Risk Management
in Irregular Warfare

Article by **Sal Artiaga**

July 11, 2026

Introduction

Irregular warfare has always required risk. There is no way around it. The practitioner who waits for perfect information, total political certainty, and zero exposure will usually wait forever. The environment does not allow it. Irregular warfare lives in the space between war and peace, legality and ambiguity, visibility and deniability. It asks leaders to make decisions when the facts are incomplete and the consequences may not become clear for years. But there is an important difference between accepting risk and managing it. One is necessary. The other is professional. The first can produce bold action. The second determines whether that action becomes strategic success or a future scandal.

Risk management in irregular warfare is not simply about protecting personnel or avoiding casualties. It is about understanding political exposure, partner reliability, intelligence gaps, legal authorities, escalation dynamics, and the possibility that an operation may succeed tactically while damaging the larger campaign. In conventional conflict, commanders can often accept higher levels of risk because the political context is clearer. The enemy is identified. The legal authorities are broad. The public understands that force is being used. During peace, competition, or a gray-zone confrontation, the calculation becomes much more delicate. A small operation can create a disproportionate political crisis.

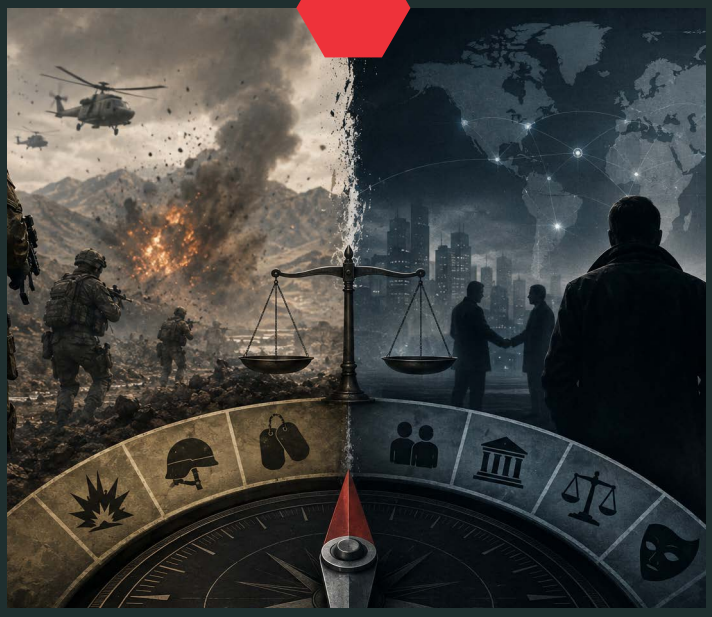
Risk Is Different in War Than in Competition

During armed conflict, the acceptable risk threshold changes. Commanders are expected to take risks because the alternative may be operational paralysis. In wartime, losses are understood as part of the cost of achieving military objectives. There is also a certain level of clarity. The adversary is known, the theater is defined, and military authorities are generally more expansive. That does not make wartime risk easy. It just makes it easier to justify.

During competition, the situation is far more fragile. The United States may be trying to influence a partner, support a resistance network, disrupt an adversary's political campaign, or collect intelligence in a sensitive environment. The operation may be small, but its exposure could trigger diplomatic backlash, undermine an ally, compromise sources, or create escalation nobody intended.

This is where irregular warfare becomes difficult. The risk is rarely just physical. It is reputational, strategic, legal, and political. The operation may need to remain deniable, but not so deniable that the partner believes it has been abandoned. It may need to create pressure, but not enough pressure to trigger a conventional response. This is the narrow path practitioners must walk.

Army risk doctrine describes risk as the probability and severity-driven chance of loss, requiring leaders to identify hazards, assess them, implement controls, and continuously supervise their effectiveness. That framework applies especially well to irregular warfare, though the hazards are broader than the traditional military checklist.



The Historical Logic of Calculated Risk

History is full of irregular warfare operations that succeeded because leaders accepted serious risk. It is also full of examples where the same appetite for risk became overconfidence.

The Jedburgh teams of World War II are a strong example of calculated wartime risk. Small multinational teams from the Office of Strategic Services, British Special Operations Executive, and Allied partners parachuted into occupied France, Belgium, and the Netherlands to coordinate resistance groups, guide sabotage, and support the Allied advance after D-Day.

These missions were dangerous by every measure. The teams operated behind enemy lines, relied on imperfect communications, and depended on local resistance networks that could be penetrated or destroyed. But the broader context mattered. Europe was already at war. The strategic objective was clear. The Allies were moving toward a decisive conventional campaign, and resistance activity could directly delay German movement and complicate their response. The risk was high, but it was connected to a larger campaign. That is the difference.

