Ethics, Intelligence, and Preemptive and Preventive Actions

Ralph L. DeFalco III

Since it appeared in the National Security Strategy of the United States in 2002, the Bush Doctrine of preemption has been a source of much confusion, partisan debate, and controversy. Part of that confusion flowed from the tendency by both the Bush administration and the press to conflate preemption and prevention. In addition, a great deal of debate in the media and in the halls of Congress was generated by the putative doctrinal approach to the use of military force in preemptive actions—and even prompted the press to pose a question on doctrine to a vice presidential candidate. The controversy, of course, stems from the U.S. military involvement in the Iraq War, an action the Bush administration claimed as preemptive and critics vilified as aggression, as preventive war, and therefore as immoral.

Despite the flurry of confusion, debate, and controversy on this issue, only modest efforts have been made to evaluate the nature of the intelligence requirements that support preemptive and preventive actions undertaken by policymakers. Even less attention has been focused on the ethical bounds of intelligence in support of preemptive and preventive actions. This article addresses the ethical issues raised by intelligence support of preemptive and preventive actions and makes an assessment of these issues presented within the context of the elements of just war tradition. It argues that the just use of preemptive and preventive acts of state, and especially those employing armed force, must be preceded by telling intelligence that unambiguously identifies the threat to the state and to its security. It also argues that intelligence in support of just war should, in and of

---

The views expressed in this paper are those of the author and do not reflect the official policy or position of the Department of the Navy, the Department of Defense, or the U.S. government.

itself, be conducted ethically, and to that end *jus in bello* tenets apply to intelligence production, evaluation, and dissemination. The aim here is to propose a framework in which the actions of intelligence providers can be viewed inside an established ethical construct, not to create a new construct. In addition, this work is presented so that it might encourage further discussion. Then, too, rather than deal with these issues in the abstract, this paper also uses a case study—the Israeli attack on Iraq's Osirak nuclear reactor—to demonstrate how the ethical dimensions of intelligence in support of preemptive and preventive actions might be assessed in practice.

Defining Preemptive and Preventive Actions

The terms "preemption" and "prevention" require definition not only because of the confusion caused by the misuse of the terms, but also because some authors have conflated the terms so far as to strip them of their distinctions. Michael Walzer, in *Just and Unjust Wars* (2006), suggests that the two terms represent ends of a "spectrum of anticipation" upon which states act when they perceive a threat to their national interests.[1] At one end are actions that are morally justifiable uses of force in the face of a threat, or preemptive actions, and at the other end lie the less morally certain preventive wars, "fought to maintain the balance, to stop what is thought to be an even distribution of power from shifting in a relation of dominance and inferiority."[2]

Walzer's assessment of the justifiable self-defense implicit in preemptive action is echoed by other authors and has been broadly accepted as morally right. Colin S. Gray, for example, contends that preemption is not controversial, legally, morally, or strategically, because "to preempt means to strike first . . . in the face of an attack that is either already underway or is very credibly imminent."[3] Here, then, is the inherent right to self-defense in the face of actual aggression or with incontrovertible evidence that aggression is forthcoming. The use of preemption relies upon a state's capability to assess the evidence of an imminent attack, specifically the adversary's capability, intent, and timing. This assessment can occur across a continuum:

> There are two ways to think about a preemption timeline: either the traditional peacetime-to-crisis-to-conflict-to-post-conflict timeline, in which preemptive action is taken in peacetime or building crisis; or, in the case of WMD, where an adversary is on the acquisition-to-use timeline. The

> points on the later continuum range from just prior to the time at which an adversary has acquired a useable capability . . . to the point where the adversary has the capability and generally hostile intent, to the point where there is a specific hostile intent and use is imminent.[4]

The measure of preemption is at the moment of danger—when an adversary has capability and intent and the use of force is imminent—and the preemptive reaction is in just self-defense, by means of the use of force calculated to blunt or even ward off the aggression.[5] Walzer, in this regard, goes further and draws his line to distinguish between legitimate and illegitimate first strikes, not in the face of an imminent attack but upon recognition of a sufficient threat—a phrase he recognizes as "necessarily vague." The Israeli attack on the Egyptian air force at the start of the Six-Day War, coming as it did in the face of undeniable and imminent Egyptian and Syrian preparations for an attack on Israel—that is, recognition of a sufficient threat—is perhaps the clearest and least controversial recent example of justifiable preemption and the use of force in self-defense.

A state, then, acts preemptively when the timing and means of hostile action against it have been chosen by another state. By contrast, the state taking preventive action chooses both the timing and nature of its intervention. Gray suggests that "by preventive action, a state strikes in order to control dangers in its external security environment."[6] States, however, have other means by which they attempt to control dangers to their security, and so Gray's definition might serve better if it were to suggest that a state acts to control danger. Other authors persist in using the term "preventive war," but the reality is that preventive actions can be actions other than war.

