some participants claimed that Washington's inability to consolidate victories in Afghanistan, and the protracted inability to resolve security problems in Iraq signaled weakness and a wavering resolve to America's enemies. The question of U.S. resolve was, contended some participants, compounded by the widespread belief in the Middle East that the U.S. would soon cut its losses and withdraw from the region.

Similarly, some participants criticized America's inability to dissuade North Korea from acquiring and testing nuclear weapons. Many of the same participants applied a similar critique to U.S. policy toward Iran arguing that Tehran's likely acquisition of nuclear weapons despite oft-expressed U.S. opposition and policy demonstrates American weakness. One respondent argued that the lesson potential nuclear actors have learned from North Korea is that the U.S. could be played; that Washington would negotiate, apply sanctions, and give concessions, but in the end, would eschew direct action. As a participant explained, "What have bad guys learned in the last 8 years? If you strike directly, you suffer. But the other side is that for all the huffing and puffing [the U.S. is] not willing to use force to stop a country from getting weapons of mass destruction."

One foreign participant noted that American society, and often democracies in general, appears weak, faint-hearted and decadent to observers from non-democratic countries. Other respondents disagreed noting that the U.S. has been consistently underestimated throughout its history. Several enemies who had believed the U.S. to be weak had been "squashed" in the words of one participant. The key is to remind potential aggressors about history consistently and persuasively, because, as one respondent noted, "generally speaking, democracies win."

Predictable vs. Unpredictable

Participants disagreed over whether it was more effective for a state to be predictable or unpredictable in signaling deterrence. Some believed that a consistent policy was the best; those who might seek to threaten the U.S. could easily look back at examples of actors who had miscalculated and suffered grievously. These participants argued for a line-in-the-sand policy in which all threats, large or small, would be met with the same devastating response.

Others held that such policy risks being ineffective. They offered two reasons. First, the type of response demanded by an inflexible and potentially disproportionate policy could be impossible to execute for political, humanitarian, or simply technical reasons. The U.S. could find it difficult to launch a devastating response depending on the target, its location, or the malefactor's patron, for example. If the U.S. declares a policy that it cannot execute, its credibility will suffer. Second, any policy that is too rigid will encourage opponents to seek effective countermeasures. Instead, advocates of a more flexible deterrence strategy argued

for measures tailored to particular circumstances. This group contended that the U.S. should occasionally "make an example" of an enemy to remind potential actors of U.S. power and resolve.

Capabilities

A brief note on military capabilities and signaling is in order. Although other Hudson reports prepared for ONA have addressed the disparity between current military capabilities and the effective response on which effective signaling depends several participants emphasized repeatedly that the American strategic arsenal today is not equipped effectively to address several important requirements of nuclear deterrence. In the Cold War, deterrence was theoretically based on the massive power of both sides' armaments and the "mutually assured destruction" which would result from prolonged nuclear broadsides. This form of deterrence is less applicable today because the precise location of many non-traditional actors is not known. Strikes based on what we think we know would likely produce large civilian casualties and could well fail to remove the sources of the threat. Deterring such actors requires strategic capabilities beyond those that were needed during the Cold War. Whether the U.S. possesses these tools or has any intent to develop them in the near future is unclear.

Potential enemies' understanding that America lacks tactical, precision strike and conventional strategic weaponry undermines the credibility of American nuclear deterrence. How can the U.S. impose unacceptable damage on an opponent who possesses buried or exceptionally well-defended weapons? Can Washington still credibly promise to strike an opponent whose weapons are within the blast radius of large civilian populations? Radical actors and regimes will be encouraged to acquire and use nuclear weapons if they believe that the U.S. lacks the capabilities to destroy their arsenals or mount a politically acceptable strike.

OTHER INSIGHTS

Values

Participants stressed that values, ideologies or motivations that differ from our own should not be dismissed as "crazy." Often these ideologies are internally rational, consistent, and thus understandable and vulnerable. For example, participants argued that, if our opponents did not value their own lives, then our task is to discover what they do value and how to threaten it. Certain actors may be willing to die for their particular cause, but they are not willing to put their own families at risk. Participants discussed cultures which require a son to carry on the family's history and bloodline. Would these actors be willing risk their family's heritage and future?

Participants asked what opponents wish to achieve if they are killed attempting to accomplish their goal. The objectives of these enemies may not be physical, financial, or familial. More likely they want to strengthen an idea, inspire others, or reduce the power of what they regard as hostile values. Could these actors be persuaded to abandon their goal, or at least their current operations, by convincing them that their goals are unattainable; that for all their efforts, including self-destruction, their cause will be vilified, mocked, or perhaps worst of all, ignored?

Non-Traditional Intelligence Sources

In discussing needed improvements to the quality of U.S. intelligence about the leaders and organizations of rogue groups and states, participants underscored the importance of non-traditional information sources. To better understand these leaders, intelligence services should identify and debrief family members, close associates, and those who interact with them on a regular basis. For example, one of the most useful sources on Kim Jong Il was his former sushi chef. Apparently, Kim would often discuss why he felt he needed nuclear weapons with his chef during meals. Another example was Mao Zedong's physician, who later revealed several of Mao's musings on nuclear technology and weapons. Consistent with

these examples, the U.S. once employed a team of psychoanalysts to interview the relatives of several Iranian leaders. In short, creative possibilities for gathering intelligence exist and can be exploited to advantage with the support of the appropriate agencies.

RECOMMENDATIONS

- **A New Theory of Deterrence-** Given the emergence of non-traditional actors and shifting nuclear balance as the U.S. commits itself to strategic draw-down, it is clear that the usefulness of the Cold War deterrence paradigm must not be taken for granted. The U.S. must reconsider nuclear deterrence policy in light of the increasingly non-traditional character of current and future potential nuclear opponents. This includes the requirement significantly to increase understanding of threats. Dismissing them as "crazy terrorists" or eccentric regimes will diminish our security. Cultural studies and analytic profiles of groups and leaders have become vital to successful deterrence policy.

   Some participants believed that appropriate analysts and experts should be encouraged to publish more articles, which might help speed the process of reconsidering deterrence. In particular, articles that highlight the limitations of previous assumptions about deterrence, and the equally problematic character of current thinking would be especially helpful. These articles should be as specific as possible for the purpose of shaping administration policy.

- **Intelligence:** To modify our doctrine of nuclear deterrence, the U.S. intelligence community must restructure and retrain itself. If the process requires 15 to 20 years there is not a moment to waste. In the meantime, several participants suggested assembling teams from inside and outside government to assist in short-term intelligence collection and analytic and psychological profiling. Respondents stated that organizing a "mini-cell"—for the purpose of tackling a specific issue or country— could serve as a pilot program to demonstrate the effectiveness of this approach. If it accomplished nothing else a mini-cell could "provide a basis for avoiding errors." Greater success would be measured by accurate predictive skill and policy

recommendations. The U.S. Strategic Command already possesses such a group, but it possesses no institutionalized capability for collecting intelligence.

