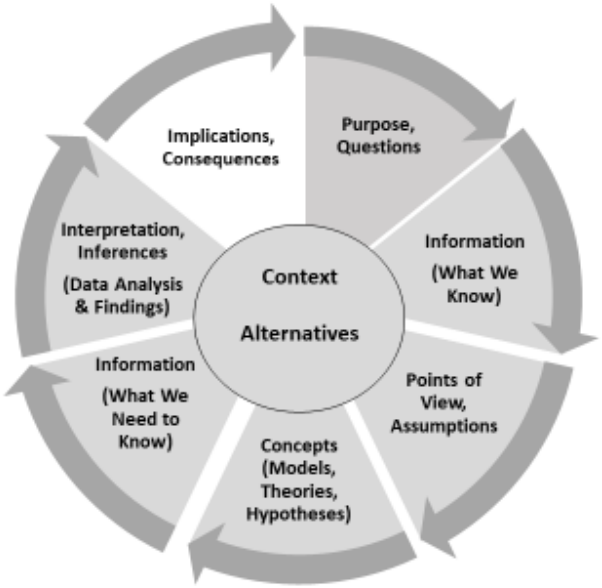
Chapter 10
Implications and Consequences



Security Analysis Critical-Thinking Framework

Bottom Line Up Front

A critical-thinking project is finalized by addressing the implications and consequences of the previously completed analysis. Results of the interpretation and inference analysis produce contentions (theses, key findings, conclusions, or recommendations), which imply certain conditions or actions. Implications indicate related behaviors, decisions, or conditions generated by the analytic results. Consequences occur when the implied behaviors, decisions, or conditions are acted upon. Cascading threat analyses are a common method to assess implications and consequences. In security analysis, there are two special cases of implications and consequences. First, in support of an intelligence threat analysis, a warning analysis is generated to update decision makers on the likelihood of adversaries' actions. Second, security policy analysts must "market or sell" their recommended policy actions to decision makers. In these cases, several

management-based techniques may be employed to increase the likelihood the recommended actions will be approved and acted upon.

Role of Implications and Consequences

Implications and **consequences** are the final elements addressed in a critical-thinking projects. The elements follow the previous critical-thinking efforts and are a check on the practicality of the analytic results. Implications claim or imply a related behavior, decision, or condition generated by the previous results.[1] They also address ideas because they directly or indirectly indicate, allude, hint, suggest, intimate, or entail beliefs, assumptions, or viewpoints resulting from the thinking. For example, if a state is assessed as a strong democracy, it implies that the state's political power resides in the people (citizens) and not in a powerful minority. There are three general types of implications: possible, probable, and necessary (certain).[2] A possible implication is one that may not be expected but still has a slight probability of occurring. For example, a recurring military patrol along a contested international border would not be expected to cause a violent conflict, but it is possible a conflict may occur. A probable implication may be expected, and thus has an increased probability of occurring. If the military patrol purposely fires across the border, then a conflict probably could be expected. A necessary implication is all but certain (near 100% probability) to result in either a positive or negative consequence. When the military patrol crosses the border and engages the adversary's forces, conflict will almost certainly follow.

Consequences, on the other hand, are the result of actions flowing from the implications. Thinking through the implications of a situation may lead to **positive consequences** that solve the problem or otherwise support the purpose of the analysis. Failure to think through the implications may result in negative or **unintended consequences** that work against the interests of the customer who requested the analysis.[3] Consequences flowing from implications result in behaviors, decisions, or conditions that are acted upon. For example, if a state

takes action to become a democracy, it can expect the positive consequences to include fair voting for societal leaders, less conflict and violence, and an improved quality of life for citizens. Consequences, either positive or negative, are thus what really happens and foster a series of outcomes. In the military patrol examples above, if conflict along the international border were to occur, the negative consequences could be a war between the adversarial states, loss of thousands of military and civilian lives, significant property destruction, and possible escalation into a regional war. Once the implications and consequences of a situation are understood, security analysis customers can decide if certain positive consequences are desired or if they can devise actions to mitigate the effects of negative or unintended consequences.

The remainder of this chapter addresses implications and consequences related to security analyses. Cascading threat analyses provide a basic process for assessing implications and consequences in most security analyses. Security analysis also has two specific areas that require expansion of basic implication and consequence analysis. First, in intelligence threat analyses, implications and consequences relate to predictive threat scenarios—the most probable threat scenarios adversaries may choose to pursue. This chapter presents a warning analysis structure to continually update an initial threat analysis, thus allowing customers to take mitigation actions. Second, security policy analysts must consider the acceptance of a policy recommendation (who will support or not support the recommendation) and the implementation of a policy recommendation to determine its cost and feasibility. The final section of this chapter discusses techniques for assessing acceptance and implementation of policy recommendations.

Cascading Threat Analysis

Cascading threat modeling is used in a number of security areas, including emergency management, infrastructure protection, cyber security, and more. This

type of modeling is particularly applicable to risk assessment, where the models help in assessing threats, vulnerabilities, and consequences. Cascading threat analyses take a systems approach (Chapter 7), which considers natural systems (earthquakes, hurricanes, wildfires, floods, etc.) and how they interact with man-made systems (communications, transportation, electrical, water systems, etc.). For example, hurricanes may damage electrical, communication, and transportation systems, while also causing property damage and flooding that affects the livability of homes and businesses.[4]

Cascading threat models assume a disaster or other action will unleash a sequence of events—often resulting in a series of negative consequences. "Toppling dominoes" is a good metaphor to visualize a series of sequential events. Lines of dominoes standing on end will topple if one end domino falls contacting and felling the next, which contacts and fells the next, and so on. The dominoes, or sequence of events, may be arrayed in one long line or may have side-branches, much the same as sequential events occur in the real world. Scenarios with a long sequence of events have individual parts that often are referred to as first order, second order, third order, etc., consequences.

