2007

The Limits of Intelligence in Maritime Counterproliferation Operations

Craig Allen
University of Washington School of Law

THE LIMITS OF INTELLIGENCE IN MARITIME COUNTERPROLIFERATION OPERATIONS

Craig H. Allen

It might come as a surprise to many of those immersed in the current debate over how best to guard against the further proliferation of weapons of mass destruction (WMD) that the alarm over the "growing number of nations in positions to acquire mass annihilation weapons" and the potentially synergistic threat of state-sponsored terrorism was sounded at least two decades ago, in Reagan-era naval maritime strategy documents authored by Admiral James Watkins.[1] Naval forces have long been at the vanguard of global counterproliferation efforts. Nearly a half-century ago, the Navy was tasked with establishing and enforcing a "quarantine" to intercept Soviet nuclear missile shipments to Cuba. In the intervening years, the maritime components of combined and joint force commands, along with the U.S. Coast Guard elements of the National Fleet, have frequently been called upon to stem the flow of contraband by sea. The debt owed by the naval forces to the intelligence community for the success of those operations is well documented.[2] All would likely agree, however, that the magnitude of the threat posed by WMD proliferation demands that the entire spectrum of counterproliferation measures and supporting intelligence activities be subject to continuous scrutiny, with a view to improving the accuracy and speed of the processes.

In 2003, President George W. Bush launched the Proliferation Security Initiative (PSI) to counter the proliferation of WMD and their delivery systems and thus prevent them from falling into the hands of rogue regimes and terrorist organizations. The PSI has been described as a political commitment, not a new legal obligation or international organization.[3] Although it came under criticism in its first year, by the time of the third anniversary meeting in Krakow

Professor Allen, of the University of Washington School of Law (where he is Judson Falknor Professor of Law), is the Charles H. Stockton Chair in International Law at the Naval War College for 2006–2007. He served in the Marine Corps from 1969 to 1971 and retired from the Coast Guard in 1994.

Naval War College Review, Winter 2007, Vol. 60, No. 1

in 2006 sixty-six states had signaled their support for the PSI;[4] the Russian Federation had joined the original group of core participants; the participating states had adopted a Statement of Interdiction Principles;[5] and six flag states had entered into treaties to facilitate PSI boardings of their vessels.[6] In 2004, the United Nations Security Council added to the legitimacy of the fledgling PSI approach by acknowledging the threat to international peace and security posed by WMD proliferation and underscoring the need for states to prohibit illicit proliferation and to cooperate in measures to enforce those prohibitions.[7] Multilateral cooperation and coordination measures like the PSI provide a flexible, responsive, non-treaty-based approach to achieving the Security Council mandate for cooperation.

The long-term practical and political success of a counterproliferation initiative like the PSI will be determined in large measure by the availability of timely and accurate intelligence to the decision makers and their field operators. "Practical" success will turn on the extent to which, through inducement, deterrence, prevention, and interdiction, the production or transfer of weapons of mass destruction and their related materials and delivery systems from producer to the aspiring user is thwarted. Because the PSI, like the more recently launched global maritime partnership concept, is indeed a "political" commitment and not a legally binding international obligation, actual and perceived legitimacy will be crucial to its long-term viability. Legitimacy will be enhanced if operations are grounded in accurate intelligence, interference with navigation rights is minimized, the use of force is strictly limited to that which is necessary and reasonable, and the interdicting states demonstrate their willingness to compensate those who suffer losses as a result of PSI interdictions that later prove unfounded. Intrusive interdictions based on intelligence that ultimately proves faulty will tend to erode public confidence in the program and may shake the resolve of other PSI participating states. Unjustified counterproliferation operations might also undermine the already fragile nonproliferation regime. It is readily apparent that the information demands of counterproliferation forces will present a daunting challenge for the intelligence community.

This article begins with an examination of the intelligence needs of those engaged in maritime counterproliferation efforts. It then turns to risk-management decision making under conditions of uncertainty, focusing on decisions at the operational level and exploring the question of whether decision strategies in the WMD context should seek to minimize false-negative or false-positive errors. It concludes that even vastly improved maritime intelligence will not obviate the need for national and operational commanders to make decisions under conditions of uncertainty and that such decisions should be made on the basis of established risk-assessment and management principles. At the same time,

risk management analysis must be sensitive to the public's attitude toward risk. When possession of WMD is at stake, sound risk management that gives appropriate weight to the public's preferences might well call for action even where the relevant event probabilities are quite low.

INTELLIGENCE DEMANDS OF MARITIME COUNTERPROLIFERATION OPERATIONS

Maritime counterproliferation operations are but one component of the global and national WMD proliferation risk management strategy. Like all risk management strategies, the WMD strategy process begins with a risk assessment.[8] Where possession or use of weapons of mass destruction is at risk, estimates must look beyond mere event probabilities; they must fairly weigh the extraordinary magnitude of the risks. It is often said that the detonation or release of a weapon of mass destruction, particularly a nuclear device, is a low-probability event—even an extremely low probability event—but one with destructive potential so enormous that it presents what most consider to be an unacceptable risk.[9] To this observation risk management analysts often add the warning that in responding to WMD risks, managers must be successful in their risk management measures every time, while the malefactors who would unleash such weapons need be successful only once.[10]