Walzer's concept of a spectrum of anticipation implies, for instance, that there is time to consider and implement a range of actions other than strike or use of force, which may be taken by the state in the face of an adversarial threat. So a definition of preventive action needs to be much broader, and needs to account not only for preventive war, but for strikes or raids and even preventive actions that include not just military but also diplomatic, informational, and economic intervention as well. Nonetheless, these can be seen as hostile actions, for they are intended to frustrate the ambitions of another state to either gain or press an advantage. Preventive actions, then, can be defined as those acts of statecraft, including strike and war, designed to diminish the dangers posed by another state and to "prevent attacks upon itself or its interests by destroying opponents or opponents' capabilities to achieve their objectives."[7]

Two examples in this regard are worth noting. The United States used aggressive economic means for nearly two years before the Japanese attack on Pearl Harbor in late 1941 in hopes of forcing Imperial Japan to change its aggressive foreign policy and abandon its war of aggression in China and French Indochina. Washington imposed progressively tighter sanctions on Tokyo that eventually resulted in a total embargo of petroleum products, scrap metals, and steel. The action proved futile: "The United States, together with the British and Dutch empires, so restricted Japan's access to raw materials, especially oil, that Japan was forced to choose between war and economic strangulation."[8] Unwilling to negotiate and unable to compel either Britain or the United States to allow it to retain its gains, Japan "simply struck out ferociously to the very limit of its reach. And then it awaited disaster."[9] Japan chose to continue its war in Asia and expanded the war to attack the Western powers; the resort to preventive means other than armed force failed. "The point is," however, "that the United States acted from a powerfully preventive motive, and it applied pressure with the economic and financial rather than the military instrument of grand strategy."[10] In 1961, during the Cuban Missile Crisis, the United States chose a naval quarantine as an action intended to prevent the movement of Russian nuclear warheads and missiles to launch sites that had already been prepared on the island. This patently hostile act of closing the open seas to the movement of Russian ships was accompanied by intense diplomatic efforts to resolve the crisis. So it is possible that prevention can also include a range of actions, sometimes conducted concurrently, other than war.

Intelligence in Support of Preemptive and Preventive Actions

The standards for intelligence in support of preemptive or preventive action are, indeed, quite high, as no well-informed decision can be made to undertake this action unless intelligence is provided that clearly identifies the threat to the state. "Intelligence gathering and analysis are at the heart of implementing any doctrine of preemptive/preventive war, since such a doctrine presumes the ability to know both the intentions and capabilities of potential enemies."[11] In addition, intelligence—and especially intelligence for any preemptive action—will need to provide strategic warning, for timing is essential to preemption. Moreover, the capability of the intelligence

community to accurately gauge the timetable of an adversary's plan figures as the critical information needed for preventive actions.

In the face of these demands for accurate, predictive, and timely intelligence, there is also a requirement for intelligence to be actionable. This is especially true for weapons of mass destruction (WMD), with their threat of sudden attack, mass casualties, and catastrophic consequences. A highly accurate intelligence assessment of the capability and the intent of an adversary is

> the load-bearing pillar of the American campaigns against WMD-armed adversaries. Without high-quality and timely reporting and analysis, the policy of preemptive or preventive military action will simply not be feasible. . . . If the United States does not have sufficient intelligence to know the "what, where, when and how" to attack an adversary's WMD—including WMD stocks, production facilities and delivery systems—American precision munitions will stand idle because neither predictive nor preventive military options will be viable for the commander in chief.[12]

The Clinton administration, for example, considered preventive strikes to strip North Korea of its nuclear weapons capabilities when U.S. intelligence determined the North Koreans were extracting weapons-grade plutonium from its research reactor at Yongbyon. Lacking actionable intelligence, specifically the location of the North Korean stocks, a strike was not considered feasible. Not knowing the real intentions of North Korea's leadership and fearing a retaliatory strike on South Korea, the costs of the strike were also considered unacceptable. The administration opted instead for the Agreed Framework of 1994, using diplomacy (and an agreement to provide fuel and two light water nuclear reactors) to prevent further North Korean development of plutonium weapons.[13] That diplomacy has failed to dissuade North Korea of its nuclear ambitions.

Intelligence, then, is not only the "load-bearing" pillar for preemptive and preventive actions regarding WMD. Intelligence may be legitimately regarded as bearing the weight of responsibility for creating decision superiority for policymakers considering any preemptive or preventive actions. Any assessment of the ethical nature of intelligence in support of preemptive and preventive action then must be viewed through this lens: Intelligence professionals support policymaking; they do not—nor should they—make policy.

> The proper relationship between intelligence gathering and policymaking sharply separates the two functions. The intelligence community

> collects information, evaluates its credibility, and combines it with other information to help make sense of situations abroad that could affect U.S. interests. Intelligence officers decide which topics get their limited collection and analytic resources according to both their own judgments and the concerns of policy makers. Policy makers thus influence which topics intelligence agencies address but not the conclusions they reach. The intelligence community, meanwhile, limits its judgments to what is happening and what might happen overseas, avoiding policy judgments about what the United States should do in response.[14]

From this perspective the ethical assessment of intelligence in support of preemptive or preventive action would seem to be judged in the context not of the *justice of war* but instead of *justice in war*. Here intelligence is not an end in and of itself, but a means that supports the policymaking process. After all, the decision to take preemptive or preventive action rests with the policymaker and not with the intelligence professional. "In practice, however, this distinction is often blurred, especially because analytic projections may have policy implications even if they are not explicitly stated."[15] Because that distinction is often blurred, the same standard applied to policymakers who decide on preemptive and preventive actions, might also be useful in assessing the ethical responsibilities of intelligence professionals whose work and judgments support those decision makers. Just war tradition provides a starting point for any assessment of the rightness of intelligence actions and judgments that inform preemptive and preventive decision making. Specifically, the following six criteria may apply: (1) just cause, (2) legitimate authority, (3) right intention, (4) proportionality, (5) likelihood of success, and (6) war as a last resort.