Techniques for conducting cascading threat modeling are listed below. Box 10.1 provides a sample modeling effort.

> *Step 1*: After completing the interpretation and inference analysis (Chapter 9), assess implications and consequences of resultant contentions starting with a group-informed-brainstorming effort (Chapter 8). List and address every contention generated by the interpretation and inference analysis. The informed brainstorming should be supported by historic inputs from past research on similar cases, generic inputs from group members with experience in the field, and creative-thinking inputs (Chapter 8). Focus on using both divergent and convergent techniques to develop a list of implications and consequences for each contention.

Step 2: Create a set of events trees (Chapter 7) that list the contentions being assessed followed by their implications and related consequences. As an events tree unfolds, continue the informed brainstorming to refine the list of implications and consequences.

Step 3: Assess insights from the events trees and design mitigations for each negative or unintended consequence for the contention selected for action.

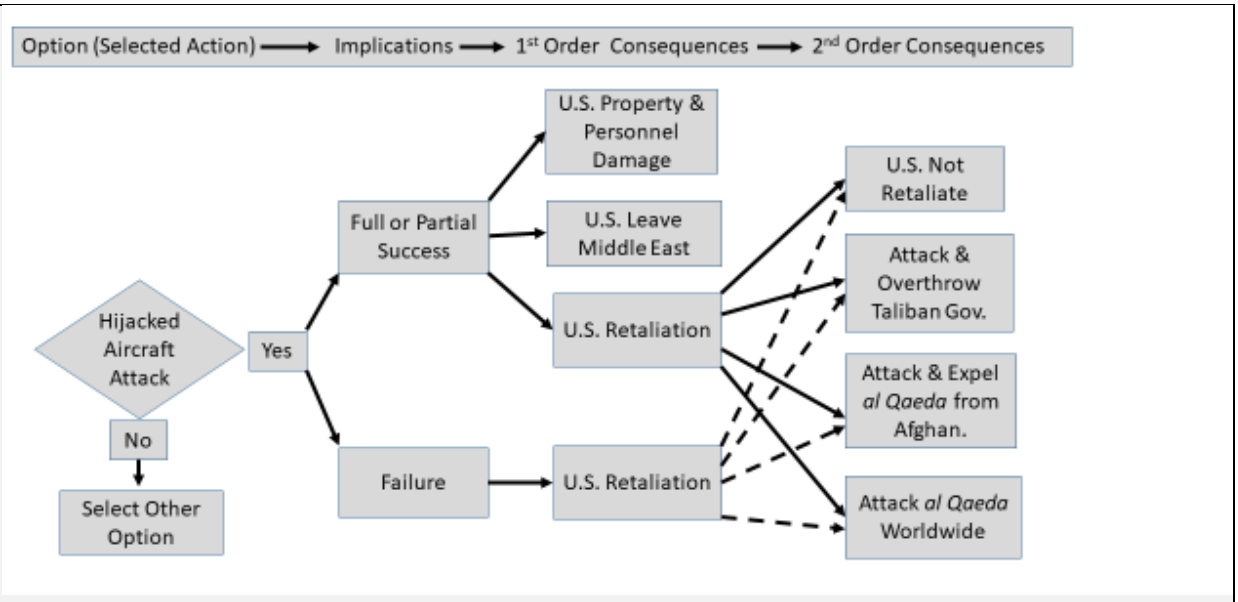
Box 10.1 Cascading Threat Model: *Al Qaeda* 9/11 Attacks

Perspective: *Al Qaeda*

Presume that *al Qaeda* returns to its initial storyboard planning (see Box 8.1) to assess the implications and consequences of its preferred decision to mount suicide attacks on the U.S. homeland with hijacked aircraft employed as missiles. As Box 8.1 describes, it appears *al Qaeda* did not conduct such an analysis. Below are the hypothetical results if they had done so.

Step 1: Select contention(s) for assessment. In this example, the contention (or decision) was to mount suicide attacks using hijacked aircraft as missiles on the New York World Trade Center, Pentagon, and U.S. Capitol. This is the only contention assessed for this example.

Step 2: Create an events tree for the contention of a hijacked-aircraft attack on U.S. homeland targets.