The U.S. *National Strategy to Combat Weapons of Mass Destruction* establishes among its highest intelligence priorities "a more accurate and complete understanding of the full range of WMD threats."[11] It emphasizes that intelligence will be crucial in developing effective counterproliferation policies and capabilities and in deterring and defending against known proliferators and terrorist organizations.[12] The president's directive on maritime security policy similarly emphasizes the importance of a "robust and coordinated intelligence effort [that] serves as the foundation for effective security efforts in the maritime domain."[13] It was in response to this directive that a number of integrated maritime security planning documents, including the *National Strategy for Maritime Security* and the *National Plan for Achieving Maritime Domain Awareness,* were produced. To meet more effectively the urgent demand for maritime domain intelligence integration and distribution, the president further tasked the involved agencies to prepare the document that became the *Plan for Global Maritime Intelligence Integration* (or GMII Plan).[14] The closely related *Maritime Operational Threat Response Plan* (MOTR Plan) provides the framework for coordinated, unified, timely, and effective response planning and operational command and control of maritime security incidents.[15]

Decades of experience in narcotics interdiction and the testimony of thousands of boarding officers witness the inestimable value of intelligence to

maritime interception operations.[16] The forces available for maritime counterproliferation operations are finite, not nearly adequate to cover the world's oceans or to board even a fraction of the vessels operating on those oceans. Moreover, the dangers and practical difficulties demand that at-sea boardings and searches be relied upon only when warranted by the circumstances. Finally, the president has made it clear that maritime interception and enforcement should be conducted in a manner that does not *unnecessarily* interfere with maritime commerce or the freedom of navigation. Better intelligence reduces the potential for unwarranted interference with those vital interests.

The intelligence community, including any organic components of the operating forces involved, provides (in the language of the well known "OODA loop") the "observe" and "orient" bases by which those charged with control over operations are to "decide" and "act."[17] The intelligence demands of counterproliferation decision makers and operators will likely differ in several respects from those of their nonproliferation counterparts. Not least among the differences will be the timeliness demands of a forward-leaning counterproliferation strategy that envisions interdicting WMD shipments during transit. The nonproliferation program relies chiefly on relatively long-term, strategic intelligence; by contrast, counterproliferation operations demand timely indications and warnings intelligence for each component in a layered defense scheme. The inverse relationship between certainty and speed is readily apparent: any additional time allocated to the observe and orient phases comes at the expense of the time remaining to decide and act. Not everyone agrees with how the time available should be allocated. Those charged with tactical thinking tend to emphasize speed of decision making ("faster is better"), while those entrusted with strategy are more inclined to prefer accuracy ("smarter is better").

Losses that could result from a false negative might well be incalculable.

Multilateral activities introduce an additional consideration. Multilateral decision processes virtually always take longer to develop, and they generally raise the intelligence bar, because the level of certainty for multilateral actions must meet the standard set by the most demanding participant. Interagency consultation processes like the scheme established by the MOTR Plan may have the same effect. Additionally, if the intercepting forces must first obtain the consent of the vessel's flag state or a coastal state, that government's information requirements must be met, even if disclosure might compromise intelligence sources or methods. The flag state will likely demand more information and greater certainty where the vessel must be diverted to accomplish the boarding or when force might be necessary to compel compliance.

Intelligence in support of counterproliferation must be adequate to answer the most pressing questions that maritime interception forces will pose regarding shipments of WMD and related materials.[18] The intelligence challenge will often begin with the "What?" question.[19] It is improbable (but nonetheless possible) that proliferators would attempt to transport an assembled and operational WMD device via commercial seagoing vessels. It is more probable that maritime shipments would consist of components, precursors, or small quantities of fissile or radiological materials. In some cases those materials would be dual-use in nature, presenting additional challenges for analysts and operators, who might not be familiar with the characteristics and applications of the materials or equipment.[20]

The second challenge will be to provide answers to the "Who?" question: Who are the parties to the suspected WMD transfer and transport transaction? It is necessary to know the identities of the consignor, consignee, and the owner and flag of the vessel, in order to assess the risk and determine which states might have jurisdiction over the vessel and whose consent or cooperation would therefore facilitate interdiction. Closely related to "Who?" is the question of the actors' intent: Why are they seeking the materials or equipment? Intent—which, unlike "Who?" and What?," always requires analysis—is critical where dual-use materials or equipment are involved. Whether a given shipment is illicit and a candidate for interdiction may turn on the identity of the end user and the nature of the intended end use. Analysts and commanders evaluating possible courses of action and the urgency of the need for action understand that the risk posed by the availability of WMD is in part determined by the willingness of the entity in possession to deploy the weapon.

The next questions the commander is likely to ask in forming an estimate of the situation and choosing a course of action concern time and space factors: Where and when will the illicit WMD likely be transported, and, perhaps, how will it be carried out? Interdictions at sea can present significant legal and practical problems. The intelligence community must be prepared to provide, if possible, accurate information on both the location of the ship and the illicit materials onboard. The "When?" question should produce an assessment of the last practicable opportunity to prevent the delivery of WMD materials to the state or nonstate actor of proliferation concern. For a variety of reasons, dockside inspections are preferable to at-sea boardings. Maritime interception forces in receipt of information that a ship under charter to a well known commercial carrier is believed to have ten drums of chemical warfare component materials in one or more of five thousand containers will likely explore alternatives to boarding at sea, perhaps raising the always contentious question of whether the intelligence is sufficiently reliable to justify diverting the vessel to a port.