Contrast that with operations conducted in ambiguous political environments. Support to the Afghan mujahideen during the Soviet-Afghan War created military pressure on the Soviet Union and contributed to the broader cost of occupation. The transfer of Stinger missiles, for example, increased the risk to Soviet aviation and boosted morale among Afghan resistance forces. The CIA's own historical account notes that Soviet losses mounted and that Moscow eventually concluded the war was not worth the cost.

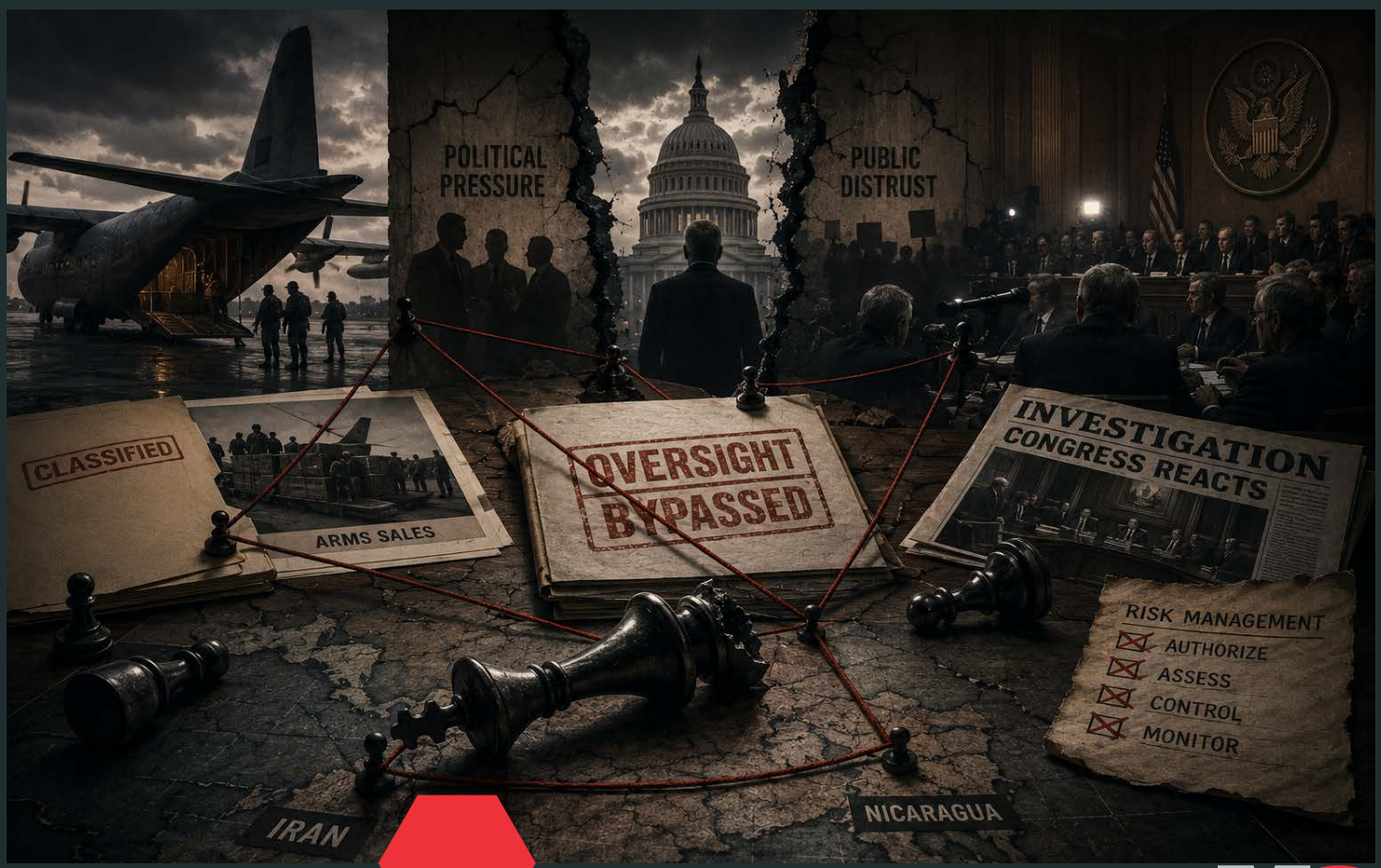
But the long-term risk was harder to control. External support moved through intermediaries. Local factions had different goals. The political environment was fragmented. Once the immediate strategic purpose changed, the networks built during the conflict did not simply disappear. This is the recurring challenge in irregular warfare. A partner can be useful today and dangerous tomorrow. Risk management must account not only for the operation but for the aftermath.

When Risk Management Fails

The Iran-Contra affair remains one of the clearest examples of risk management collapsing under political pressure. The issue was not simply that the operation was sensitive. Sensitive operations are often necessary.

The problem was that authorities, oversight, and strategic logic became disconnected. Funds from arms sales to Iran were diverted to support the Contras in Nicaragua, creating legal and political consequences that ultimately led to congressional investigations, public distrust, and significant institutional damage.