Step 3: *Al Qaeda's* insights from their perspective would include that hijacked-aircraft attacks on the U.S. homeland would either be a full success, partial success, or failure. *Al Qaeda* already assumed the suicide attack would kill their operatives, so this consequence is not shown on the above events tree. A 1st order consequence would indicate a full or partial success would result in U.S. property and personnel damage (amount depending on level of success). *Al Qaeda* also assumed a full or partial success might convince the U.S. to leave the Middle East. While this was *al Qaeda's* primary motive, this consequence did not come about. Also, *al Qaeda* should have considered U.S. retaliation for the attack. The 2nd order consequences reveal there was a small probability the U.S. would not retaliate, supported by the fact there was no U.S. retaliation for the *USS Cole* attack in October 2000, *al Qaeda's* last major attack on U.S. interests before September 11, 2001 (9/11). Instead, the U.S. retaliated for the 9/11 attack by forcibly overthrowing Afghanistan's Taliban government, attacking and expelling *al Qaeda* from its safe havens in Afghanistan, and beginning a worldwide campaign against *al Qaeda.* This campaign, known as "The War on Terror," focused an extensive U.S. intelligence effort to locate *al Qaeda* operatives, who were then attacked by U.S. forces. Captured *al Qaeda*

personnel were sent to the U.S. military detention camp in Guantanamo Bay, Cuba. In May 2011, this worldwide campaign against *al Qaeda* culminated in the death of *al Qaeda* leader Osama bin Laden by U.S. special forces in Pakistan. The implication of the 9/11 attack being a failure also could have resulted in U.S. retaliation, but possibly at a lower level of intensity (dashed lines in event tree) than for an attack deemed a full or partial success.

Al Qaeda actions indicate their leadership was not ready to take mitigation actions if the U.S. retaliated—a major flaw in their attack plan. It appears the opportunity to make a "spectacular" attack on the U.S. homeland, and their wishful thinking concerning how this would convince the U.S. to leave the Middle East, overcame their considerations of the risk involved in a U.S. retaliation. The above events tree could be extended further to third order, fourth order, etc., consequences based on the U.S. retaliation plan against the Taliban and *al Qaeda* in Afghanistan and against *al Qaeda* worldwide. It appears that *al Qaeda* had not considered the full implications and consequences of attacking the U.S. homeland.

Warning Analysis

Sometimes called warning intelligence or indications intelligence, **warning analysis** is a method used by intelligence analysts to update customers (policy makers or tactical commanders) as changes occur in their threat analyses. The main function of warning analysis is to anticipate—insofar as intelligence collection and analysis will allow—what the adversary is likely to do, especially whether adversaries are preparing to initiate action in the foreseeable future.[5] Intelligence threat analyses usually present more than one potential action or scenario an adversary may choose and estimate which of these actions or scenarios are the most likely to occur. This is accomplished by assessing

probabilities that a scenario may take place—but it is impossible to know exactly which will occur.[6] This type of analysis starts with the interpretation and inference element of a threat analysis and allows analysts to revise their original likelihood estimates to hopefully avoid any surprise actions by the adversary; avoiding surprise is a primary goal of security policy makers and tactical commanders. For a more in-depth understanding of warning analysis, see U.S. intelligence analyst Cynthia Grabo's seminal work, *Handbook of Warning Intelligence*.[7]

Warning analysis may be strategic or tactical, which differ in terms of timeliness and resources. Strategic warning is usually longer-term and provides warning of potential actions of an adversary requiring a response with the significant reallocation of resources. Tactical warning is more short-term and provides warning of potential actions of an adversary normally requiring a response with existing resources. Strategic warnings often address complex "wicked problems," which also are considered **low-probability/high-impact events**—meaning the probability of an adversary's actions may be low; but, if the actions did occur, there would likely be significant political, military, or economic consequences. For example, monitoring for a North Korean invasion of South Korea is a strategic warning situation classified as a low-probability/high-impact event. Short-term tactical warning is most applicable to tactical field commanders and supports allocation of existing friendly forces in reaction to an adversary's actions. Watching for an anticipated terrorist attack entails tactical warning, which often is confused with current intelligence analysis. Tactical warning analysis focuses on a specific problem and the related intelligence indications of an adversary's potential actions. Current intelligence looks at the latest information, and analysts try to make sense of the information and keep policy makers and tactical commanders informed. Current intelligence often addresses situations where a warning analysis does not exist.

Both strategic and tactical intelligence rely on robust intelligence analysis as described in this book. Warning analysts must have an in-depth knowledge of the adversary and use all the tools in their analytic "tool box" (critical-thinking and

analytic techniques) to anticipate the adversary's most likely future actions. With the initial results of their threat analysis, normally with more than one potential action or scenario the adversary may pursue, the analyst then develops an *indicators analysis* to identify potential observable factors pointing to the likely action of the adversary. That analysis is used to create a focused *intelligence plan* to collect and identify information on the observable indicators and allow revisions to the original threat analysis (see below). With a continually revised threat analysis and associated indicators analysis, security policy makers and tactical field commanders can reallocate resources and identify mitigation actions in reaction to the adversary.

When a focused warning analysis is required, it is usually referred to as an **Indications and Warning (I&W) Problem.** There are dozens of existing I&W problems in the security community; including the North Korean invasion of South Korea, China's invasion of Taiwan, and Iranian attacks on Saudi Arabia. The remainder of this section presents the steps to develop an I&W problem using the lead-up to the September 11, 2001 (9/11), *al Qaeda* attacks on the U.S. homeland as an example. This is a case where it appears a U.S. I&W problem was not established, and the case was handled as current intelligence analysis.

Step 1: Establish the **threat analysis** from the interpretation and inference element (Chapter 9). Using the analytic techniques presented herein, or more advanced techniques, establish a threat analysis for the situation. That analysis usually will result in a number of actions or scenarios the adversary may take. It is up to the analysts to rank order the threat actions or scenarios based on their likelihood to be selected by the adversary. The priority ranking may entail a simple pair-wise comparison (see Figure 9.5), a weighted ranking analysis (see Box 9.2), a CARVER analysis (see Box 8.2), a matrix analysis, or a subjective assessment of the information available in the situation.