Just Cause

Self-defense is a just cause. A preemptive action, especially the use of force taken in the face of imminent aggression, is morally justifiable. Preventive actions are also morally justifiable in the face of a sufficient threat, that is, when an adversary has both capability and intent, and the failure to act could result in greater harm in the foreseeable future. In these instances, the intelligence professional will find the demand for a morally justifiable action rests on the accuracy of the measures of an adversary's capabilities and intent. Here the ethical standard is one of truth, insofar as intelligence is capable of discerning the truth of the capabilities and intentions of

an adversary. A less than fully truthful assessment of an adversary's capabilities, especially one made to assuage policymakers bent on action, would clearly be unethical. There is also an ethical burden on the intelligence analyst to provide an accurate gauge of the adversary's intent, for clear intent to harm must be present to cause a sufficient threat.

The institutional predilection to exaggerate threats, however, can lead the intelligence professional astray. By "emphasizing warning over prediction," intelligence professionals are often drawn over the line too quickly, especially so as they are often susceptible to ruse and deceptions by the adversary.[16] Clearly it would be unethical to exaggerate the threat to justify preemptive or preventive action, especially to justify a course of action already decided. But "political and military leaders prefer that the Intelligence Community err on the side of warnings that are too many or too strident rather than too few or too ambiguous."[17] In the face of numerous uncertainties, these leaders often demand certitude. The lessons of both Pearl Harbor and 9/11 have anguished leaders who may be forced to face intelligence warning failures and the devastating surprise attacks that result. The potential for misreading an adversary's intent is also quite high, since "one of the most serious limitations on confidently predicting hostile action by another state is that governmental leaders themselves may not know their minds or may not be in complete control of events."[18] So the intelligence professional making an assessment to inform a decision for preemptive action is often presented with a moral dilemma: to err on the side of a more cautious and perhaps more truthful warning, acknowledging less than prescient knowledge of the adversary's plans, or to risk at some point in the future a devastating attack with little or no warning.

Legitimate Authority

Legitimacy speaks to the moral use of authority, with that authority rooted in law or custom. In this case, only the policymaker has the legitimate authority to decide to take preemptive or preventive action. The intelligence analyst who seeks to make policy by shaping intelligence judgments that would force the hand of the policymaker acts immorally on two counts. First, there is the deliberate deceit to alter or adduce evidences—a lie—to justify a conclusion that provokes action. The effort can be made to induce the policymaker to act precipitately or to demur, but in either instance, the decision is

influenced by the bias of the intelligence provider. While the difficulties of eliminating an unknowing bias from the intelligence estimate cannot be overstated, it is quite another matter when a purposeful bias to action wholly shapes the conclusions of the estimate so as to misdirect the policymaker. Second, there is the unethical abrogation of the legitimate authority of the policymaker, when the intelligence provider acts in a way that forces the hand of those in authority. The intelligence provider who seeks to make policy by deliberately misinforming the policymaker usurps both the rights and the obligations of another and so steals from another. This is not theft in the sense to which we are accustomed, that is, taking the property of another; it is rather the taking of the lawful authority or merit of another.[19]

These unethical actions should not be confused with the obligations that the intelligence provider has to make an informed assessment of the consequences of policy decisions. A candid assessment of the likely outcomes of courses of action considered by the decision maker may, in fact, influence the decision-making process. The point, however, on which this argument turns is the distinction between informing decision making and making the decision; intelligence providers have no legitimate authority to make decisions of state.

Right Intention

If it holds true that the intelligence analyst who adulterates analytical judgments to influence policymaking both lies and usurps the legitimate authority of the policymaker, then it is true, too, that the analyst fails to act with right intention in this instance. More insidiously, analysts who alter their judgments to curry favor with their superiors or with policymakers also fail to act with right intention. Analysts who take this route seeking preferment or advancement, in hopes of gaining recognition or increased stature, sacrifice truth for self-aggrandizement and personal gain. Actions taken with these motives are unethical regardless if they are intended to inform preemptive or preventive decision making.

In much the same way, analysts who alter or amend their judgments to support a decision that has been made to act preemptively or preventively in the absence of a just cause also fail to act with right intention. By withholding critical evidence so as to adduce evidence to support a predetermined action, analysts and intelligence leaders fail in their moral obligation of truth telling and cross the line between purveying intelligence and making policy.

Proportionality

The intelligence assessment of an adversary's capabilities and intent drives the policy decisions for proportionality. Here again the burden for ethical assessments falls squarely on the analyst. In this case, too, the distinction between justice of war and justice in war now applies, for the means chosen by the policymaker are often actually dictated by the assessment. Should the intelligence provider knowingly exaggerate the adversary's capabilities or intent, the moral culpability for a disproportionate action would largely fall on the analyst for having shaped the evidence that gave rise to the action. Deliberately misleading assessments, however, must be separated from assessments made in honest ignorance. Intelligence analysts rarely work with perfect knowledge of an adversary's capabilities. A truthful estimate of an adversary's capabilities, made on the basis of all that is known and verified at the time of the estimate, is the most that can be expected. The analyst who makes an estimate in this way acts justifiably. Even if evidence found at a later date were to call the original assessment into question, or to invalidate it in its entirety, the analyst who provided the assessment in full good faith cannot be judged as having acted immorally in the first case.