Decision makers and operators will also want to know who else might be involved in the transaction. Interdicting a shipment is only one element of the larger counterproliferation strategy. The emergence of proliferation networks, such as the lucrative multinational enterprise operated out of Pakistan by A. Q. Kahn, amply demonstrates that nonstate actors now participate as both suppliers and consumers of WMD technology.[21] Those global networks must be identified and interdicted as well. The networks' financial assets must also be located and frozen or seized. Finally, decision makers will want to know the degree of confidence in the intelligence assessment. In many cases, it will be based on analysts' subjective judgment of probability. In contrast to objective probabilities—derived, for instance, from accurate and reliable sources like mortality tables—subjective probabilities involve events the likelihood of which can only be estimated, based in part on the judgment and experience of the analyst. (For example, President John F. Kennedy is said to have estimated the probability of war with the Soviet Union during the Cuban missile crisis as one in three.) Because such judgments are influenced by a variety of factors and are subject to cognitive errors, they are likely to differ from one person to another.[22] Candid evaluations that are clear about the bases of the probability assessment, any ambiguities in the evidence relied on, the degree of uncertainty, and whether competing theories or dissenting views exist are indispensable to decision makers, who must evaluate the assessment (and the assessors), weigh the respective event probabilities, and project the potential consequences of an erroneous decision.

RISK ASSESSMENT WHEN POSSESSION OF WMD IS AT STAKE

> *Since we recognize the limits of combating WMD intelligence, planning and execution decisions will be made using limited or incomplete information.*
>
> CHAIRMAN, JOINT CHIEFS OF STAFF (2006)

The chairman's statement reminds us that limited or incomplete intelligence regarding a WMD threat does not obviate planning and execution decisions.[23] The geostrategic environment of the twenty-first century is frequently described as one fraught with uncertainty and subject to rapid and sometimes radical change. If one defines certainty as precluding any possibility of subsequent challenge in light of additional or more accurate observations or more comprehensive reasoning, uncertainty seems inevitable in the maritime counterproliferation operating environment.

Although we must accept that national security decisions must on occasion be made on the basis of incomplete or uncertain information, we may nevertheless expect them to be tempered with practical wisdom and mature judgment.

Even so, we must admit that time for making decisions is not unlimited. The commander must be prepared to complete the observation-to-action decision loop before the adversary can deliver or acquire that weapon of mass destruction. The greater certainty accruing from multiple corroborating sources may increase confidence but also impose delays the commander cannot afford.

It is important to bear in mind also that even "correct" decisions do not ineluctably produce desired outcomes. Whether a decision was correct must be judged by the quality and quantity of information reasonably available at the time it was made, not by that which was only revealed later.[24] The goal, of course, is to timely reach the correct conclusion despite any information deficit; however, the possibility of error can rarely be eliminated altogether.

Under international law and the PSI Statement of Interdiction Principles, boardings must generally be predicated on some level of suspicion of illicit activity, described by such vague formulae as a "reasonable ground" to suspect or "good cause" to believe that the vessel is engaged in the illicit activity.[25] Under U.S. law, the standard for arrest or seizure is typically "probable cause" to believe a crime has occurred. It is noteworthy that none of these measures require for field action anything approaching certainty "beyond a reasonable doubt." The practical reasons are apparent. A requirement for prior certainty that a vessel is engaged in piracy sets the bar impossibly high, permitting the vessel to operate without fear of interdiction so long as it hides the evidence reasonably well. Moreover, the degree of intrusion represented by a boarding is far less than that of seizure or arrest. The information that warrants visit or boarding might also be necessary to persuade the vessel's flag state or a coastal state through whose waters it will pass to authorize yet another state, which is willing and able to board, search, and perhaps seize the vessel, to do so. That second state is, of course, free to set its own standard for information reliability, either by treaty or ad hoc agreement.

The Value of "Good" Intelligence

The intelligence community's predilection for modest silence is well known. With few exceptions, intelligence agencies are not given to self-promoting publicity following intelligence "successes." The transparency that is otherwise the hallmark of constitutional democracies is antithetical to the long-term success of the intelligence community. It should come as no surprise, therefore, that states participating in the PSI, knowing that illicit proliferators would take advantage of such announcements to probe for weaknesses, have given notice that they may never reveal many of their interdiction activities.[26] Unfortunately, denying proliferators and transporters such an opportunity means that the public

and nonparticipating states will often have no direct means of learning of the program's accomplishments.[27]

There is no shortage of books, articles, and congressional or commission reports documenting actual or perceived intelligence "failures."[28] Almost none salute the intelligence community's many successes. Modern critics might offer a brief tip of the hat to the courage and resourcefulness of the Office of Strategic Services operatives and code breakers in World War II, and perhaps to the U-2 pilots who risked (and, in one case, lost) their lives obtaining the photo images of the Soviet missile sites in Cuba that Ambassador Adlai Stevenson displayed so effectively to the Security Council, but then they tend to focus their attention quickly on the failures. Accordingly, it is fitting to acknowledge briefly two recent intelligence success stories involving maritime counterproliferation operations. The first involved the interdiction of the North Korean cargo vessel *So San*.

Spanish marines were forced to fast-rope onto deck of *So San* when it refused to comply with boarding requests.

U.S. Navy, released by Spanish Defense Ministry

In late 2002, American intelligence agencies had good reason to believe that a vessel later identified as the *So San* was transporting missiles from North Korea. They were uncertain, however, of the cargo's destination. The U.S. Navy eventually requested that a Spanish warship intercept the vessel and board it on the high seas off the coast of Yemen. A team of Spanish marines from the frigate *Navarra,* later joined by U.S. Navy personnel, conducted a noncompliant boarding of the *So San* and during the subsequent search discovered North Korean–made Scud missiles and components hidden beneath the cargo of bagged cement. Not surprisingly,

The boarding team discovered fifteen disassembled Scud missiles concealed under tons of bagged cement.