Box 10.2 Threat Analysis: *Al Qaeda* Attack on the U.S. Homeland

Perspective: United States

Time Period: As of July 2001

By late-June and early-July 2001, the U.S. Intelligence Community (IC) had received increasing information regarding a significant *al Qaeda* attack on U.S. interests. Central Intelligence Agency (CIA) Director George Tenet described this information as "the system blinking red." There were conflicting conclusions about where and how the attacks would take place. The CIA's Counterterrorism Center (CTC) estimated the attack(s) likely would be on U.S. interests in Israel and Saudi Arabia. The Federal Bureau of Investigations (FBI) put little credence in a potential terrorist attack on the U.S. homeland. It was not until late-July 2001 that CTC acknowledged the attacks might take place on the U.S. homeland. Director Tenet was working closely with U.S. National Security Advisor for Counterterrorism (NSAC) Richard Clarke on the possibility of *al Qaeda* attacks. NSAC Clarke concluded in early-2001 that the attacks could be against the U.S. homeland. Despite the efforts of Director Tenet and NSAC Clarke (both remaining in their respective positions from the previous Clinton administration), their warnings of near-term *al Qaeda* attacks on the U.S. homeland gained little interest in the White House by the new Bush administration, in the Department of Defense (DOD), or at the FBI.

Assessing where *al Qaeda* might attack U.S. interests first requires consideration of whether the attacks would be on the U.S. homeland or overseas. Before 9/11, *al Qaeda* attacks on U.S. interests were mainly overseas, with the lone exception being the 1993 New York World Trade Center truck bombing. Overseas attacks included U.S. military facilities (Khobar Towers, *USS Cole*) and political facilities (U.S. embassies). Additional attacks overseas likely

would also target U.S. military and political facilities. Identifying potential facilities for an *al Qaeda* attack on the U.S. homeland is complicated by the hundreds of U.S. political, military, financial, and infrastructure targets, in addition to targets meaningful to U.S. citizens such as monuments, sporting events, or other key cultural sites and events. In 2001, there were few counterterrorism-related security measures in place across the United States, with the exception of security barriers to keep potential truck bombs away from important buildings. In his book *Keeping Us Safe*, Arthur Hulnick highlights that when it comes to the U.S. homeland, it is impossible to defend every possible terrorist target all the time.[8]

This threat analysis assumes that U.S. analysts modeled the perspective of *al Qaeda* by placing themselves in the shoes of the *al Qaeda* planners (see Box 8.1, Figure 8.3, Box 8.2, Box 9.1, and Box 9.2). The modeling of the *al Qaeda* perspective; however, would not reveal the exact decisions made by *al Qaeda* leadership; in particular, specific U.S. facilities that might be targeted. By July 2001, the challenge for U.S. analysts was to answer two main questions: (1) What likely type of attack will *al Qaeda* attempt? And (2) What targets will *al Qaeda* likely attack? The key to answering these questions was to assess the capabilities and intentions of *al Qaeda*. In the lead-up to the 9/11 attacks there was information on the capabilities of *al Qaeda* but little verifiable information on their intentions. After completing their *al Qaeda* perspective analysis and conducting a complimentary CARVER risk analysis assessing both the types of attack and the targets most likely to be attacked, U.S. analysts would construct a matrix analysis (Chapter 9); specifically, an **Analysis of Competing Hypotheses (ACH)**[9] shown below, that would assess *al Qaeda's* likely actions if the attacks were to be mounted in the United States.

The ACH below example is based on what U.S. analysts knew—or should have known—by July 2001, if agencies had been sharing information. It was known

that *al Qaeda* was experienced at vehicle (truck, boat) bombings. The aircraft hijacking attacks only were suspected from communications intercepts and informant reporting of how *al Qaeda* operatives were being trained in aircraft hijackings, which generated speculation of what they intended to do with the aircraft. This information was not verifiable, although there were verifiable reports of Middle Easterners being trained in U.S. flight schools. Surface-to-air missile attacks were suspected only from unverified information that *al Qaeda* possessed this capability, but there were no such attacks by *al Qaeda* since the end of the Soviet occupation of Afghanistan. The target designations listed below would have been developed from an *al Qaeda*-perspective CARVER analysis, plus the counterfactual knowledge of where the actual attacks took place. This is a counterfactual analysis; that is, the final outcome is known. What we know now is that before 9/11, the New York World Trade Center (a 1993 al Qaeda failed bombing target), the Pentagon, and U.S. Capitol should have been priority targets for this threat analysis.

Potential attack scenarios (hypotheses) resulting from the in-depth analysis of the *al Qaeda* threat to the U.S. homeland (based on what was known in July 2001):

Scenario 1 (S1): Priority structural facilities with truck bombs.
Scenario 2 (S2): Priority structural facilities with hijacked aircraft used as missiles.
Scenario 3 (S3): Commercial aircraft hijacked and crew/passengers held hostage for exchange of *al Qaeda* prisoners.
Scenario 4 (S4): Transportation facilities with chemical, biological, or radiological attacks.
Scenario 5 (S5): Passenger aircraft shot down using surface-to-air missiles.