Likelihood of Success

The prospect for success of preemptive and preventive actions is ineluctably linked to the accuracy and timeliness of intelligence. But this criterion introduces another standard of measurement that is not easily applied to the actions of the intelligence provider. Clearly, the responsibility for gauging the likelihood of success of preemptive or preventive action must be made by the policymaker and, by rights, should figure prominently in the decision to act. Having made that point, it is also clear that the policymaker must have a high degree of confidence in the intelligence assessments and predictions. So while the intelligence provider is not morally responsible for the consequences of failed action, that provider does have an ethical responsibility to fully inform the policymakers of the prospects for success and of the consequence of failure. These assessments of prospects and consequences are held to the same standards of veracity and completeness as are the assessments of adversarial capabilities and intent.

If, for example, the full capabilities of an adversary are only dimly perceived, if there is some uncertainty as to the strength or location

or timing of the threat, then the intelligence provider is ethically compelled to communicate to policymakers the degree of uncertainty that accompanies the intelligence assessment. In addition, if the consequences of the proposed actions cannot be fully assessed—if, for example, not enough is known to predict the response of the adversary—then this must also be communicated to the policymaker. Here even an informed speculation must be tempered with the open acknowledgment that there are few absolute certainties in the behaviors of other actors. More pointedly, the intelligence provider is bound to tell the policymaker what is not known. This candor is required to meet the ethical requirement to fully inform the policymaker's appraisal of the likelihood of success.

Last Resort

The sixth and last criterion usually applied in just war theory, the test of war as a last resort, does not at first glance seem readily applicable to test the moral rightness of intelligence in support of preemptive and preventive actions. The decision to make war—in spite of the blurring of the roles and responsibilities of the policymaker and the intelligence professional—does, in fact, finally rest with the policymaker. However, as discussed earlier, preventive actions include other means than war. The test of war as a last resort might then be applied in two ways.

The first application of the measure of last resort is to determine if the intelligence provided was both sufficient and timely enough to offer the policymakers actionable alternatives. Clearly, if the intelligence were neither sufficient nor timely because of the difficulties inherent in collecting that which is deliberately hidden, or if there were little confidence in judging the intentions of an adversary, there is no unethical action. However, if accurate and timely intelligence were to be purposefully delayed so as to close off consideration of options other than war, then this conduct would be immoral, though it is difficult to imagine a scenario in which this might occur, given the risks and uncertainty attendant any military action.

The second test might also be applied to the intelligence provider's responsibility of informing the decision-making process. As discussed above, intelligence providers have an ethical responsibility to provide policymakers with a truthful appraisal of the likelihood of success of various actions. Were the intelligence provider to deliberately discount the potential for effective actions other than war, then this

would be unethical. Again, it is difficult to imagine the circumstances in which an ethical intelligence provider would deliberately withhold an assessment that would forestall the use of force and a rush to war when time and other credible means are available.

While the approach thus far has dealt with these issues in the abstract, there is little in the way of utility that comes from this effort unless it can be applied in practice. To that end, an actual case may serve to show how this approach can be used.

The Raid on Osirak

In the deepening dusk of the evening of June 7, 1981, eight Israeli air force F-16 fighters raced at rooftop level over the suburbs of Baghdad, Iraq. Moments later, the attacking aircraft thundered up to altitude and then dove down on bombing runs aimed at the nuclear reactor dome at Osirak. Within eighty seconds, the eight aircraft, attacking in staggered flights of two, sent their bombs crashing through the dome to explode in the heart of the reactor's cooling pool, with its nest of nuclear reactor rods. Seven of the eight attackers bombed with pinpoint accuracy, and all then sped away unscathed into the cloak of night on a 680-mile return flight to the air base in the Sinai from which they had launched earlier that afternoon.

With this single raid, Israel destroyed Iraq's nearly fully functional nuclear reactor, and with it, Saddam Hussein's plan to extract weapons grade materials and build Iraq's arsenal of nuclear bombs. Using the definition as developed earlier, the Israeli attack was a preventive action, fully intended to destroy Saddam's capability to build a nuclear weapon. As such, it was the use of force not in the face of an imminent threat, but rather in the attempt to control mounting danger in Israel's external security environment. Israel saw the development of Iraqi nuclear weapons as a threat sufficient to justify action in its own self-defense.[20] The attack provoked a maelstrom of criticism from outraged leaders around the world as being both unprovoked and aggressive, an illegitimate use of force. U.S. Ambassador Jeanne Kirkpatrick, in a rare U.S. action critical of Israel, voted for the United Nations resolution condemning Israel, even going so far as to compare the unprovoked Israeli attack to the Soviet invasion of Afghanistan.