- **Typology:** Participants favored developing a typology of nuclear threats. They emphasized the need to categorize threats and maintain options for responding to opponents. Though most respondents favored this idea, they did not reach agreement about a specific format. Some favored a spectrum that would represent threats, including states, non-states, and individuals, by plotting them along visual axes based on critical factors. Another idea was to choose six of the most dangerous groups, and complete exhaustive profiles on their motives, capabilities, and organizations. Whatever the eventual structure, some form of typology is vital in providing policymakers with a basic description of opponents.

- **Signaling:** The U.S. must undertake a complete review of signaling capabilities to ensure swift and effective communications in a crisis. To gain a better understanding of this complex subject, participants agreed that a full review of American response doctrine and long-term signaling is needed to understand when the U.S. has succeeded in long-term deterrence signaling. The same study should concentrate no less on when, how, and why the U.S failed to communicate a clear, credible, and consistent message. One participant argued emphatically that the U.S. must review its doctrines on the use of force. This participant contended that unclear U.S. signals have contributed substantially to the likelihood of unfavorable outcomes as North Korea and Iran seek status as nuclear powers.

- **Know Where to Find Expertise**- Thirty years ago, the U.S. government tracked and maintained records of all PhD degrees awarded. The objective was to build a knowledge base for when the government required particular expertise. This program eventually disappeared. Multiplying non-traditional threats against the U.S. should prompt reconsideration of the discarded practice. This would offer policymakers a catalogue of experts who could be consulted as new threats emerge or new intelligence suggests a serious increase in existing threats.

Appendix I: Discussion Papers

Dissuading Undeterrable Opponents

(b) (7)(C)

It is an odd but undeniable fact that, throughout their 250-year history, liberal democracies have consistently been underestimated as strategic competitors by their non-democratic rivals. At the start of the 19th century, Europe's monarchies had little regard for the new American republic and few expected it to survive for very long, let alone to surpass them in wealth and power in a matter of decades.

In the twentieth century, totalitarians of all stripes were contemptuous of democracy. German, Japanese and Italian fascists regarded the United States and its Western allies as soft, decadent, indecisive, weakened by racial and ethnic impurity and by their Judeo-Christian beliefs, and, above all, lacking in will. After meeting with British and French leaders at Munich Hitler reportedly described his counterparts as "worms." Seven years later Hitler was dead, fascism was finished and the worms had won.

Lenin and Stalin had somewhat more respect for their Western capitalist rivals, in part because they saw them as occupying a necessary step on the ladder of socio-economic evolution, but also because they regarded the captains of industry and finance who were the real string-pullers behind the charade of liberal democracy as worthy adversaries: tough, ruthless and determined to hold on to their privileges. In the long run, however, Soviet leaders from Khrushchev right down to Mikhail Gorbachev seem to have believed that their system of production would ultimately be proven superior and that, one way or another, they would someday "bury" the West.

Despite liberal democracies' repeated triumphs, and despite the fact that they are themselves far weaker than their predecessors, today's post-Cold War dictators are still inclined to make the same mistakes. Saddam Hussein apparently believed that the United States would not attack him because the American people could not accept the casualties that he would inflict on their armed forces. Strangely, and ultimately fatally for Saddam, he seems to have continued to believe this even after his own experience had proven it to be false.

Albeit for somewhat different reasons, Al Qaeda and other Islamist extremist groups have an equally contemptuous attitude towards the West. Osama bin Laden's theory of victory turns on the assumption that, if he can inflict enough pain on the United States he can compel it to withdraw from the Middle East, leaving its secular puppets ripe for overthrow by his followers. The jihadists' believe the West is weak because it does not follow the true faith and has therefore succumbed to the temptations of materialism and the flesh. If Westerners truly fear death as much as the Islamists believe, while they themselves embrace it as fervently as they claim, there can be no question of who will ultimately win the struggle between them.

Notwithstanding their bluster, adversaries who are state leaders can be deterred in the usual way, by convincing them that they will pay too high a price for whatever acts of aggression they have planned. Because supreme leaders like Saddam seem invariably to be unbridled narcissists, the best and perhaps the only way to deter them may be to convince them that they themselves will die if they go too far. (Despite its brutality, the grainy cellphone footage of Saddam's execution probably served a useful purpose in this regard. Pictures of Hitler's funeral pyre, his Nazi underlings in the dock at Nuremberg or Slobodan Milosoveic on trial at the Hague or Manuel Noriega rotting in his maximum security prison cell should also be required viewing for dictators contemplating war with the United States.)

Stateless terrorists eager for martyrdom are another matter, for reasons that are by now all too familiar. Deterring them may be impossible either because they believe they can escape punishment or because they do not fear it. In such cases the best that we can do is to try to convince potential attackers that, whatever tactical successes they may achieve, they will ultimately fail to gain their strategic objectives. This is partly a matter of reminding enemies that liberal democracies (and the United States in particular) can be tough when sufficiently provoked. Whatever else we have achieved in Iraq and Afghanistan in the last eight years we ought to have succeeded in dispelling the notion that the United States is unwilling to take casualties.

Beyond this, however, is the less tangible fact of liberal democracy's resilience. The long-term historical record alluded to here, the fact that, for over two centuries, liberal democracy has seen off one challenger after another, may be too remote and abstract to have

much of an impact on a contemporary terrorists' thinking. But more immediate examples can convey a similar message: the 9/11 attackers brought down the World Trade Center, but new buildings will soon rise in their place. The Madrid and London bombers blew themselves to bits and won notoriety for a time. But now they are forgotten and those two great cities, and the societies of which they are a part, have gone about their business as if nothing had ever happened. A nuclear weapon detonated in a Western city would do far greater damage, of course, but we need to do what we can to persuade potential attackers that the end result would be the same. Our message should be that liberal democracies, with their flexible economies and adaptive political institutions, cannot be destroyed or even deflected by the kind of damage that even the most cunning and bloody-thirsty terrorists can do. If we cannot deter suicide terrorists with threats of punishment we will have to try to dissuade them with the promise of futility.

Deterring Ideological and Sub-state Actors from Using Nukes

<u>The Concept of Deterrence</u>

Conceptually, deterrence is a simple process between two parties in conflict. Deterrence serves the preservation of the status quo. The party preferring the status quo tries to influence the challenger of the status quo (the deterred party) to not take action. The deterring party issues threats clarifying that if the other party will pursue its intentions to harm the interests of the first party, there will be costly retaliation. The deterring party attempts to influence the cost-effective calculations of the intended deterred party assuming bounded rationality of the decision making process.

Several elements revolving around the notion of threat are needed to create effective deterrence.