Analysis of Competing Hypotheses: Al Qaeda Terrorist Attack on the U.S. Homeland

Evidence or Assumptions	S1	S2	S3	S4	S5
Meets *al Qaeda* goals to attack U.S. interests (per media reporting from announcements and interviews of bin Laden & assumptions)	CC	CC	CC	C	C
Meets bin Laden's goal of a "spectacular" attack at the heart of the United States (media reporting)	C	CC	I	I	II
Known or suspected (assumed) *al Qaeda* attack capabilities	CC	C	C	I	C
Known *al Qaeda* command & control capabilities	CC	C	C	C	C
Known or suspected *al Qaeda* information, surveillance, and reconnaissance capabilities	CC	C	C	C	C
Known *al Qaeda* logistics capabilities (support of operatives, move weapons/explosives into U.S, etc.)	CC	C	C	I	I
ACH Results: Number of inconsistencies	0	0	1	3	3
Al Qaeda Perspective CARVER Results	3	1/2	4	5	6
Estimated Likelihood of Attack	L	L	EC	VU	U

Legend: Scenarios rated for consistency or inconsistency with evidence or assumption: C = consistent, CC = very consistent, I = inconsistent (1 point), II = very inconsistent (2 points)

Based on the ACH results (assessing scenarios with least inconsistencies) and CARVER results (how *al Qaeda* might rate the scenarios) and the totality of information available, the analyst estimates the relative likelihood of each scenario taking place. Likelihood estimates might become more precise as additional information is collected. This estimate of a scenario taking place may be expressed in odds or its corresponding probability. For example, odds of 3-1 of the attack scenario taking place are equal to a 75% probability of the scenario taking place. Likelihood also may be expressed in verbal statements (unlikely, very likely, etc.), which often are better understood by analytic customers. Likelihood ratings, assuming each scenario is a mutually exclusive event, may include:[10]

Likelihood rating	NC	VU	U	EC	L	VL	AC
Verbal statements of likelihood	almost no chance	very unlikely	unlikely	roughly even chance	likely	very likely	almost certain
Numeric probability	01-05%	05-20%	20-45%	45-55%	55-80%	80-95%	95-99%

Findings: The overall threat analysis indicates a truck bombing or attack by a hijacked aircraft used as a missile on U.S. structural targets were the most likely scenarios for a foreign terrorist attack on the U.S homeland. Scenarios 3 to 5; however, could not be completely discounted and must be included in Step 2 below.

Step 2: Develop an **indicators analysis**. This type of analysis establishes an **indicators list** and then correlates the indicators with potential threat scenarios the adversary is likely to mount. The indicators list allows the analyst to watch for mounting evidence in support of a particular threat scenario, such as target location and type of attack. Indicators instill rigor in the analytic process when analysts inform policymakers and tactical commanders that a threat is about to materialize. When an indicators list is included with a threat analysis, it demonstrates to the decision maker or tactical commander how the analysts will track new developments as they keep them informed. In providing indicators before a threat materializes, the analyst makes the assessment much more transparent and available for scrutiny. In his book *Intelligence and Surprise Attack*, Erik Dahl highlights situations where national leaders are given only strategic warning and not specific warning of threats (*how*, *where*, *when).* Lacking specific warning usually results in low decision maker receptivity to the threat, which increases the probability of a successful attack.[11] The indicators analysis technique entails:

- Identify the likely set of competing scenarios from the results of the ACH analysis above.
- Create separate lists of observable indicators for potential activities, statements, or events expected for each likely scenario.
- Regularly review and update the indicators list to assess any changes.
- Identify which scenarios are unfolding based on changes to items identified in the indicators list.

Indicator lists should concentrate on those activities or events that can be observed by available intelligence collectors. The indicators list will consist of items on threat **capabilities** (weapons types, weapon delivery methods, etc.) and the adversary's **intentions** to use those capabilities (weapon movements, training activities, statements of intent, changes in propaganda levels, etc.).[12] When addressing a threats to a fixed structure, a good place to start is developing an indicators list from the actions attackers might take to surveil and collect information on a target, as shown in Figure 10.1.

Figure 10.1 **Infrastructure Attack Potential Observables[13]**

Information on Avenues of Approach and Ease of Access

1. Location of the target.
    a. Surrounding terrain or buildings:
        - Maps
        - Blueprints
        - Types of building construction
        - Critical points
        - OCOKA (observation, cover and concealment; obstacles; key terrain, and avenues of approach).
    b. Available paths to target:

- Exact path(s) to take
- Go and no-go areas (because of barriers, obstructions, or impassable terrain)
- Areas of restricted or limited access (security restrictions)
- Rules or laws governing movement (vehicular and otherwise) in target area
- Traffic conditions (all relevant vehicular and pedestrian modes).

Information on Characteristics of the Target

1. Possible locations from which to launch the attack.
2. Possible times or windows of time to launch the attack.
3. Mobility and variability of the target; if mobile, the predictable paths it may take.
4. Relevant features and structure of the target; i.e., technical details.

Information on Protective Security Forces

1. Locations of headquarters, stations, and checkpoints.
2. Overall size and types (e.g., uniformed, plainclothes, canine):
    - Number on duty at any one time, hours of duty, and variation
    - Applicable operational jurisdictions
    - Capabilities
    - Vehicles and other mobile assets
    - Radio frequencies used (and other communications used)
    - Rules of engagement or use-of-force policy.
3. Specific or individual deployments:
    - Fixed positions
    - Patrols (e.g., routes, schedules, number of personnel, vehicles)
    - Times of observations (e.g., cameras, live operatives)

- Number of security personnel required to be “passed”
- Variations by times of day.