Despite the worldwide condemnation, the Israeli strike was a justified use of a preventive action because the decision to take that action was remarkably well informed by intelligence that uncovered

unambiguous evidence of a threat to the security of the state. Israeli intelligence provided policymakers, both in the Israeli government and in the Israel Defense Forces (IDF), with accurate and timely assessments of the intent of Iraqi leadership, the capabilities of the nuclear plant and its operational timeline, the design and construction of the site and its defenses, and the critical vulnerability of the target.

Israel had been the target of Iraqi hostility and military attacks for decades. Iraqi ground forces invaded Israel in the Independence War of 1948, the Iraqi air force tried to attack Tel Aviv in 1967, and Iraqi artillery shelled Israeli towns during the War of Attrition (1969–1970). Iraq's hostile intent was a given for Israeli leaders. Israeli leaders were also well informed of the intent of Iraqi leader Saddam Hussein. Saddam's hostility toward Israel and his public statements—including his boast to use a nuclear weapon "against Zionist enemies"—were taken at face value.[21] The fact that the compound at the Osirak nuclear reactor was named Al-Tuwaitha—"the Truncheon"—was not lost on Israeli analysts. Two months before the actual attack, Israeli intelligence prepared a thirty-three-page psychological profile of Saddam and forwarded it to Prime Minister Menachem Begin.[22] This action met the ethical requirement for intelligence providers to develop and disseminate to policymakers a credible and accurate assessment of the intent of enemy leadership. The report offered a chilling view of the Iraqi leader, a man who would not be deterred:

> If in his estimation, the use of atomic weapons would give him the chance to strike Israel, and gain for himself at the same time a leadership position in the Arab world, he would not hesitate to use the bomb . . . even if it would cost him similar retaliation from Israel, which would create damage and loss of life in Iraq itself.[23]

The Begin government also solicited the advice of Israeli intelligence in assessing the consequences of a proposed military raid on the Osirak facility. It is interesting to note that Chief of Israeli Military Intelligence General Yehoushua Saguy and Yitzhak Hofi, chief of the Mossad, Israel's secret intelligence service, opposed any military attack. They were joined in their objections by Deputy Prime Minister Igael Yadin. "Such violation of a nation's sovereignty was an act of war, they argued. It was too risky and there were too many unknowns."[24] In spite of his objections, Hofi directed the development of intelligence plans and operations that would provide

the Israeli government with estimates and intelligence that opened up a range of options.

Prior to the strike, Israeli intelligence provided policymakers with sufficient intelligence to pursue other means than the resort to military force. Scientific and technical analyses of the weapons-grade production capabilities of the reactor when fueled with enriched uranium were passed to Israeli officials, who lobbied the French government to suspend the uranium shipment. After receiving intelligence that French technicians were working at the site, Begin sent a personal note to French president Giscard d'Estaing "virtually begging him to pull out the French technicians from al-Tuwaitha and hold back from sending Iraq . . . the final twelve kilos of enriched uranium."[25] Israeli intelligence uncovered the shipping dates for critical components of the reactor and determined their exact warehouse locations in France. With that information, Israeli officials authorized a covert operation to damage the components en route. The successful attack delayed but did not halt the construction of the reactor. Israeli intelligence, then, provided the opportunities for the Israeli government to undertake both diplomatic and covert actions before resorting to the use of military force.

Israeli intelligence had also been keeping close watch since 1977 on the development and construction of the reactor at Osirak.[26] Iraq had contracted with France to build the reactor in 1973, and by the middle of the decade French engineers and scientists had joined Iraqi scientists in planning the Osirak site. Israel was also aware of UN International Atomic Energy Agency reports that France had agreed to provide the Iraqis with enriched uranium, a reactor fuel that would produce plutonium for weapons-grade materials. Israel had used French assistance to secretly build its nuclear arms program and so was no stranger to the French reactor technology; Israeli nuclear engineers provided reliable scientific and technical intelligence. This human intelligence was supplemented by that provided by the Mossad, which recruited an Iraqi nuclear engineer as an unwitting source of information on the program.[27] So, by early 1980, Israeli military planners had detailed plans and even some photographs of the growing Osirak facility. Israeli intelligence, then, had sufficient information to make for policymakers a credible estimate of the capabilities of the Osirak reactor.

Based on the reports coming from the site at Osirak, Israeli scientists and engineers also estimated the production timetable for completion of the reactor and the fueling of the core. Israeli intel-

ligence had also acquired high-resolution KH-11 imagery from U.S. reconnaissance satellites, a significant addition to the grainy photos smuggled out of Iraq.[28] With this and other information, Israeli intelligence was able to determine with some precision the point at which the nuclear reactor would be fueled with the enriched uranium and go "hot." This, in and of itself, would not guarantee that Iraq had the capability to build a nuclear weapon. Indeed, scientific and technical intelligence estimated that Iraq was a year or more away from building a bomb, even with a functioning reactor. Israeli intelligence estimated that Iraq would have enough plutonium to build two atomic bombs by 1982.[29]