U.S. Navy, released by Spanish Defense Ministry

the missiles were not listed in the vessel's manifest. Although the ship and cargo were eventually released at the request of the government of Yemen, to which it was learned that the missiles were being shipped, the interdiction demonstrated the capability of the intelligence community to detect and track maritime WMD shipments over considerable distances. Much of the information on the *So San* interdiction remains classified; however, publicly available accounts suggest that intelligence assets detected the missiles being loaded in North Korea and tracked the vessel from there to the interception point.[29] Apparently, however, the intelligence community was unable to determine the buyer's identity before the boarding.[30]

The second incident involved the multilateral interdiction of the German-flag *BBC China* in October 2003. American and British intelligence agencies concluded that the *BBC China* was transporting component parts for uranium enrichment centrifuges from Dubai to Libya. Demonstrating the kind of cooperation the PSI was designed to foster, Germany agreed to order the vessel to divert to a port in Italy for inspection. The vessel's owner and master readily complied with the flag state's order. Italy then agreed to allow the vessel to enter one of its ports and to conduct the search. The intelligence proved accurate, leading to the discovery of thousands of parts for gas centrifuges of a kind that can be used to enrich uranium. Some suggest that the *BBC China* interdiction contributed to Libya's decision in late 2003 to abandon its WMD program.

Intelligence, Inferential Errors, and Risk Management Decisions

The fulcrum of the debate over intelligence and WMD counterproliferation in the coming years will likely be the relationship between the tolerance for risk and error, on the one hand, and our willingness to bear the financial, societal, and political costs of incremental security measures, on the other.[31] As President

Bush remarked in response to the report of the 9/11 Commission, "There is no such thing as perfect security in our vast, free Nation."[32] Nor do security decision makers often have the luxury of waiting for complete and perfect information, or for intelligence that provides the kind of assurance Israelis have described (in the *Karine A* war materiel interdiction) as "unequivocal, clear, and undeniable."[33] The goal therefore cannot be perfect security but rather optimal security, and optimal security decisions will inevitably be based not on perfect knowledge but on optimal intelligence assessments.[34]

On occasion, the assessments made by the intelligence community will later prove to be wrong. Error may result from information that is incomplete, conflicting, or susceptible to more than one plausible interpretation or inference. To simplify the analysis in this counterproliferation setting it will be helpful to posit that the "wrong" inference or conclusion might take one of two hypothetical forms. In the first, a ship that intelligence analysts have concluded is transporting WMD components is intercepted and boarded at sea; an exhaustive, day-long search reveals that the intelligence assessment was wrong and the vessel's cargo is entirely legitimate.[35] In the second, a ship that is in fact transporting a WMD to a densely populated port city is not boarded because the decision maker concludes that there is insufficient evidence. Surveillance of the vessel is later lost when it enters a crowded traffic lane, and the weapon is delivered and later detonated in the city. Those charged with responsibility for the decision in the OODA cycle must be prepared to determine which of the two erroneous outcomes poses the more serious risk (just as the criminal justice system did by adopting a "beyond a reasonable doubt" standard to minimize the chance of wrongly convicting a person of a crime). A false positive in a counterproliferation operation may require the interdicting state to issue an apology and provide appropriate compensation to the vessel inconvenienced. Losses that could result from a false negative might well be incalculable. As the U.S. *National Security Strategy* declares:

[Risk] managers must be successful . . . every time, while the malefactors who would unleash [WMD] need be successful only once.

> The greater the threat, the greater is the risk of inaction—and the more compelling the case for taking anticipatory action to defend ourselves, even if uncertainty remains as to the time and place of the enemy's attack. To forestall or prevent such hostile attacks by our adversaries, the United States will, if necessary, act preemptively.[36]

The False Positive Error. Statistical decision theory recognizes two types of inferential error. The false positive, or *Type I,* error refers to a conclusion that a condition exists or a proposition is true when in fact the condition does not exist

or the proposition is not true. Prewar intelligence estimates of Iraq's WMD, characterized on one occasion as a "slam dunk," present a recent and notorious example of such a "false positive" error, as was the less well publicized four-day boarding of the container ship *Palermo Senator* in 2003.[37]

A 1993 incident involving the Chinese containership *Yin He* and the 1998 cruise missile strike on a Sudanese chemical plant in Al Shifa are cited as examples of the kind of international embarrassment the United States can expect to suffer by taking action based on a false-positive intelligence assessment.[38] The United States alleged that the *Yin He* was carrying chemical precursors that could be used to produce mustard and sarin nerve gases from China to Iran.[39] Secretary of State Warren Christopher publicly asserted that the intelligence on the *Yin He* was reliable. In fact, an American intelligence official went so far as to declare, "We know these chemicals are bound for Iran's chemical weapons plants, and it is a lot of tonnage, tens of tons."[40] China vehemently disputed the U.S. allegation, but it eventually agreed to a boarding of the vessel in a Saudi Arabian port. The inspection by Saudi officials, accompanied by American technical advisers, uncovered no trace of the precursors American intelligence officials had alleged were aboard. Beijing blasted the United States for acting like a "self-styled world cop."[41] Nevertheless, the United States refused to offer either an apology or compensation for the vessel's delay;[42] Washington asserted that it had "had sufficient credible evidence that those items were in the cargo."[43]

In the latter incident, the United States struck the Al Shifa plant in the belief, based on intelligence, that the plant was engaged in producing chemical warfare agents. Poststrike investigations revealed that the assessment was almost certainly wrong.