4. Security plans (e.g., operational details):
   - Security response plans
   - Past performance in previous (or similar) incidents
   - Behaviors, plans, and capabilities at different levels of alert
   - Response times.
5. Kinds of checkpoints to be passed:
   - Search procedures (e.g., What will officials be looking for or asking for?)
   - Cameras, scanners, and detection equipment in the area to be traversed
   - Sensitivity of detection devices
   - Frequency at which sensors are “read”
   - Illumination.
6. Specific countermeasures such as vehicle barriers.
7. Other people at the facility (Why are they there? What are they doing?):
   - Bystanders, recreational users of facility, passengers
   - Differences in population at different times of day
   - Vigilance instructions or emergency phones
   - Level of security training for non-security employees
   - Schedules of regular arrivals and departures from target area
   - Ease of camouflage as a member of one of these groups.

Information on Threats to the Attackers

1. Threat posed by security forces and law enforcement measures:
   - Deployments, response times, vehicles, equipment, and plans
   - Cascading information (from organizational oversight and HQ locations to who will be on the avenue of approach on attack

day)

- Estimated effectiveness of security response capabilities (including communications).

2. Threat posed by employees of the target.
3. Citizens (e.g., concentrations of, heightened vigilance of).
4. Weather as it affects effectiveness of the operation.

For threats that do not fit the Figure 10.1 framework, another technique to develop an indicators list is to conduct an informed-brainstorming **What If? Analysis.**[14] This type of analysis assumes the action or scenario will occur and then focuses on explaining how the event might occur. To conduct a What If? Analysis, the analyst or group of analysts should:

- Assume the action or scenario will happen or has happened.
- Determine what triggering events permitted the action or scenario to unfold to help make the What If? plausible. Triggering events could include: death of a leader, a political or economic event, a religious date of significance, the anniversary of a significant societal event, etc.—anything that could spark a change from the adversary planning an attack to actually carrying one out.
- Develop a chain of events based on a combination of logic and evidence to explain how the event could have occurred. Events trees (Chapter 7) are a good technique to employ. Figure 10.1 provides information to assist in developing an events tree for an infrastructure attack.
- "Think Backwards" from the event in concrete ways; that is, specify what must actually occur at each stage of the action or scenario.
- Identify one or more plausible pathways that lead to the action or scenario; often, more than one pathway will appear possible.

- Generate an indicators list or "observables" for each action or scenario that would help to detect its origins.
- Consider the scope of the positive and negative implications and consequences of the indicators list and their correlation to each action or scenario.

Box 10.3 provides an example of an indicators list and indicators analysis related to the Box 10.2 threat analysis results, based on a What If? Analysis.

Box 10.3 Indicators Analysis: *Al Qaeda* Attack on the U.S. Homeland

The Box 10.2 ACH provides only partial information needed by U.S. decision makers to counter an *al Qaeda* attack. In the *al Qaeda* case, the ACH threat analysis attempts to assess the *how* or type of attack. It only assesses the *where* in a general sense, as all the threat analysis scenarios could occur at hundreds of locations across the United States. To better assess the *where* and *when* in an I&W problem requires establishment of an indicators analysis that identifies those adversary activities associated with the potential types of attacks and locations of attacks that are observable by the U.S. intelligence collection system (Chapter 5). Based on the scenarios assessed in Box 10.2, the following indicators list can be established:[15]

1. Identification and location of potential *al Qaeda* operatives residing in the United States or arriving by legal means.
2. Travel of potential *al Qaeda* operatives inside the United States and overseas. *Remember*: prior to 9/11 the U.S. "no-fly" list did not exist.
3. Personal contacts by *al Qaeda* operatives residing in the United States.
4. Financial transactions of potential *al Qaeda* operatives inside the United States (bank accounts, credit cards, vehicle or housing leases, etc.).

5. Other transactions of potential *al Qaeda* operatives inside the United States (driver licenses, pilot licenses, education, training, religious activities, etc.).
6. Facility surveillance by *al Qaeda* operatives (per Figure 10.1).
7. Interest of potential *al Qaeda* operatives in aviation security or other aviation-related activities (surveillance of airports, etc.).
8. Evidence of potential *al Qaeda* operatives being smuggled illegally into the United States.
9. *Al Qaeda* operatives smuggling in or procurement of arms, ammunition, explosives, biological/chemical materials, or radiological materials.

The indicators list then would be turned into an indicators analysis matrix. Each indicator is assessed for applicability to each scenario analyzed in Box 10.2

Indicators Analysis: Foreign Terrorist Attack on the U.S. Homeland

Indicators	**S1**	**S2**	**S3**	**S4**	**S5**
1. *Al Qaeda* operatives in United States	X	X	X	X	X
2. *Al Qaeda* operative travel inside U.S. or overseas	X	X	X	X	X
3. Contacts between *al Qaeda* operatives	X	X	X	X	X
4. Financial transactions by *al Qaeda* operatives	X	X	X	X	X
5. Other transactions by *al Qaeda* operatives	X	X	X	X	X
6. Key facility surveillance by *al Qaeda* operatives	X	X		X	
7. Aviation security surveillance by *al Qaeda* operatives		X	X	X	X
8. Illegal smuggling of *al Qaeda* operatives into U.S.	X	X	X	X	X
9. Smuggling/procurement of weapons by *al Qaeda*	X		X	X	X

The above indicators analysis correlates the indicators list with the threat analysis scenarios (Box 10.2). In this case, the indicators are general in nature, and most of the indicators correlate to all the scenarios. Thus, if any indicator is observed, it would be difficult to determine which scenario is more likely to take place. What this analysis reveals is a concentrated U.S. law enforcement and corporate security effort within the United States to gain information on the above indicators, could lead to developing more specific information on the *how*, *where*, and *when* of a foreign terrorist attack on the U.S. homeland.