Israeli intelligence was at pains to determine the vulnerabilities of the site. Israeli nuclear engineers were recruited by Mossad to meet with American scientists and engineers at the U.S. Nuclear Regulatory Commission in Washington, DC. Ostensibly the Israeli engineers were interested in learning details about an electric power reactor that Israel might purchase. Feigning concerns about sabotage and terrorist attack, the Israelis pressed to know the most vulnerable part of the reactor and what the consequences would be of an explosion inside the reactor. U.S. officials confirmed that the reactor rods and the cooling system were most vulnerable and warned that if the reactor were blasted while fueled, there would be danger of precipitating an uncontrolled nuclear event. After the meeting, the U.S. officials noted that the Israelis seemed to have little interest in building the plant underground as a protective measure and that it was not clear whether they wanted to know how to defend one of their own plants or how to destroy one.[30]

Determining the Iraqi production timetable was critical to Israeli decision making, however, because it identified the narrow window in which Israel had time to legitimately act in its own defense without disproportionate force and unintended consequences. Intelligence assessments of an attack that would breach a hot reactor core estimated tens of thousands of civilian casualties would be caused by the deadly fallout plume or a runaway nuclear event. But Israeli intelligence also estimated that an attack made before the reactor went hot would still deprive Iraq of weapons-grade production capabilities. With this assessment, Israeli intelligence provided policymakers with information on which to gauge the likelihood of success if an early attack were delayed and to measure the consequences of a delayed attack that might kill tens of thousands of innocent civilians downwind of Osirak. Based on these intelligence estimates, Begin

chose to attack before there was any danger of fallout and the risk of loss of civilian lives.

In this case, Israeli intelligence provided the Begin government with accurate, timely, and predictive intelligence. The intelligence provided was sufficient to allow the Israeli leaders to consider a range of options, and in fact they first used means other than military force to try to achieve their national security objective. If the intelligence providers' actions are measured against the criteria developed above in the context of just war theory, it is apparent the moral requirement here was met.

Just Cause—Israeli intelligence accurately assessed the Osirak capability and determined Saddam's intent to build and use an atomic weapon against Israel, and thereby established the sufficient threat for Israel to act in a just cause.

Legitimate Authority—Despite their objections to military action, Israeli intelligence leaders Saguy and Hofi ensured that Begin had all the information possible to make an informed decision. Though asked for their opinions, both men yielded the decision to Begin, Israel's lawfully elected head of state.

Right Intent—Nothing here would indicate that the intelligence providers acted otherwise than with the right intent. Even in their objections, Saguy and Hofi directed their agencies to produce the intelligence required by the policymakers to develop and execute a range of preventive actions, including, finally, the military strike.

Proportionality—Israeli target development of Osirak, including the pinpoint identification of its critical vulnerability and detailed scientific and technical intelligence, ensured the raid was proportional to the threat. The bombing destroyed the weapons production capability only. By recommending the strike occur on a Sunday evening, intelligence planners minimized casualties; one French researcher and ten Iraqi soldiers died in the attack. Intelligence also fixed the production timetable at the site and determined the point at which the reactor would go hot. A nuclear event was avoided; tens of thousands of civilian lives were spared.

Likelihood of Success—The case shows that extraordinary efforts were made to ensure the success of the bombing raid. Military planners were provided with detailed imagery, scientific and technical data, hours of operation, the site's likely production timetable, and myriad other pieces of intelligence to develop a sound attack plan. Israeli air force pilots and technicians chose their at-

tack strategy and tactics based on solid intelligence of their weapons capabilities and defenses at the site and this also increased the likelihood of success.

Last Resort—The military raid was the final attempt made by Israel to prevent Iraq from acquiring an atomic weapon. Intelligence had provided policymakers with sufficiently accurate assessments to exercise opportunities to take diplomatic actions. Israeli intelligence also mounted covert actions intended to delay or destroy the Iraqi nuclear capability.

The Moral Implications of Intelligence for Preemptive and Preventive Actions

Morally justifiable preemptive or preventive actions—and certainly those that are openly hostile—call for decision making that is well informed by intelligence. This is especially true of actions that require the use of armed force, and clearly, "in order to be morally justifiable, preventive war must be based on the firm knowledge of a hostile opponent's capabilities and intentions."[31] The moral quotient of the preemptive and preventive actions taken by the state will often be judged in the court of world opinion.[32] Intelligence that supports these actions must be so compelling as to dispel doubt. Intelligence must accurately gauge the nature of the threat and its timing and clearly identify the sufficiency of the threat to the security of the state. Intelligence, then, must of necessity precede any deliberations and decision making for preemptive or preventive actions, and especially those involving the use of force.

In addition, the argument here is that intelligence in support of preemptive and preventive action must be held to a moral standard. The demand for intelligence in support of policymakers weighing preemptive and preventive courses of action places a heavy burden on the intelligence provider for accurate, predictive, and timely assessments. This should not be confused, however, with a demand for omniscient or prescient intelligence. The test here is for intelligence that is actionable. In the case of preemptive action,

> A lower quality of information will suffice to enable the preemptor to achieve a seriously disrupting effect. In fact, one could argue that given the would-be preemptors choices—to strike first or be struck first—it almost does not matter how good is the intelligence. One preempts as best one can with the information available. Since it is far too late

> to prevent the attack, virtually any harm that can be inflicted on the enemy's confidence, plans and forces, must be welcome.[33]

Preventive action, peering as it does into a future that may be only dimly perceived, requires intelligence that is as accurate as time, capability, and reason permits. Given the difficulties that confront any intelligence provider seeking to know what is not known, to find what is hidden, and even to divine the intent of an adversary, it would be unreasonable to demand perfect intelligence. It is not unreasonable to demand the best that can be had and to take measures to ensure the intelligence is sufficient for the state to justify its course of action.