1. The threat must be communicated to the deterred party and a certain degree of clarity about the nature of the planned retaliation is needed. Ambiguous threats might be interpreted in ways not conducive to deterrence.

2. The threat must be credible. Credibility is important in two primary senses: capability and determination. The physical capability to carry out the threat must be unequivocal, as well as the freedom to act in accordance with the threat issued. Similarly, the political intention of the deterring government to make good on the threat must not be questioned.

3. The threat must allude or specify a magnitude of cost that will be great enough to affect the cost-effective calculations of the deterred party.

Conventional deterrence is substantively not different from nuclear deterrence. Therefore, creating effective deterrence against nuclear opponents requires the same rationale. The presence of nuclear weapons in the equation only indicates a larger cost involved in the strategic interaction.

In addition, the conceptual framework above can in principle be applied to many international actors with a few exceptions. Actors lacking instrumental rationality, i.e. there is a logical connection between means and ends, are not easily deterred. Absence of instrumental rationality prevents cost-effective calculus, which is crucial in the deterrence

process. Similarly problematic is establishing deterrence versus entities that have suicidal tendencies because their sensitivity to cost is close to zero. Such entities are not susceptible even to threats that extract massive costs. A strategy of deterrence does not work against such irrational organizations. In those cases prevention and/or annihilation must be adopted to prevent damage to the interests of the status quo power.

US Deterrence against Nuclear Attacks by Ideological States and Sub-state Actors

Most of the current enemies of the US, such as North Korea, Iran or Al-Qaeda, are not categorized as irrational actors despite their features of "crazy state/organizations." Such actors are usually described as subscribing to far-reaching goals (challenging US dominance in world affairs), great commitment to attain them (even at the expense of an armed conflict with the US) and an unconventional style in pursuing their goals (See Yehezkel Dror, *Crazy States*). In any case, the enemies of the US are unable to annihilate a superpower and, therefore, adopt a strategy of attrition – a series of small attacks (pricks) to gradually weaken the US.

Noteworthy, their conventional abilities to harm the US are limited. Even if we envision several attacks on American soil of 9/11 magnitude, the estimated damage is manageable within a relatively short time. Even if the enemies of the US acquire nuclear warheads capable of attacking US territory and American targets abroad, the damage will still be far less than a Soviet-inflicted attack. Current technologies, such as Weapons of Mass Destruction (WMD) and anti-ballistic missiles, still do not allow these actors to impose a fraction of the cost of a nuclear exchange between the Cold War superpowers.

The mere fact that prospective damage is limited hampers deterrence. The challengers believe they can get away with causing limited damage that is not an existential threat to the US. A nuclear attack on an American target overseas obviously does not cross the existential threshold. Even one nuclear explosion over an American target could be viewed in such a fashion. This is particularly true if this occurs after the crossing of the nuclear threshold by exploding one or several radioactive devices that fail to trigger a large-scale American response. The dilemmas of how to respond to a strategy of attrition are well known, but "moderate" responses and reluctance to escalate are not conducive to deterrence.

By definition, the actors discussed here have a different value system than Western democracies. Therefore, it is extremely important to understand the psycho-cultural ideosyncracies of such actors to successfully apply the framework of analysis delineated above. Intelligence regarding their understanding of the world and their belief system is a precondition for building effective deterrence. In short, Washington must learn how to communicate with such hostile entities and to understand what they value most.

It is important to understand how such entities view the US to craft successful deterrence. Islamist groups usually view America paradoxically. On one hand, the US "imperialist" impulses and its "decadent" culture are viewed as a grave danger to the Islamic world and its traditional values. On the other hand, America is regarded almost deterministically as a declining great power and civilization, essentially not tough enough to withstand the pressures originating in the ascending fundamentalist Islamist elements.

Having such an image of American capabilities and resolve undermines American deterrence, particularly in the case of nuclear armed sub-state entities.

Communicating a threat that a nuclear attack will trigger retaliation is the first element in the model presented above. The intention to use nuclear weapons against the US simplifies the need to communicate a deterring threat because the mere nuclear attack warrants a serious response. This is clear to nuclear armed states. America can clarify its message through public statements or diplomatic channels. Yet, this "automatic" dialogue is less clear to sub-state entities that might think that the US is unaware of their existence (the anonymous strike), or of their recently acquired nuclear capabilities. Therefore, communicating a threat in public or via the sponsors of the sub-state entity is important for the US to establish a nuclear "dialogue of antagonists" (A Raymond Aron phrase). Issuing a threat, however, might carry a price – undermining efforts to annihilate the entity or its nuclear arsenal. Furthermore, under certain conditions it might create panic at home.

Sub-state entities without a territory in their control can hardly develop nuclear weapons. Therefore, in most cases, these entities will acquire nuclear weapons from nuclear states. Alternatively, sub-state entities can steal/obtain such weapons from weak or failing nuclear states (Pakistan). States with the potential of providing sensitive technologies or

weapons are easier to deter. As mentioned, communicating the threat is not a problem, although its content could be subject to various interpretations. This will affect credibility.

The second element crucial to deterrence is the credibility of the threat. Taking into consideration the image of America in the eyes of the Islamists, or other radicals, is a problematic issue for the US. While the US has the capability to damage any target in the world, its ability to identify a target of consequence to a sub-state entity is questionable. The leaders of the sub-state entity might believe (even if it is not true) that their peculiar status provides no clear address for retaliation. The mere fact that Bin Laden remains at large and sends videotapes to international television channels is not beneficial to American deterrence.

Moreover, Washington's determination to strike back is questionable in the eyes of the Islamists, particularly if the American target was not on American territory. America is, after all, seen as a paper tiger who avoids retaliating in kind. The Islamists may correctly perceive that the US will hesitate to break the nuclear taboo even if attacked first by nuclear weapons. Moreover, the enemies of the US may choose to attack under political circumstances perceived to hinder an American response (i.e. on election day or just before it, or when American forces are engaged elsewhere). Radical anti-American ideological organizations have greater chances for misperceiving American determination.

Finally, the threat must clarify what is at stake and must specify that something valuable to the challenger of the status quo will be targeted and eliminated. The states that might challenge the US with nuclear weapons directly or via proxies might decide they are ready to pay a heavy price for a nuclear hit on the US. Iranian leaders stated that they are ready to risk the loss of millions of their countrymen in order to destroy Israel – in their eyes a terrible theological affront. Such readiness to bear pain is precisely one of the reasons why economic sanctions rarely work. Hardships of ordinary people are of marginal impact on the strategic calculus in such states. The issue is not their rationality, but their sensitivity to cost. Even massive nuclear retaliation seems to be insufficient to deter such leadership.