At most, decision makers who rely on a false positive assessment may be accused of being rash or alarmist and may be required to issue apologies or compensate the owner of a vessel or cargo. However, frequent or egregious actions taken on the basis of erroneous intelligence will eventually undermine public and partner-states' confidence in the program.[44] False positive errors can also demoralize members of the intelligence community and may cause them (and operational commanders) to be more cautious, more guarded, and less willing to pass on preliminary or tentative findings in the future.[45] Ironically, such wariness might lead to errors of the opposite kind, demonstrating the interdependence of errors caused by too much and too little caution. Finally, false positives, like false negatives, can educate would-be proliferators and transporters on the tactics and methods employed by counterproliferation forces, providing them with information useful in circumventing the regime's strengths and exploiting its weaknesses.

The False Negative Error. The false negative, or *Type II,* error is committed by concluding that a condition does not exist or that a proposition is not true when in fact the condition does exist or the proposition is true. For example, a provocative quarantine might be imposed around Cuba on the assumption that even if the situation escalates, Soviet troops on the island number only three thousand and that no nuclear weapons or missile delivery systems are available to them.[46] Or a hypothesis that a handful of Muslim extremists have enrolled in flying lessons in preparation for turning airliners into instruments of mass devastation might be erroneously dismissed as too far-fetched. At best, erroneous false negative decisions simply delay responsive action.[47] At worst, they may convince those with blind spots or a high tolerance for risk that it is safe to open the city's gates and wheel that massive wooden horse inside.

ACTING ON UNCERTAIN RISK ASSESSMENTS WHEN POSSESSION OF WMD IS AT STAKE

> *War is the realm of uncertainty; three-fourths of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. A sensitive and discriminating judgment is called for.*
>
> CARL VON CLAUSEWITZ, *ON WAR*

Risk assessments help us categorize and quantify a risk, but they do not tell us what, if anything, to do about it.[48] That second question falls in the domain of risk management, which nearly always entails a policy judgment. Decisional "purists" will ground their decision on objective risk-management principles.[49] The purist's approach evaluates the various alternative courses of action applying decisional criteria that include an alternative's predicted effectiveness in producing the desired result and the cost of achieving that result in that fashion. Those who define their decisional criteria more broadly will also consider the public's likely reaction to the decision. Where the decision is a binary one—between interdicting a vessel and taking no action, where a subjective probability assessment indicates a risk that it is transporting WMD—the latter group will factor in the public's attitude toward risk. Put another way, these analysts will ask how cautious the public expects its national and homeland-security leadership to be.

The nation's reaction to the 11 September 2001 attacks and to the 9/11 Commission hearings and report suggest that as a nation the United States is risk averse, preferring the embarrassment of an occasional false positive to the potential horrors of a false negative. To the extent they were willing to accept errors of any kind, the majority of Americans appeared to demand that the risk of "false negatives" be minimized, if not eliminated, when the threat is to the

homeland.[50] Some would characterize their preference as one akin to the "precautionary approach" advocated by many environmentalists, wherein lack of certainty regarding a risk does not excuse failure to take avoiding action.[51] Two critical considerations are less clear, however. The first concerns the cost the public is willing to bear for a true precautionary approach to homeland security. That cost includes not only the financial costs of an enhanced security system but also possible criticism from abroad and encroachments on civil liberties. The second concerns the chronic tendency toward short-term thinking, what some derisively refer to as "strategic attention deficit disorder," perhaps coupled with what cognitive psychologists call the "availability heuristic"—the tendency to make judgments about the future based not upon a broad body of historical evidence but on recent, vivid events that skew perceptions. The cautionary preferences manifested in late 2001 or when the 9/11 Commission first denounced a collective "failure of imagination" may not reflect preferences five or ten years after the traumatic event.

In assessing the public's attitude toward risk and the consequences of error we must also be mindful of the political and media reaction to the most significant false positive error in recent history—the prewar intelligence assessments of Iraq's WMD program.[52] Like the pre-9/11 risk assessment of the homeland's vulnerability to large-scale terrorist attacks, they may be reduced for analytic purposes to an intelligence judgment that presented decision makers with two possible "truths": either Iraq was engaged in a clandestine program to produce WMD or it had abandoned its earlier design and production activities and disposed of its stockpiles. In this light a rational decision maker following accepted risk management principles would have to consider, among other things, the respective consequences of a false positive and a false negative error.[53] As Philip Bobbitt, former strategic planning director of the National Security Council, has argued, judgments regarding the consequences of an erroneous decision might actually cause a decision maker to pursue a course of action that is *not* based on the state of affairs analysts have concluded is the most probable.[54] Under accepted risk management principles, if a scenario with a lesser, but still significant, probability presents an overall risk that the decision maker deems unacceptable (as measured by the magnitude of the expected harm, discounted by the event's probability), the "correct" course may be to abate or at least reduce that risk. Bobbitt further warns that in judging a decision we must avoid "Parmenides' fallacy," which occurs when one assesses the correctness of a decision based solely on the state of affairs it produced, without comparing that state

The information demands of counter-proliferation forces will present a daunting challenge for the intelligence community.

of affairs to the outcomes that would have been produced if one of the alternative courses of action had been chosen.[55] One need not delve deeply into notions of efficient or proximate cause to understand that any given end state is the product of a multitude of causes and factors, many of which are not under the control of the decision maker.