Step 3: Develop and activate a focused **intelligence collection plan**. Obtaining information on each of the items on an indicators list usually requires a coordinated interagency intelligence collection effort. Depending on the nature of the threat, this intelligence collection effort could be mounted inside the United States, overseas, or a combination of both. Analysts first should start with a broad plan of the intelligence collection requirements. From this requirements summary, analysts or dedicated intelligence collection managers, then would activate the necessary collection systems. The intelligence management actions could include adding the requirements to the IC standing requirements for recurring long-term collection, the shorter-term (minutes to days) time-sensitive requirements, or ad hoc collection requirements generated when a formal collection requirement does not exist or a one-time collection effort is required.[16] It is imperative that analysts provide the collectors the background on the threat, the full threat analysis, and specific collection actions required. This allows the collectors to tailor their efforts to obtain and report the desired information. Developing a focused interagency intelligence collection effort has the added advantage of informing the appropriate agencies of the priorities to be placed on the threat.

In addition to notifying federal agencies when a collection effort takes place inside the United States, it often requires the support of state and local law enforcement agencies. At times, support of corporate security officials also is required. The vast majority of the U.S. critical infrastructure is owned by businesses and corporations that employ thousands of their own security personnel. There are several considerations when soliciting intelligence collection support from other than federal agencies. First, any supporting documents or briefings will likely need to be declassified and provided to participating agencies. Second, depending on the nature of the threat, the analyst should ask several questions:

- Should the owners of the locations of the most likely attacks be informed of the threat?
- Should the supervisors and workers at the locations of the most likely attacks be informed of the threat and asked to assist in the data collection efforts?
- Should the general public be notified of the most likely attacks?
- Should the general public be asked to assist in the data collection efforts?

Box 10.4 presents an example of a broad intelligence collection plan resulting from the Box 10.3 indicators analysis.

Box 10.4 Intelligence Collection Plan: *Al Qaeda* Attack on U.S. Homeland

Intelligence Collection Plan

Period Covered: June to September 2001

Indicators for Focused Collection Effort	Location of Collection Effort (details attached as needed)	Agencies/Platforms Tasked for Collection Effort
1. *Al Qaeda* operatives in United States (arriving or already in U.S.)	U.S. Borders and internal locations nationwide to include U.S. Ports of Entry and areas between Ports	U.S. Immigration & Naturalization Service (INS), Border Patrol (BP), U.S. Customs Service (USCS), FBI, State/Local Police
2. *Al Qaeda* operative travel inside U.S. or overseas	Worldwide	FAA, FBI, CIA, NSA, State/Local Police
3. Contacts between *al Qaeda* operatives	Worldwide	NSA, FBI, CIA, State/Local Police
4. Financial transactions by *al Qaeda* operatives	Worldwide	Department of Treasury, FBI, NSA, CIA, U.S. Secret Service (USSS)
5. Other transactions by *al Qaeda* operatives (enrollment in aviation	Nationwide in U.S.	FBI, State/Local Police

training programs, obtaining drivers licenses, renting housing, renting vehicles, visiting public weapons ranges, etc.)		
6. Facility surveillance by *al Qaeda* operatives	Nationwide in U.S.	Federal Protective Service (FPS), National Park Service (NPS), State/Local Police, Corporate Security
7. Aviation security surveillance by *al Qaeda* operatives	Nationwide in U.S.	FAA, Corporate Security at Airports
8. Illegal smuggling of *al Qaeda* operatives into U.S.	Nationwide in U.S., with main focus at U.S. Borders	BP, USCS, INS, U.S. Coast Guard, State/Local Police
9. Smuggling/procurement of weapons by *al Qaeda*	Nationwide in U.S.	Alcohol, Tobacco, Firearms, (& Explosives) (ATF), BP, USCS, U.S. Coast Guard, State/Local Police

Unfortunately, there appeared to be no focused intelligence collection plan as shown above for potential *al Qaeda* attacks on the U.S. homeland prior to the 9/11 attacks in 2001. It appears there was also no ACH threat analysis (Box 10.2) and no indicators analysis (Box 10.3). Instead, the IC appeared to handle the *al Qaeda* threat to the U.S. homeland as a current intelligence effort, waiting for new information to become available through normal intelligence collection and analytic sources. U.S. decision makers were given little more than broad strategic analysis on the *al Qaeda* threat and not the specific threat information (*how*, *where*, *when*) to spark decision maker action and increase intelligence collection and protective security measures. This largely explains why the *al Qaeda* 9/11 attacks were not prevented.