The lesson is not that covert or irregular activities should never be conducted. The lesson is that risk cannot be managed informally. When leaders convince themselves that urgency justifies bypassing oversight, the operation may become tactically clever but strategically reckless.



In irregular warfare, shortcuts are usually expensive. They may not appear expensive immediately. The bill arrives later, often in the form of political scandal, damaged alliances, compromised legitimacy, or a partner force that no longer trusts the relationship.

Why Modern Operations Are Harder to Execute

Many historical irregular warfare operations would be far more difficult to conduct today. The modern operating environment is saturated with cameras, commercial satellites, biometric systems, cellular metadata, social media, and open-source investigators. An insertion that might have remained hidden in 1944 could now be visible to commercial satellite providers, local surveillance systems, and citizen journalists within minutes.

The democratization of drones, cyber capabilities, and influence tools has made irregular warfare more accessible, but it has also made operational security more difficult. Recent Army analysis on Ukraine highlights how drones, cyber tools, and influence operations have become widely available to ordinary citizens and smaller actors, fundamentally changing how irregular activity can be conducted and observed.

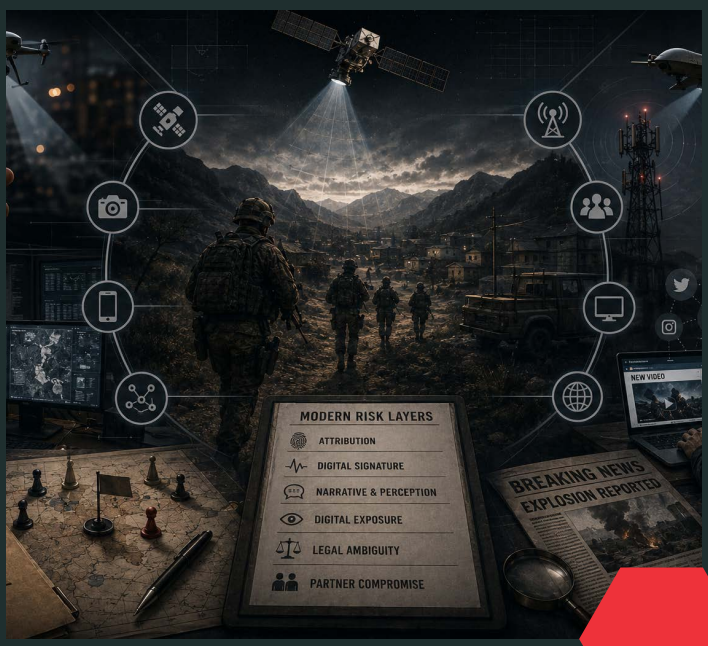
This means that risk management today must include a new set of questions. What is the digital signature of the operation? What commercial data could reveal it? What narrative will emerge if images surface online? Can an adversary manipulate evidence, create synthetic media, or turn a minor incident into a strategic communication defeat?

The old risk categories remain. Personnel. Equipment. Weather. Logistics. But now there are additional layers, such as attribution, narrative, digital exposure, legal ambiguity, and partner compromise.

Risk Management as a Leadership Function

Risk management is often treated as a process. A worksheet. A matrix. A briefing slide. In irregular warfare, it must be more than that. It has to become a leadership habit. The best leaders are not the ones who avoid every risk. They are the ones who understand which risks are worth taking and which are being accepted only because someone wants speed, prestige, or a short-term win. They know that an operation can be technically feasible and strategically foolish at the same time.

They also understand that risk changes over time. A mission that is acceptable during active conflict may be unacceptable during competition. A partner force that is reliable during a crisis may become a liability when political conditions shift. A tool that works quietly one year may become impossible to use the next because technology has changed the exposure environment. This is why supervision matters. Risk management is not completed when the operation begins. It continues through execution, through assessment, and through the political consequences that follow.



Conclusion

Irregular warfare will always require risk because it operates where certainty is scarce and the stakes are often hidden. But risk without discipline becomes recklessness, and recklessness has destroyed more campaigns than enemy action ever could. During armed conflict, leaders may have more room to accept risk because the political environment is clearer and the operational need is urgent. During peace and competition, the margin is smaller. A single exposed operation can damage alliances, trigger escalation, or undermine the legitimacy that irregular warfare depends upon.

The historical record is clear. The Jedburgh teams show that high-risk operations can succeed when linked to a coherent campaign. Afghanistan shows that support to partners can create effects that outlive the original objective. Iran-Contra shows what happens when urgency and secrecy overpower authority and judgment. The future will be even more demanding. Technology has made operations easier to observe, harder to deny, and faster to exploit. The practitioner who understands this will not become timid. They will become more disciplined. That is the real purpose of risk management in irregular warfare. Not to eliminate danger, but to ensure that when danger is accepted, it serves something larger than the operation itself.