Therefore, the US must threaten what is valuable to such leaders. It could be regime survival, although temporarily losing a grip of a country is not necessarily a terrible loss for ideologues with a long historical perspective and who are confident that God (a powerful international actor) is on their side or that their cause will eventually win. Radical leaders

might care about their tribe members (Takhritis for Saddam), or their close associates (they might be dispensable). Usually, the most valuable asset is their lives and the lives of their close family relatives.

In ancient times deterrence was achieved by taking rival family members as hostages. Their welfare was contingent upon the good behavior of the opponents. Democracies of today may have difficulties adopting such measures, but relatives of the rival leaders who are convicted to death could be used in a similar fashion. Their execution could be delayed in exchange for specified abstinence on part of the radical entities. Diplomatic immunity should be conditioned on good behavior as well. What is required of course is much greater legal flexibility on part of the Western democracies.

Since the radical enemies of the US seem to display a propensity for accepting high risks in challenging the US by the mere use of a nuclear device, the US must make sure that its planned retaliation entails a heavy cost (in the challenger's eyes). As miscalculation is always possible, reduction of uncertainty requires an increase in the planned price to be exacted for a nuclear challenge. The price must nevertheless be somewhat commensurate with the expected damage to the US. Otherwise, the threat loses its credibility. For example, threatening a non-state entity with the total destruction of its host country is not credible.

For the purpose of enhancing the credibility of deterrence, the US needs to establish a reputation for ruthlessness and for not hesitating to use unconventional methods to get back at enemies of the state. Since the view of the US among its ideological opponents is sinister, there is a receptive audience that views the US in barbaric terms. The US faces moral and legal constraints in exhibiting ruthlessness. The difficulties surrounding the approval of assassinations constitute a good example. A honest and realistic debate over how to treat dangerous organizations and states should be encouraged by the American strategic community in order to allow greater leeway to American agencies fighting the "bad guys." Deterrence cannot be maintained for long without a reputation for ferocious responses. Actually, the US should capitalize on the opportunities it has to use military force in a manner conducive to building such a reputation. For example, apologizing for mistaken attacks on civilians hampers deterrence.

In the absence of an ability to demonstrate ruthless qualities in public, the US should spread rumors of ruthless American acts. In certain quarters, castration generates greater fears than the death penalty. Psychological warfare is part of the policy menu. This is not exactly the public diplomacy the American government envisions nowadays, but the US must realize that there is an inevitable tension between projecting a friendly image abroad and a deterrent posture. "Engagement" policies are often seen as appeasement and they project weakness. This is especially true in the Middle East. Such policies reinforce the "paper tiger" image and are counterproductive for the achievement of deterrence. Attempting to reach an optimum mix of Dr. Jekyll and Mr. Hide is problematic.

It is plausible that the psycho-cultural differences among the various entities challenging the US require tailored deterrence. Each one of America's challengers might require distinct deterrent postures. Such a multi-deterrence policy must show awareness that what is effective in one case can undermine deterrence elsewhere.

Conclusion

Deterrence requires a thoughtful approach to communicating the appropriate threat and maintaining its credibility. Deterrence is a good way to protect ourselves, and it has a decent chance of succeeding if the US adopts the right strategy. However, deterrence is not completely reliable. Misperception and miscalculation are ubiquitous, and in a few cases deterrence is patently ineffective. With lives at stake, the US should also consider additional strategies to reduce harm if deterrence fails.

Deterring Unconventional and/or Ideological Actors from Using Nuclear Weapons
(b) (7)(C)

It is by no means certain that one can identify a separate category of unconventional or ideological actors. A common fallacy in the deterrence debate is the inclination to distinguish between traditional deterrence and so-called new challenges. A closer look at History would call for a more measured assessment. Many adversaries of the West in the past, from Nazi Germany and imperial Japan to the Soviet Union and Communist China, were, to a large extent, ideological or unconventional actors. Deterrence during the Cold war was a complex exercise, never as simple as many believe it was in retrospect. And the idea that some actors are rational and others are not – thus suggesting two very different ways to deal with a threat – has been disproven by several decades of research. Almost all actors are rational, but none of them is entirely rational. Rationality is a matter of degree – it can be "thick" or "thin" – but it is always "bounded".

It is also questionable to claim that deterring State and non-State actors are two fundamentally different exercises. Almost actors have values as well as goals and means (though the two might not always be connected). Even when they do not have a clear return address, have at least a physical existence, assets, training camps and bases of operations, supporters and sponsors. Osama bin Laden himself has referred several times to the concept of deterrence, including in relation with weapons of mass destruction. Finally, the relationship between States and non-States should be defined in shades of grey, not black-or-white. A non-State actor can live in osmosis with a State (Al-Qaida in Afghanistan before 2001), share a territory with it (the Taliban in the Pakistani FATA), be a parasite (Hezbollah in Lebanon), or be a predator that feeds on the States' remains (Somalia, Congo, etc.). Coups can result in the existence of quasi-States with no clear legal status (think of the Gaza Strip under Hamas rule, or of the French Algerian departments in 1961 during the generals' coup[2]).

As an example of a particularly tricky "non-Westphalian" deterrence scenario, consider the following hypothesis. A terrorist group has built a nuclear weapon on the

---

[2] The latter may appear as a particularly appropriate example given that there was a nuclear device on Algerian territory, and that at least one of the four generals involved in the coup was reportedly interested in its existence.

territory of the Georgian breakaway Republic of Abkhazia. Who do you "hold accountable" for having failed to prevent such an act: Georgia, an ally of the West, or Russia, the patron of the secessionist Republic?

In operational terms, this means not only that many lessons the past decades may still apply to current and future challenges, but also that we should attempt to construct something like a "unified theory of deterrence" rather than try to define a separate code of conduct for so-called new challenges.

What follows is an attempt to define a series of possible rules for particularly complex deterrence challenges when faced with a potential nuclear threat, whatever the shape and nature thereof. It seeks to go beyond the usual – and useful – recommendations of "getting to know your adversary" and "tailoring deterrence".

It does not seek to evaluate the probability of nuclear use – or the temptation of such use. This author believes that this probability is rather small. Few authors would have betted in 1989 that no nuclear use would have taken place twenty years later. Each passing year without a nuclear weapon detonated in anger reinforces the idea that there is a general norm of non-use. There is no evidence that any State possessing nuclear weapons considers them as war-fighting instruments; all claim that they are for deterrence. The only drawback is of course that this creates a possible *incentive* for some particularly twisted minds, leaders of States or terrorist groups, to be the first to break the taboo, and, incidentally, to become at that very moment, in historical terms, the symbolic equal of the United States.

General Rules

Since the stakes are high and the challenge complex, deterrence as a matter of principle should be multifaceted and use all available means. We should, for instance, guard against the temptation to equate deterrence by reprisals with State threats, and deterrence by interdiction with non-State threats. The trilogy "Dissuasion-Interdiction-Retaliation" should be considered as a portfolio of options useful for all circumstances. In most scenarios, all three elements should be used to varying degrees, while tailoring them to a given situation.