Those charged with making and acting on national security decisions regarding weapons of mass destruction should never accept less than the best available intelligence; nonetheless, they must also be prepared to make timely decisions when that intelligence falls short of certainty. Excoriating the intelligence community or decision makers for committing false-positive errors even though they followed appropriate risk assessment and management methods risks driving them in the future to accept a higher risk of false negatives or at least to be more reluctant to take action on probable but uncertain intelligence assessments. Such tendencies would undermine a precautionary approach. The long-term political success of counterproliferation operations requires that both intelligence analysts and operations decision makers be candid with regard to uncertainties. An intelligence agency that represents an assessment on weapons of mass destruction as a "slam dunk" will find its credibility seriously questioned. For the same reason, the cost of error should not fall on the innocent shipowner. States conducting maritime interception operations must be prepared to compensate for any loss or damage caused by operations that turn out to be unwarranted.

NOTES

1. Adm. James D. Watkins, "The Maritime Strategy," Naval Institute *Proceedings* (January 1986), pp. 2, 6. See also Elliott Hurwitz, "Terrorists and Chemical/Biological Weapons," *Naval War College Review* 35, no. 3 (May–June 1982), pp. 36–40.
2. In describing intelligence activities in support of the maritime interception forces enforcing the Iraq sanctions, the doctrinal publication *Naval Intelligence* records, "U.S. maritime intelligence activities provided a wealth of intelligence derived from international shipping registers, vessel sightings, electronic intelligence, cryptologic reporting, open sources, satellite imagery, human intelligence, and aerial reconnaissance photographs. This information was collated, analyzed, and fused into intelligence products that were provided to naval operating forces. Complementing this intelligence with information from organic radar, cryptologic sensors, and other surveillance assets, the maritime interdiction patrol force intercepted more than 10,000 ships by the spring of 1991. This enabled the Gulf War coalition to maintain, in the words of General H. Norman Schwarzkopf, a 'steel wall around the waters leading to Iraq' that helped hasten the defeat of the Iraqis on the battlefield" (U.S. Navy Dept., *Naval Intelligence,* NDP-2 [Washington, D.C.: 30 September 1994], chap. 2).
3. U.S. State Dept., *Proliferation Security Initiative,* available at www.state.gov/t/isn/c10390.htm; Andrew C. Winner, "The Proliferation

Security Initiative: The New Face of Interdiction," *Washington Quarterly* 28 (Spring 2005), p. 129. For a discussion of the legal issues raised by the initiative, see Daniel H. Joyner, "The Proliferation Security Initiative: Nonproliferation, Counterproliferation, and International Law," *Yale Journal of International Law* 38 (Summer 2005), p. 537.

4. A list of all seventy-seven states that have participated in PSI is available at U.S. State Dept., *Proliferation Security Initiative*, available at www.state.gov/t/isn/71884.htm.

5. U.S. State Dept., *Proliferation Security Initiative: Statement of Interdiction Principles,* available at www.state.gov/t/isn/rls/fs/23764.htm.

6. The six states are Belize, Croatia, Cyprus, Liberia, Marshall Islands, and Panama.

7. UN Security Council Resolution 1540, UN Doc. S/RES/1540 (2004). The measures decided in Resolution 1540 were extended two years by Resolution 1673; UN Doc. S/RES/1673 (2006).

8. The Department of Defense defines "risk assessment" as "the identification and assessment of hazards." "Risk" is, in turn, the "probability and severity of loss, linked to hazards." U.S. Defense Dept., *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02, www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

9. See Richard A. Posner, *Catastrophe: Risk and Response* (London: Oxford Univ. Press, 2004), pp. 120–22 (describing a "psychological asymmetry," which causes many to downplay low-probability/large-destructive-potential events, even when their expected costs are greater than some high-probability/lower-destructive-potential events). Judge Posner identifies a disturbing paradox in prevailing attitudes toward low-probability attacks: "A surprise attack is likelier to succeed when it has a *low antecedent possibility of success* and the attacker is weak, because on both counts the victim will discount the danger and because the range of possible low-probability attacks by weak adversaries is much greater than the range of possible high-probability attacks by strong ones" (page 93, emphasis added).

10. John Lewis Gaddis, *Surprise, Security, and the American Experience* (Cambridge, Mass.: Harvard Univ. Press, 2004), p. 75 (defenders must anticipate all contingencies; terrorists need provide only one).

11. White House, *National Strategy to Combat Weapons of Mass Destruction* (Washington, D.C.: December 2002) [hereafter NS-CWMD], p. 5, available at www.whitehouse.gov/news/releases/2002/12/WMDStrategy.pdf.

12. Ibid., pp. 5–6.

13. White House, *National Security Presidential Directive 41/Homeland Security Presidential Security Directive 13,* NSPD-41/HSPD-13 (Washington, D.C.: 21 December 2004), pp. 5–6, available at www.fas.org/irp/offdocs/nspd/nspd41.pdf.

14. *Global Maritime Intelligence Integration Plan for the National Strategy for Maritime Security* (Washington, D.C.: October 2005). The GMII Plan was one of the eight plans promulgated in support of the National Strategy for Maritime Security. The plan's designation as "for official use only" precludes a discussion of its contents here. See also James R. Holmes and Andrew C. Winner, "WMD: Interdicting the Gravest Danger," Naval Institute *Proceedings* (February 2005), pp. 72, 74.

15. *Maritime Operational Threat Response Plan for the National Strategy for Maritime Security* (Washington, D.C.: October 2005); MOTR Protocols, 4 April 2006. The MOTR Plan's designation as "for official use only" precludes a discussion of its contents here.

16. It must be acknowledged that many interdictions of vessels engaged in human and narcotics trafficking are based solely on what some would call "organic," self-generated intelligence—or, simply being at the right place at the right time. Such techniques are inefficient and will rarely be relevant to WMD interception operations.