It is also reasonable to hold the intelligence provider to standards of moral conduct in developing assessments to inform policymakers weighing the merits of preemptive and preventive actions. Just war tradition provides workable criteria for these moral standards. The intelligence analyst is ethically bound under these criteria to conduct that is truthful in making assessments of the adversary's intent and capabilities to ensure policymakers act in a just cause. These providers are also ethically bound to fully and faithfully inform decision makers in the exercise of their legitimate authority. They are also obligated to ensure that intelligence is unbiased and free of any undue outside influence that would otherwise color an assessment, to provide intelligence with the right intention, and to make candid assessments of the likelihood of success of various actions. The intelligence provider also bears the ethical responsibility for making assessments that allow the policymakers to craft actions proportional to the threat. Insofar as they are informed and able, intelligence providers must be prepared to assess the impact of actions other than war—diplomatic, economic, and informational—so that the use of force is, indeed, a last resort and one likely of success.

Critics of this approach and the use of the elements of just war theory to assess the ethical action of intelligence analysts and providers might well argue it is a meaningless exercise. In the end, the moral obligation for taking preemptive or preventive actions rests with the decision maker. The discussion above, however, shows the ways in which the work of the intelligence provider influences decision making. So while the decision maker admittedly has the ultimate obligation to act morally, the intelligence provider cannot avoid the obligation to act ethically in the collection, production, and analysis of intelligence, simply because this intelligence must precede any

consideration of preemptive or preventive action. Intelligence is truly the load-bearing pillar for these decisions.

Others might argue that the framework has been applied in this test to the "best case." This is a fair criticism. Many foreign policy experts and academics now regard the Israeli attack on the reactor at Osirak as a textbook example of a morally justified preventive action. So while it is true that the attack itself was morally justified, the intelligence actions taken can and should still be judged—and found wanting or not—on their own merits.

It has been suggested here that ethical obligations apply at every level of the intelligence cycle and to all intelligence providers who support policymakers weighing preemptive and preventive actions. Moreover, since this is but one case, others may wish to develop additional cases and further test the validity of this approach for assessing the ethical actions of intelligence providers. The criteria of just war theory may well be found to be readily applicable to intelligence providers in these cases; the framework proposed here, then, can create a standard for the ethical practice of intelligence that supports both preventive and preemptive action. It is in this way that intelligence can be said to be conducted in a just cause—and by just means.

Acknowledgments

The author wishes to thank Dr. Brian Smith and Dr. Mark Overstreet for their insightful comments and review of this work.

Notes

1. Michael Walzer, *Just and Unjust Wars*, 4th ed. (New York: Basic Books, 2006), 74–75.
2. Ibid., 76.
3. Colin S. Gray, *The Implications of Preemptive and Preventive War Doctrines: A Reconsideration*, Strategic Studies Institute, July 2007, v.
4. M. Eliane Bunn, "Preemptive Action: When, How and to What Effect?" *Strategic Forum*, Institute for National Strategic Studies, National Defense University, no. 200 (July 2003): 3, http://www.ndu.edu/inss/strforum/SF200/sf200.pdf (accessed November 10, 2008).
5. Prevailing definitions of preemption have, at their core, the concept of the use of force in self-defense to deflect or ward off the blow of an adversary. However, it may be possible to use means other than force to preempt the use of force. The scope of this paper, with its focus on the ethics

of intelligence in support of preemptive and preventive actions, precludes an extended discussion of these alternative means to the preemptive use of force. Even so, one historical example may suffice to make the point regarding both the difficulty and the efficacy of responding with other means to the imminent use of force. In April 1861, newly elected president Abraham Lincoln was confronted with an openly hostile secessionist movement in South Carolina. Officials in that state had ringed the harbor in Charleston with guns aimed at the federal Fort Sumter, still then in Union hands. Badly outnumbered, outgunned, and surrounded, the Union troops holding the fort faced imminent attack. Lincoln had sworn himself to protection of all federal properties even in the face of secession. Lincoln might have chosen to preempt the attack on Sumter by reinforcing the garrison with men and arms. Instead he chose to provide humanitarian relief to the garrison and attempted to reprovision them with food and medicine. This objective was clearly communicated to the secessionist officials, who acknowledged Lincoln's message and resolved to oppose the humanitarian mission with force if need be. Faced with the prospect of an action that would have demonstrated continued federal control of the fort, the secessionist leadership opened an attack on Sumter. While the garrison was forced to surrender and abandon the fort, the attack galvanized public opinion in the North in favor of opposing secession by force of arms. Even so, Lincoln's actions actually precipitated the attack he wanted to avoid. See William Lee Miller, *President Lincoln: The Duty of a Statesman* (New York: Alfred A. Knopf, 2008), 48–71.

6. Gray, *Implications of Preemptive and Preventive War Doctrines*, 13.

7. James J. Wirtz and James A. Russell, "U.S. Policy on Preventive War and Preemption," *Nonproliferation Review*, Spring, 2003, 116.