Regarding terrorist use, dissuasion may be as important as deterrence. Contrary to what some experts assert, it seems reasonable to consider that terrorist acquisition of a nuclear weapon would be geared towards its use. The investment would have been too great, and the temptation would be too strong. There would be no proper way for the group to communicate the existence of the existence of its nuclear capability for compellence or deterrence purposes[3]; and the timeframe between our possible discovery of their project and the planned detonation may be too short for attempting to deter use. For such a case, "dissuasion" is thus arguably more important than "interdiction" or "retaliation".[4] Improving dissuasion could be achieved through several means. *First,* we need to reduce the apparent attractiveness of nuclear terrorism. It is not helpful, for instance, to claim publicly that building a nuclear weapon is an easy task. Most importantly, continuously claiming that a nuclear terrorist attack would be a transformative event which would alter the very foundations of our civilization contributes to its attractiveness. As Brian Jenkins has cogently argued, our fears have allowed Al-Qaida to become the first terrorist nuclear power.[5] *Second*, we need to enhance the potential costs of nuclear terrorism in situations where it may be a means towards a political or religious goal. For instance, the help of respected but moderate clerics could help diminishing the perceived benefits of such acts, by condemning them in advance and help turn Muslim public opinions against their perpetrators – thus inducing the rational decision to avoid resorting to nuclear means for fear that it would hurt, rather than enhance, the prospects for the establishment of a global Caliphate.[6]

---

[3] One conceivable way to do so for a group which has been able to build a nuclear weapon would be to send a few milligrams of fissile material (highly enriched uranium or plutonium) to the appropriate addressees, along with a copy of the design used. However, the group would have to be certain to have used a functional design, and there would still remain a major uncertainty regarding the success the group had in actually building the device.

[4] Some of the parameters of dissuasion and interdiction are well-known: securing nuclear weapons and fissile material sites, establishing monitoring devices, develop protective measures such as missile defense, force protection, civil defense, etc. For this reason, they are not developed here.

[5] There is arguably a dilemma here. Emphasizing the risks of nuclear terrorism might be necessary to muster the will and political support that may be needed for interdiction measures (detection, forensics, fissile material stockpile security, etc.). It may also be an unwanted by-product of deterrence statements: forceful declarations regarding the kind of reprisals we would make in case of a terrorist attack reveal that we attach a high price to avoiding the materialization of the risk of nuclear terrorism.

[6] Some clerics may also recant under pressure: after his arrest, Nasir bin Hamd al-Fahd, the author of the infamous treatise on the legality of the use of mass destruction means, publicly rescinded his fatwa on Saudi television.

Try to make the deterrence learning curve steeper. As shown by the case of South Asia, deterrence education may take several decades despite the enormous corpus of knowledge and experience gained by the nuclear parties to the Cold war. Informal seminars and targeted publications may help reducing the time needed for new nuclear actors to fully grasp the language and codes of nuclear deterrence, as well as the meaning and details of our own conceptions in this domain. This may (marginally) reduce the chances of nuclear use.

To take into account your adversary's irrational behavior, adopt his mindset. Leaders may have irrational behaviors due to illness, the use of drugs, or the influence of traditional beliefs. Assuming there is good intelligence about a leader's physical health, personality and behavior, the help of doctors, clerics, and even astrologers or numerologists may be precious when attempting to predict the adversary's decisions or reactions.[7] Finally, even in situations when "the reward is the afterlife", there could be ways to affect the notion that suicidal behavior will be beneficial. Again, some clerics can be mobilized to counter the notion that mass killing of innocent civilians is ethical – especially if it involves suicidal behavior. At the extreme, the prospect of the afterlife itself could be manipulated: for instance, the colonial practice of threatening to bury a rebel in a pig's skin could be revived to have a deterrent effect.

Retaliation Threats

Precedents matter; general deterrence comes from cumulative effects. Adversaries unfamiliar with Western culture may easily misunderstand us, and we have to take into account the possible deterrence impact of our strategic decisions. Western actions in Lebanon in the 1980s or Somalia in the 1990s brought the perception that we were weak.[8] The

---

[7] Adolf Hitler reportedly believed in the magical power of the number seven. The date of birth of Kim Jong-Il (16 February) has such value that officials of the inner circle would have it on their license plate. (A healthy reminder: traditional beliefs are not exclusive to ideological/unconventional actors: Ronald Reagan had events planned according to astrological opinion, and Woodrow Wilson believed that the number thirteen had brought him good luck throughout his life.)

[8] By contrast, the Soviets sought (apparently with some success) to "establish deterrence" in a famous action where they allegedly kidnapped and mutilated the son of a religious Lebanese leader. There is also the story – that may or may not be apocryphal – about the alleged threat of a Soviet missile "accidentally" falling on a key Iranian target (depending on the version one believes in, it would have been Khomeiny's residence on the Caspian Sea, or the holy city of Qom).

invasions of Afghanistan and Iraq may have had a deterrent effect, like the increasing number of national and international prosecutions for war crimes may have a deterrent effect (for instance, Tariq Aziz and "Chemical Ali" were tried for, inter alia, chemical weapons use against the Kurds). Perceptions of our actions and their cumulative effects need to be thoroughly studied. Deterrence may have to be established or re-established when it has failed. The 1986 bombing of Libya was unsuccessful if one considers that Tripoli was directly responsible for the 1988 Lockerbie sabotage. Some actors may have concluded from the subsequent difficulties of the United States and its partners in Iraq that Washington will never do "regime change" again. The 2006 US warning to North Korea, according to which the transfer of nuclear weapons would be considered unacceptable, may have been unsuccessful given the continuation of the Syrian reactor project (and perhaps others).

There should be no taboos in deterrence of nuclear use. Like dreaming, deterrence happens in a virtual world. Unlike compellence, it does not seek to produce any positive material effects. Action policy can be very different from declaratory policy. Thus there should not be any morality or legality considerations in deterrence – only credibility matters – especially when one tries to deter nuclear use.[9] There should be no restraints, regarding hypothetical possible targets (from families to religious sites), or possible means (from hostage-taking, torture and mutilation to massive nuclear weapons use). For instance, if it appeared that threatening Mecca, Medina or Qom could be a particularly efficient device to deter a nuclear jihadist actor, we should not hesitate in doing so – with the obvious caveat that such a threat could not be made in public, because of the dramatic unwanted political effects it might have.[10] Extreme scenarios call for extreme deterrence. Again, this does *not* mean that planning should exist for the actual destruction of such cities – especially since this would be illegal in most Western countries.[11]

---

[9] The 1996 International Court of Justice advisory opinion on the "use or threat of use" of nuclear weapons seems to indicate a different point of view. However, the Court did not assimilate "deterrence" to the "threat of use".