17. The author of the observe-orient-decide-act (OODA) cycle concept was Col. John Boyd, U.S. Air Force.

18. Not considered here are the equally important applications of intelligence to WMD defense, reducing infrastructure vulnerability, and response and mitigation planning, each of which is a recognized element in the "counterproliferation" pillars of the NS-CWMD, p. 3.

19. "Indications and warnings" intelligence refers to intelligence activities intended to detect

and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied/coalition military, political, or economic interests or to American citizens abroad. It includes forewarning of: enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied/coalition nations; hostile reactions to U.S. reconnaissance activities; terrorist attacks; and other, similar events.

20. Dual-use materials are those that have both legitimate (peaceful) and illegitimate (weapons-related) applications.

21. Phil Williams, "Intelligence and Nuclear Proliferation: Understanding and Probing Complexity," *Strategic Insights* 5 (July 2006), p. 1, available at www.ccc.nps.navy.mil/si/2006/Jul/williamsJul06.pdf. ("The focus is now in large part on proliferation networks. These networks range from criminals trafficking nuclear materials from the former Soviet Union through the Caucasus, Balkans, and Central Asia, to the A. Q. Kahn network, which was, in effect, a privatized nuclear diffusion network.")

22. See John S. Hammond et al., *Smart Choices* (Boston: Harvard Business School Press, 1999), p. 209. Cognitive errors may result from a variety of causes, including experience bias, selective perception, wishful thinking, and overconfidence.

23. U.S. Defense Dept., *National Military Strategy to Combat Weapons of Mass Destruction* (Washington, D.C.: Joint Staff, 13 February 2006), p. 21.

24. See Peter F. Drucker, *The Essential Drucker* (New York: Collins, 2001), p. 251. ("A decision is a judgment. It is a choice between alternatives. It is rarely a choice between right and wrong. It is at best a choice between 'almost right' and 'probably wrong.'")

25. 1982 UN Convention on the Law of the Sea, art. 110 ("reasonable ground for suspecting" basis for right of visit); 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, art. 8 *bis* ("reasonable ground for believing"); *Proliferation Security Initiative: Statement of Interdiction Principles,* paras. 4(b) ("good cause shown") and 4(d) ("reasonably suspected of").

26. Wade Boese and Miles Pomper, "The Proliferation Security Initiative: An Interview with John Bolton," *Arms Control Today* (11 December 2003), p. 37, available at www.armscontrol.org/act/2003_12/PSI.asp.

27. The U.S. Department of State provided a thumbnail sketch of eleven "successful efforts" by the PSI partners between August 2004 and May 2005, mostly involving ballistic missile and nuclear technology shipments bound for Iran. The report does not indicate whether any of the interdictions took place at sea. See Robert Joseph, Undersecretary of State for Arms Control and International Security, "Transforming our Counterproliferation Efforts in the Asia Region" (remarks to the Institute of Defense and Strategic Studies, 15 August 2005, Singapore), available at www.state.gov/t/us/rm/51129.htm.

28. Commonly cited intelligence "failures" in nonproliferation monitoring efforts include the surprise 1998 nuclear tests in South Asia and, for some, the nuclear weapons program in North Korea.

29. See Nuclear Threat Initiative, *North Korea: U.S., Spanish Forces Seize Scud Shipment,* 11 December 2002, available at www.nti.org/d_newswire/issues//2002/12/11/7p.html.

30. Thus, the intelligence community's assessment can be said to be accurate but incomplete. Nevertheless, decision makers decided to go forward with the interdiction, exercising the internationally recognized "right of visit." See 1982 UN Convention on the Law of the Sea, art. 110.

31. Kenneth Rogoff, "The Cost of Living Dangerously: Can the Global Economy Absorb the Expenses of Fighting Terrorism?" *Foreign Policy* (November/December 2004), p. 70.

32. White House, *Bush Administration Actions Consistent with 9/11 Recommendations* (Washington, D.C.: 30 July 2004), available at www.whitehouse.gov/news/releases/2004/07/20040730-18.html.

33. "Israelis Say They Seized Palestinian Arms Ship," CNN.com, 4 January 2002. The freighter *Karine A* was intercepted by the Israel Defense Forces in the Red Sea on 3 January 2002 carrying Katyusha rockets, mortars,

sniper rifles, bullets, antitank mines, antitank missiles, and explosives. Although the ship was carrying conventional weapons, not WMD, when the IDF interdicted it en route to its Palestinian buyers, the operation stands out prominently in the annals of successful applications of intelligence to maritime interdiction operations.

34. See Congressional Research Service, *Port and Maritime Security: Background Issues for Congress,* CRS Report RL31733 (Washington, D.C.: updated 27 May 2005), 17. ("Perfect maritime security can only be achieved by shutting down the transportation system.") The quest for perfection raises what some refer to as the "asymptotic dilemma"—that is, increasing security investments run up against the iron law of diminishing returns: the result approaches, but never quite achieves, perfect security.

35. It is rare indeed to hear an intelligence assessment characterized as a "slam dunk." It will no doubt be rarer still in the coming years. It is far more common for such assessments to be cast in terms of probabilities. Where an estimate concludes that it is "probable" that a given ship is carrying a cargo of WMD concern, a boarding that turns up nothing does not render the assessment "wrong." It had, after all, been couched in terms of a probability of less than 100 percent.

36. White House, *The National Security Strategy of the United States of America* (Washington, D.C.: 17 September 2002), p. 15, available at www.whitehouse.gov/nsc/nss.pdf.