8. Angelo Codevilla and Paul Seabury, *War: Ends and Means*, 2nd ed. (Washington, DC: Potomac Books, 2006), 233.

9. Ibid., 234.

10. Gray, *Implications of Preemptive and Preventive War Doctrines*, 23.

11. Greg Thielmann, "Intelligence in Preventive Military Strategy," paper from the Ridgeway Working Group on Preemptive and Preventive Military Intervention, Ridgeway Center, Graduate School of Public and International Affairs, University of Pittsburgh. October, 2006, 2, http://www.au.af.mil/au/awc/awcgate/mcnair41/41sum.htm (accessed November 15, 2008).

12. Richard L. Russell, "The Weakest Link: Intelligence for Preemptive and Preventive Military Action," in *Rethinking the Principles of War*, ed. Anthony D. McIvor (Annapolis, MD: Naval Institute Press, 2007), http://books.google.com/books?id=zvUAXd18pJkC&pg=PA456&lpg=PA456&dq=richard+russell,+the+weakest+link&source=web&ots=Nx1IYIu-Eu&sig=ga5QlxlbuZ67XXGP99dySdKc0Bs&hl=en&sa=X&oi=book_result&resnum=1&ct=result#PPA456,M1 (accessed November 15, 2008).

13. Gregory F. Treverton, "Intelligence: The Achilles Heel of the Bush Doctrine," *Arms Control Today*, July/August 2003, http://www.armscontrol.org/act/2003_07-08/treverton_julaug03 (accessed November 16, 2008).

14. Paul R. Pillar, "Intelligence, Policy and the War in Iraq," *Foreign Affairs*, March/April 2006, http://www.mtholyoke.edu/acad/intrel/bush/pillar.htm (accessed November 15, 2008).

15. Ibid.

16. Thielmann, "Intelligence in Preventive Military Strategy," 3.

17. Ibid., 5.

18. Ibid., 4.

19. Stealing the authority or merit of another is not so rare as one might assume. A person who acquires a badge and wears a uniform to impersonate a police officer does so, in many instances, in an attempt to exercise the lawful authority granted by the state to the legitimate officer. Impersonating a police officer is a criminal offense. In much the same way, society attaches a great deal of approbation to those persons who claim the merit of another, for example, those who wrongfully claim to have served in the military and, more egregiously, those who claim to have been awarded a military decoration for valor appropriate to themselves something that does not belong to them—namely, the merit earned by another.

20. "Another historical perspective to consider in any analysis is the exchange of words between Israeli PM Menachem Begin and U.S. Ambassador to Israel Sam Lewis immediately after the Osiraq mission. Those words are a mirror image of what is being said at the highest levels of the Israeli government today. Here is the text of that exchange:

USAMB Lewis: 'I have to tell you in all honesty that I suspect some people in the White House will be pretty furious about this. Your weaponry was procured from us under the Arms Export Act, for purposes of self-defense only.'

Menachem Begin: 'Self-defense? What greater act of self-defense could there be than to demolish Saddam Hussein's weapons of mass destruction, designed to bring Israel to its knees, kill our people, vaporize our infrastructure—in a word to destroy our nation, our country, our existence? Over these past months I've told you again and again, Sam, that either the US does something to stop that reactor, or we will have to.'" Sean Osborne, "An Analysis of Israel's Explicit Threat to Strike Iran," Northeast Intelligence Network, http://homelandsecurityus.com/?p=675#more-675 (accessed November 16, 2008)

21. John Grinspan, "Attack on Iraq's Nuke Plant," AmericanHeritage.com, June 7, 2006, http://www.americanheritage.com/places/articles/web/20060607-israel-iraq-nuclear-weapons-baghdad-saddam-hussein-alexander-haig-menachem-begin-osirak-preemptive-strike.shtml (accessed November 15, 2008).

22. Herbert Weissman and Steve Krosney, *The Islamic Bomb: The Threat to Israel and the Middle East* (New York: Times Books, 1981), 20.
23. Ibid.
24. Rodger W. Claire, *Raid on the Sun* (New York: Broadway Books, 2004), 42.
25. Ibid.
26. Grinspan, "Attack on Iraq's Nuke Plant."
27. Claire, *Raid on the Sun*, 54–60.
28. Ibid., 107.
29. Ibid., 97.
30. Ibid., 104.
31. Thielmann, "Intelligence in Preventive Military Strategy," 20.
32. Walzer, for one, has suggested that the deliberations leading up to the preventive use of armed force "is couched, I suppose, in strategic more than moral terms. But the decision is judged morally, and the expectation of that judgment, of the effects it will have in allied and neutral states and among one's people, is itself a strategic factor." *Just and Unjust Wars*, 75.
33. Gray, *Implications of Preemptive and Preventive War Doctrines*, 36.

Ralph L. DeFalco III's career in the intelligence community spans more than twenty-one years. He currently serves on the staff of the director of naval intelligence. A captain in the U.S. Navy's Reserve Intelligence Program, he has served on the OPNAV Staff, the Joint Staff, and at the Joint Intelligence Command, Headquarters, International Security and Assistance Force in Afghanistan. He is a graduate of the Joint Military Intelligence College and the Naval War College and subsequently joined its faculty as fleet professor of joint maritime operations.