[10] A difference may thus have to be made here between States and non-States: private communication to a government is easy, while finding the proper addressee for a non-State may sometimes be very difficult.

[11] With regard to deterrence vis-à-vis States, it should be reminded that the threat of regime change has proven unsuccessful for compellence vis-à-vis Afghanistan and Iraq. It is by no means certain that it would be enough as a deterrence threat.

But the threat of nuclear retaliation is a tool of limited usefulness. The threat of a nuclear response would be clearly useful in two cases: that of a State attack, and that of a deliberately and clearly State-sponsored attack. It is by no means certain that its usefulness go much beyond that. It would not be credible, for instance, to threaten to annihilate an entire region of a State which has no responsibility for the attack. However, it could be suggested that we would leave no chance to the possibility of further attacks and that, therefore, the scope of our retaliation strikes might have to go beyond the destruction of the perpetrator's centers of power.

Strategic ambiguity has significant drawbacks. Strategic ambiguity (for instance through the use of expressions such as "grave consequences" or "overwhelming and devastating retaliation") is a device used to avoid unwanted diplomatic effects of deterrence statements, maintain the freedom of action of political leaders and avoid the "commitment trap". However, it can lead to a significant misunderstanding of our intentions. Deterring nuclear use might require more strategic *clarity*.

The medium may be almost as important as the message. Some actors may be more receptive to messages delivered by close confidants than by public threats; for instance, in many traditional cultures, the best messenger may be a close relative of the Head of State or Government. Others may be more receptive to messages delivered by their own kind: for instance, a military officer might be the best messenger to talk to an enemy military officer. In general, to ensure that the deterrent message is well-heard and understood, redundant channels of communication should be used.

Inducements may be necessary. In some circumstances, a way out may need to be provided to the adversary. A State may consider nuclear use if all his options have failed. Discreetly granting personal immunity to leaders or executants in case they give up their nuclear option may help them weighing their choices differently.

"Indirect" Deterrence

Deterring State sponsorship should be tailored to the exact situation. Just like the general relationship between States and non-States, the nature and degree of sponsorship can vary significantly. At one extreme, one finds the proverbial deliberate decision by a leader to

transfer operational nuclear weapons to an independent non-State actor – an extremely unlikely scenario, but one where deterrence can play in a fairly straightforward way, in particular in rare situations where nuclear forensics databases allow for near-perfect attribution (e. g. North Korean plutonium).[12] At the other extreme, there is the scenario where a government had absolutely no idea that a group was building a nuclear weapon on its territory. In between, there are various scenarios of failing States where government actors or terrorist groups have access to weapons or fissile materials. There is no silver bullet to cover all these scenarios, and deterrence may have to be tailored on a case-by-case basis. In the second case, for instance – as demonstrated in Michael Levi's work – it might be counterproductive (e.g., prevent bilateral cooperation) to state that we would hold fully accountable a government which would have unknowingly and passively assisted a terrorist group. However, generic statements to the effect that we would expect good nuclear stewardship from any government having such weapons or materials may be useful.

Personal deterrence can be exercised at multiple points. Complex deterrence situations call for deterrence threats to be applied to a variety of actors, both on the "vertical axis" (along the chain of command) and the "horizontal axis" (to sponsors, facilitators and supporters).[13] This would help, in particular, dealing with situations where a leader or a group has an apocalyptic mindset – it is unlikely that all those surrounding them, or in charge of implementing their orders, would have the same extreme views. In the situation of a failing government, deterrence may have to be applied simultaneously to the State and to various non-State actors in the same country.

Think about deterring of a possible second (and third, etc.) use. A State or terrorist group foolish enough to use a nuclear weapon could still be deterred. If nuclear use has taken place, it would be a useful assumption to believe that a second one could too. Both immediate *and* general deterrence would need to be quickly restored: the former to avoid a second use by

---

[12] One possible caveat: the sale of North Korean technology abroad might make it more difficult to attribute with certainty a nuclear event to North Korea.

[13] For terrorists groups seeking to build a nuclear weapon, a "weak point" could be scientists and engineers: notwithstanding the existence of a few nuclear scientists with extreme views (the likes of the Pakistani maverick Sultan Bashiruddin Mahmood), there are probably very few experts in the world who would both have the capability and willingness to embark in such a project. Also, beyond existing national legislations (which have been made mandatory by UN Security Council Resolution 1540), leaders of private firms who may have sold to terrorist groups equipment or materials used in the making of a nuclear weapon need to be warned of the personal consequences they may suffer.

the same actor, and the latter to ensure that perceptions of the consequences of such an act do not heighten the probability of use by another actor. This would certainly be a time for stronger, more explicit punishment threats, at least to ensure that those who have chosen to break the nuclear taboo have not been encouraged by a misperception of our likely reaction. In sum, the prevention of nuclear use by unconventional and/or ideological actors could require "total deterrence" (the use of all possible available means) and "extreme deterrence" (breaking some of the taboos we rightly hold regarding certain military or societal practices). In most scenarios, the "software" part of deterrence – including intelligence, knowledge of specific cultures, psychology and communication skills – will be much more important than the "hardware" part.

APPENDIX: THE CASE OF IRAN

There is obviously no simple answer to the question "could we deter Iran from using nuclear weapons and if yes, how?" But a few ideas can be proposed.

There is ample evidence that the Iranian regime is receptive to deterrence, and in particular understands the basic logic of deterrence through retaliation. The US-Iran military confrontations of the 1980s, the Iranian reaction to alleged US threats after the 1996 Khobar Towers bombing, the 2003 decision to halt military-related nuclear activities, or the recurring bombastic statements from the Revolutionary Guards leadership about their reactions to an Israeli strike all point in one direction: the current regime understands the logic of deterrence through the threat of retaliation.[14]

The probability that deterrence works with Iran depends heavily on the dominant beliefs of the leadership at one given time. In situations where the prudent/pragmatic mindset that has dominated much of the past thirty-year history prevails, deterrence would have a good chance of working. In situations where the messianic/apocalyptic mindset that is common to the current President and much of his entourage prevails, deterrence would be much more difficult to achieve.

The *modus operandi* of deterrence would be dependent on the exact domestic situation prevailing in Iran. One can imagine at least four distinct scenarios: one where the Supreme Leader has unchallenged personal authority over the use of nuclear weapons; a second where the regime has become much more collegial; a third where clerical authority has collapsed and nuclear weapons are entirely in the hands of the Revolutionary Guards; a fourth where the country has become a failing State and where it is unclear where the weapons are and who would have the legal and physical ability to fire them.