37. The German-flag containership *Palermo Senator* was delayed for four days while the Coast Guard and other federal agencies conducted a boarding to determine the source of radiation emissions from the vessel's cargo. Ultimately, it was determined that the radiation was being emitted from a cargo of clay tiles. The Coast Guard was later criticized for relying on obsolete radiation detection equipment. Ronald Smothers, "Ship's Radiation Is Traced to Harmless Tiles," *New York Times,* 14 September 2003, p. A-7.

38. Jason D. Ellis and Geoffrey D. Kiefer, *Combating Proliferation: Strategic Intelligence and Security Policy* (Baltimore, Md.: Johns Hopkins Univ. Press, 2004), pp. 149–53, 156–66.

39. An officer from U.S. Central Command asserted that the vessel was transporting thiodiglycol and thionyl chloride to Iran (ibid.). Both chemicals are dual-use products.

40. Ibid.

41. Ibid., citing Patrick E. Tyler, "No Chemicals aboard China Ship," *New York Times,* 6 September 1993, p. A4.

42. Rone Tempest, "China Demands Apology: Search of Ship Fails to Find Warfare Chemicals," *Chicago Sun Times,* 6 September 1993, p. 10.

43. Ellis and Kiefer, *Combating Proliferation,* p. 152. One possible explanation why no chemicals were found during the boarding in Saudi Arabia was that they had been dumped over the side before the ship arrived.

44. False-positive judgments in other contexts may result in devastating consequences, as did the conclusions drawn by the Soviet Union in 1983 when it shot down Korean Air Lines flight 007, and by USS *Vincennes* in 1988 that an approaching aircraft was hostile when in fact it was an Iranian passenger jet (U.S. State Dept., *Cumulative Digest of United States Practice in International Law, 1981–88, vol. 2* [Washington, D.C.: U.S. Government Printing Office, 1994], pp. 2340–49; and David Linnan, "Iran Air Flight 655 and Beyond: Mistaken Self-Defense and State Responsibility," *Yale Journal of International Law* 16 [1991], p. 245). The 1983 KAL 007 incident resulted in the deaths of all 269 on board (see *Cumulative Digest, 1981–88,* vol. 2, pp. 2349–50). The *Vincennes* incident resulted in the deaths of all 290 passengers on board the Iranian airliner. The *Vincennes* incident came on the heels of a missile attack on the USS *Stark* the year before. Thirty-seven *Stark* crewmembers were killed when two Exocet antiship missiles fired by an Iraqi F-1 Mirage jet struck the frigate. Iraq claimed the pilot had mistaken the *Stark,* a frigate, for an Iranian oil tanker (*Cumulative Digest,* vol. 2, pp. 2337–40).

45. In a rare public speech explaining some of the intelligence failures regarding Iraq's WMD programs, former CIA director William Tenet warned that "we cannot afford an environment to develop where analysts are afraid to make a call, where judgments are held back because analysts fear they will be wrong."

Remarks as prepared for delivery by Director of Central Intelligence George J. Tenet at Georgetown University on 5 February 2004, available at www.cia.gov/cia/public_affairs/speeches/2004/tenet_georgetownspeech_02052004.html.

46. Decades after the Cuban missile crisis ended, the United States learned that the Soviet forces had actually totaled approximately forty thousand men (twenty times the estimate) and that tactical nuclear devices—nine *Luna* missiles and six launchers—were already on the island.

47. See Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," in *The Art and Practice of Military Strategy* (Washington, D.C.: National Defense Univ. Press, 1984), pp. 378–79 (noting that "making warning systems more sensitive reduces the risk of surprise, but increases the risk of false alarms, which in turn reduces sensitivity").

48. The epigraph is taken from Michael Howard's and Peter Paret's edition and translation (Princeton, N.J.: Princeton Univ. Press 1984), p. 101.

49. The Department of Defense defines risk management as "the process of identifying, assessing, and controlling, risks arising from operational factors and making decisions that balance risk cost with mission benefits." Joint Publication 1-02.

50. The central importance of popular support for national security measures has long been acknowledged. See Clausewitz, *On War,* book 1, chap. 2 (identifying the "will" of the enemy as one of three factors critical to the outcome) and book 8, chap. 4 (identifying public opinion as a potential center of gravity to be defended or exploited in war). Similarly, in approaching an enemy, Sun Tzu advocated, "When he is united, divide him." Sun Tzu, *The Art of War,* trans. Samuel B. Griffith (London: Oxford Univ. Press, 1963), p. 69.

51. Although definitions of the precautionary approach or precautionary principle vary, at a minimum it stands for the proposition that uncertainty as to whether a course of action will cause harm (usually to the environment) should not be an excuse for failing to take action.

52. Some of the same questions have been raised about some of the intelligence assessments of Iran's nuclear program and that nation's role in the 2006 Hezbollah conflict with Israel.

53. In a response to the leading investigations into the British and American prewar WMD assessments, Professor Philip Bobbitt reminds the reader that the UN inspectors had been "fooled" by Saddam's claim in 1995 that he had abandoned his program (Philip Bobbitt, "How Proof Became a Burden: Saddam's Intentions Had to Be Part of the Spook's Judgment Call," *Guardian,* 28 October 2004). They realized their mistake only after Saddam's son-in-law, Hussein Kamal, defected and revealed the details of a new clandestine WMD program.

54. See Philip Bobbitt, "Seeing the Futures," *New York Times,* 8 December 2003.

55. Philip Bobbitt, "Today's War against Tomorrow's Iraq," *New York Times,* 10 March 2003. The relevant question would therefore not be whether we are better off or safer today than we were before an action was taken, but whether we are better off or safer than we would have been had we pursued an alternative course of action, including taking no action.