In practical terms, deterrence options would vary from one situation to another: targets may be military sites or key religious shrines; actors to be deterred may include religious or military leaders; actors whose support would be sought to avoid nuclear use may include

---

[14] Famous comments by Ali Akhbar Hashemi Rafsanjani about the nuclear balance of power between Israel and the Muslim world and possible consequences of a bilateral nuclear exchange even show an understanding of the concept of "deterrence of the weak by the strong". Rafsanjani's point was to claim that it would not work – because the Muslim world is much bigger than the State of Israel.

moderate clerics, low-level Revolutionary Guards officers, or key civil society actors such as the Bazaar.

A CRUDE DETERRENCE MATRIX

	State-specific	*Common to both*	Group-specific
ssuasion	-Develop attribution capabilities	*-Develop propaganda towards supporters*	-Develop domestic propagan -Enhance threat reduction -Develop border security
erdiction	-Develop missile defense	*-Develop civil defense, force protection,* *consequence management*	
taliation	-Threaten centers of power	*-Threaten leaders and their families, inner* *circle, facilitators, executants* *-Threaten symbolic sites*	-Threaten bases, training cam -Threaten scientists, engineer private firms

Deterring Non-State Actors

Typical views about deterrence and terrorist non-state actors (NSAs) are that such actors cannot be deterred because they are irrational and have no territory or state-based assets to be held at risk. It is possible to test these common views by examining past conflicts between states and terrorist NSAs—the latter having posed security challenges to states for centuries. Access to WMD has increased the potential lethality of NSAs, but past case studies may nevertheless provide insight into the questions of if and how NSAs might be deterred.

There are numerous pertinent case studies to help gain this insight. A review of a select set of ten cases provides several tentative lessons concerning possible deterrence strategies. The cases listed below span roughly 200 years, range in duration from less than a year to over two decades, cover many regions of the world, and include a variety of different cultural issues and contextual factors.

These ten case studies are:

- *The United States and Barbary Piracy: 17831805*
- *Pancho Villa and the Punitive Expedition: 19161923*
- *The AngloIrish War: 19191921*
- *British Deterrence and Coercion in Mesopotamia: 19191932*
- *Urban Terrorist Groups in Continental Europe: 1970s1980s*
- *Soviet Reponses to Terror Attacks at the Time of Civil War in Lebanon: September-October 1985*
- *Deterring Non-State Terrorist Groups—The Case of Hizballah: 19852006*
- *Aum Shinrikyo Case Study: 19891995*
- *Deterring Non-State Terrorist Groups—Palestinian Groups—Fatah and Hamas:*
- *2000-2006*
- *Russian Responses to Terrorism: The Chechen War: 1994-2006.*

A survey of these cases suggests that in some past cases terrorist NSAs have indeed been deterred. In general, states learned through trial and error to combine threats of punishment, denial of objectives, and sometimes inducements to deter NSA leaders. It should be noted that deterrence was seldom the initial explicit goal of states. Rather, the initial state goal typically was to defeat or eliminate the NSA. Successful strategies of deterrence tended to evolve over time from strategies to defeat or eliminate the NSA.

One of the lessons learned from these cases is that the characteristics of an NSA can affect the potential feasibility of deterrence. Four characteristics of particular significance emerge:

- **Organizational Arrangements (centralized or decentralized).** These distinctions play an important role in the ability of a state to apply pressure to the appropriate nodes of power with the hopes of deterring or coercing.

- **Operational Area (Internal: on territory of state, External: adjacent, External: separated).** These factors can affect the avenues through which intelligence may be gathered and deterrence and coercion strategies put into practice.

- **Host and Patron States (single or multiple decision-makers).** There may be multiple decision-makers to be deterred with diverse motivations. The roles of patron and host states are very important when identifying and evaluating the key decision-makers behind the behavior of an NSA, when identifying the types of threats that may provide greatest leverage, and when identifying the channels of communication that may best display those threats.

- **Motives.** The motives that animate NSA actions and decision-making vary greatly. Different motives can allow different possibilities for the type of calculated tactical retreat, compromise or conciliation necessary for deterrence to function predictably. Understanding the motives behind NSA decision-making and actions can be key to

understanding the feasibility of strategies of deterrence. In the case studies listed, NSAs were motivated by a combination of factors:

- o Economic gain
- o Influence/Prestige
- o Separatism
- o Opposition to Occupation
- o New Order
- o Political Power
- o Religion

- **NSA Methods**

  In addition to the characteristics of NSAs, the methods of the NSA are important to understand if a state wishes to deter its leaders (including host state and patrons, if applicable). The NSAs in the case studies employed a spectrum of hostile actions against state opponents to achieve their goals. These methods included: attacks on civilians within, and external to, the state; attacks on commerce; attacks on military forces; attacks on state leaders; and kidnappings or hijackings. In almost all of the cases, the NSAs engaged in various kinds of attacks on civilians or state leaders.

  The methods used by each NSA, in turn, affected the types of methods the state could consider to deter the NSA in question. In particular, it appears important to understand NSA methods to identify how best to defend, disrupt and deny NSA goals—measures that often proved important for the goal of deterrence. Methods used by an NSA also will likely influence how willing a state will be to pursue deterrence and how it will do so, or, in contrast, if the state will instead be compelled to destroy and eliminate the group.

Methods Used by States Against Non-State Actors

The cases illustrate a wide variety of methods used by states to defeat, deter, or coerce NSAs. These methods overlap, but can be grouped into three broad categories: threatened punishment, denial of goals, and inducements. Threatened punishment and denial are traditional

elements of a deterrence or coercion strategy. Inducements, while not a tool of deterrence or coercion, have been used in combination with deterrence and coercion measures to influence NSA decisions and behavior. Preventing hostile action by an NSA may not be simply a matter of deterrence by threat of punishment. For most of the cases examined, when deterrence was achieved denial methods played a significant role. And, inducements on occasion appear to have contributed positively to efforts to shape NSA behavior.

Threatened Punishment. Threatened punishment typically is intended to link the prospect of cost to a particular type of aggression to try to influence the NSA's decision-making. Punitive threats have included: direct threats to NSAs and their leaders; threats to patron or host states; and threats to family members or others that NSA leaders might value. States also threatened or periodically demonstrated an ability to damage assets (such as infrastructure, bridges, power plants, etc.) in order to put pressure on NSA leaders. While the case studies demonstrate that punitive deterrent threats are available to states willing to use them and that such direct pressure on NSA leaders and/or indirect pressure on patrons can be effective, these measures alone have had mixed success of limited duration. The case studies provide ample evidence of the added value of denial measures, used in combination with punitive threats, to more effectively deter and coerce.

Denial. To deny an adversary its goals—whether the goals are political, territorial, material, or other—has been a longstanding element of U.S. deterrent strategy against states. Measures taken by states to deny an NSA its objectives have included defensive measures, antiterrorist laws, establishment of specialized response capabilities to counter NSA tactics (e.g., commando units for hostage rescue), military operations to disrupt NSA activities, eliminating sanctuaries and refusal to negotiate with NSAs. Memoirs by incarcerated European terrorists of the 1970s often point to the deterring effect of policing actions intended to capture or kill terrorists. Typically, states sought to eliminate the threat by extirpating the NSA. The goal of eliminating the threat by decisively defeating non-state adversaries, however, typically proved difficult, particularly in the near-term.

Inducements. In the majority of these case studies, states combined some form of inducement with punitive and denial deterrence measures to encourage the desired change of behavior by the NSA. The effectiveness of inducements for this purpose appears to have been dependent upon the NSAs' motives, goals, and related willingness to accept tactical retreat or strategic conciliation. It may seem intuitive, based on the extreme goals of many NSAs and the corresponding goal of states, that the states in the case studies were not eager to offer concessions or inducements to NSAs. However, in multiple cases, inducements or concessions to NSAs appear to have had some value *when used in combination with deterrent or coercive threats*. This combination was employed by states to reach an accommodation with the NSA leaders, to encourage defections from NSA ranks, or to undermine the NSA's base of support. Another form of inducement is amnesty for "reformed" or "penitent" NSA members. Amnesty, selectively used, appears to have undermined support for the NSA, either from the cadres or its popular base. However, the case studies also included examples in which inducements, offered as straightforward compliance with NSA demands, *were unproductive or counterproductive*.

States, where successful, tended to find a workable combination of deterrence and inducement strategies following a long and painful learning process. They learned by experience how to structure a deterrence strategy for the specific NSA and context they confronted, and to combine it with inducements to achieve the desired deterrent effect. The cases provide examples of states devising strategies roughly suited to specific characteristics of the context, cultures, motivations, and decision-making relationships for each NSA.

Leverage Through Threats to Third Parties

To be effective, threatened punishment may need to be directed at NSA patron or host states. The existence of patrons, hosts, or a social network does not imply that this form of indirect deterrence will be effective. However, in cases in which the NSA receives ample support from a patron and its decision-making is influenced significantly by that patron, pressure on the third party leadership is likely to be needed for an effective deterrence strategy.

Intelligence to Inform a Deterrence or Coercion Strategy

The cases demonstrate the importance of a comprehensive understanding of the NSA—its key leaders, leadership structure, culture, motives, goals, sponsors and definition of cost. An understanding of these matters can improve the chances of crafting an effective strategy for deterrence. Generic threats communicated indiscriminately may deter, but these cases suggest that a strategy informed by an understanding of the target and context will have a greater chance being effective.

The Record of Deterrence and Coercion in the Case Studies

Examination of these cases suggests that the common notion that terrorists cannot be deterred is mistaken. On occasion, deterrence and coercion can be effective against NSAs. Perhaps the most accurate description is that some NSAs can be coerced and deterred at least some of the time. The case studies also provide evidence that states in conflict with NSAs can also be vulnerable to deterrence and coercion by the NSAs. This vulnerability can limit the state's deterrence strategy options. This linkage can be important: the better defended are states against NSAs, the greater is their freedom to pursue deterrence strategies.

The types of circumstances in which coercion or deterrence is more likely to be effective typically include the following factors:

- Central leadership and control of NSA and its operations.
- Lack of third-party support or control that significantly influences the behavior of the non-state actor.
- NSA operates in territory accessible by the state (no sanctuary for NSA operatives).
- NSA motives and goals that are not immediate and absolute—there is some "room" for tactical retreat or compromise (however labeled).[15]

---

[15] See the discussion of this point in, Keith B. Payne, *The Great American Gamble: Deterrence Theory and Practice From the Cold War to the Twenty-First Century* (Fairfax, VA: National Institute Press, 2008). Pp.340-346.

Additional Observations on the Deterrence of Non-State Actors

Deterrence as a Goal or as a Concomitant Effect

The Cold War experience has conditioned many to think of deterrence as the priority strategy or objective. An observation from these cases is that deterring NSAs often is not the initial or primary aim of states; deterrence, however, can be a byproduct of state efforts to defend against and eliminate the NSA threat.

The observation that deterrent and coercive leverage may be the result of actions taken for other reasons (e.g., to defeat the NSA opponent or defend against the NSA threat) is noteworthy. It suggests that states may find important advantage in being opportunistic—observant enough to see the potential for these byproducts and flexible enough to take advantage of them when possible.

Deterrence May Be Limited in Time and Scope

The long duration of some of the case studies involving NSAs provides some empirical evidence that deterrent effect can be achieved over time but, once achieved, may be difficult to sustain. Its effectiveness may be limited in time and scope by the unique characteristics of the NSA and the immediate circumstances. There will be cases where deterrent options indeed are inapplicable or infeasible.

Deterrence is Unpredictable

The case studies indicate that deterrence is unpredictable and thus unreliable as an *exclusive* means of dealing with NSA threats. The threats that work in some cases are only adjuncts to a broader approach in others, and may fail either in availability or effectiveness in still other cases. In many cases, the utility of deterrence and coercion is determined by how well a state is able to learn about and adapt to its NSA adversary as NSA leaders revise their tactics in response to measures used by the state.

Contextual Factors and Deterrence

Finally, the broader contextual factors surrounding conflicts between a state and an NSA typically include key variables that help shape how the states and NSAs operate. Consequently, claims about if and how deterrence will function may be limited to the unique contexts within which those claims were pertinent.

Summary

Some practical advice can be suggested for officials charged with understanding today's NSAs and deterring their activities. This set of insights, rules of thumb, and cautions may have particular merit because it derives not from a priori presumptions, deductive logic, mirror-imaging, an abstract model, or even from knowledge hard won in battling a single non-state enemy. It follows from broad, real-world experience involving a variety of NSAs, third parties, geographic settings, historical periods, security challenges, strategies, tactics and tools (of both states and their non-state enemies), and conflict outcomes.

Instead of a universal approach to deterrence requirements such as Secretary of Defense McNamara's "assured destruction" Cold War template, these cases indicate the following:

- *There is no single formula for deterring or coercing nonstate actors.*
- *Attempts to deter or coerce NSAs can draw on an array of possible methods and means.*
- *Denying geographic sanctuaries to NSAs can be key to bringing punitive or*
- *denial pressures to bear on the leaderships.*
- *Deterrence of NSAs may be a multilateral matter*
- *Deterrence of NSAs should not be considered in isolation from broader*
- *efforts to counter such groups; deterrence may be the concomitant effect of those efforts and apparent only over time.*
- *Accurate intelligence enables–but does not guarantee–the deterrence or*

- *coercion of nonstate actors.*

- *Domestic constraints may affect, though not necessarily in a determinative*

- *way, the strategies, tactics, and means available for deterring or coercing*

- *nonstate actors.*