Likely unknowingly, *Al Qaeda* exploited a seam where U.S. foreign and domestic intelligence standard operating procedures conflicted.[17] The rules, routines, and repertoires of the CIA, responsible for U.S. foreign intelligence; and the FBI,

responsible for U.S. domestic intelligence; created almost impenetrable walls between U.S. foreign and domestic intelligence over the 50-plus-year history of the IC (see Figure 1.1). While there was limited cooperation between the CIA and FBI prior to 9/11, this foreign-domestic intelligence wall precluded sharing significant amounts of information. Thus, no one agency had all the pertinent information to "connect-the-dots." Additionally, without a focused intelligence collection plan, there were numerous missing "dots."

As the lead federal law enforcement agency, the FBI's intelligence functions prior to 9/11 focused on investigating crimes, apprehending criminals, and obtaining convictions. While counterterrorism was an FBI mission prior to 9/11, few resources were dedicated to this mission in the Clinton and early Bush administrations.[18] The FBI rules, routines, and repertoires bounded its actions into a criminal case file mentality (i.e., resources were not dedicated to cases where a federal crime had not been committed and lacked a good chance of an eventual conviction). Without any hard evidence that *al Qaeda* was about to strike the United States in the summer of 2001, the FBI showed little interest in investigating that possibility. After the 9/11 attacks, the House-Senate Joint Inquiry counted a total of 12 lost opportunities by U.S. government agencies where aggressive follow-up on a lead could have uncovered the 9/11 plot.[19] The CIA focused its collection and analysis activities outside the United States. CIA's mission was to inform and alert U.S. senior decision makers on foreign matters. Part of the alerting function is to warn decision makers of threats to U.S. interests. The CIA's Counterterrorism Center's (CTC) *al Qaeda* research section, which included FBI representatives, was focused on an overseas attack. In late-June 2001, as the CIA was focused on threats to U.S. interests overseas and the FBI was bounded by its criminal case file mentality, little attention was given to preventing *al Qaeda* attacks inside the United States.

In the months leading up to late-June 2001, the CTC staff, CIA Director Tenet, and NSAC Clarke and his staff kept in frequent contact as they followed the developing *al Qaeda* intelligence. During the first week of July 2001, NSAC Clarke convened the White House Counterterrorism Security Group (CSG) and asked each agency to consider itself on full alert. Clarke stated, "I asked the CSG agencies to cancel summer vacations and official travel for the counterterrorism response staffs. Each agency should report anything unusual…. I asked the FBI to send another warning to the 18,000 [U.S.] police departments, [Department of] State to alert the embassies, and Defense Department to go to Threat Condition Delta …. I asked the senior security officials at FAA, Immigration, Secret Service, Coast Guard, Customs and the Federal Protective Service to meet at the White House. I asked the FAA to send another security warning to the airlines and airports and requested special scrutiny at the ports of entry."[20]

NSAC Clarke's actions in the first week of July 2001 did not mobilize the U.S. government to any great extent. The FBI did notify law enforcement agencies of possible *al Qaeda* strikes overseas. The notification included the statement: "The FBI has no information indicating a credible threat of terrorist attack in the United States."[21] It added; however, that domestic strikes could not be ruled out.[22] Participants in the July CSG meeting at the White House with NSAC Clarke reported they were asked to take the information back to their home agencies and "do what you can" with it.[23] An Immigration and Naturalization Service (INS) representative at the meeting asked for a summary of the information that could be shared with INS field offices, but the summary was never provided.[24] Although NSAC Clarke made a well-intentioned attempt to mobilize the U.S. government to detect and prevent a potential attack, it was not successful domestically because Clarke did not convince agencies to change much in the way of their existing intelligence data collection and security protocols—changes that would have required Presidential or at least Cabinet-level direction.

In accordance with the above hypothetical ACH threat analysis, indicators analysis, and intelligence collection plan, conducting these analyses, combined with a mobilization of U.S. federal, state, and local agencies in early-July 2001, could have averted the al Qaeda attacks on 9/11.

Step 4: Update the threat analysis likelihoods for each scenario. As new information is revealed from the indicators analysis and corresponding intelligence collection plan efforts, the analyst must continually revisit the original threat analysis and update the original likelihood estimates, as appropriate. For example, from the Box 10.4 intelligence collection plan, if it had been found several potential *al Qaeda* operatives had enrolled in U.S. aviation training programs, it may have resulted in an increase in the likelihood estimate from likely to very likely for the Box 10.2 scenario 2 (possible attack of U.S. structural facilities with hijacked aircraft used as missiles). In fact, in summer 2001, two reports of aviation training enrollments by Middle Eastern males were reported to FBI headquarters, but both reports were discounted and further investigation not conducted. In these two reports, it was the 9/11 *al Qaeda* operatives being trained to fly—but not land—wide-body commercial aircraft in the training programs.

Bayesian analysis should be considered by analysts in revising estimated threat likelihoods (Chapter 7). There will seldom be sufficient information in a threat analysis to calculate precise numeric probabilities for use with Bayes' Theorem to update probabilities. Instead, the warning analyst becomes more like a casino card-counter, who uses new information to make an intuitive estimate of how the likelihood of specific scenarios change, allowing the card-counter to adjust their betting and playing strategy. While warning analysts primarily are generating subjective estimates of likelihood, these estimates still provide the customer the best assessment of what may be about to happen.

Warning analysts face the challenge of making estimates in highly complex situations, where information is usually incomplete, and with human adversaries often making unpredictable decisions. But the analysts still must provide decision makers the best estimates possible. The biggest failure in most warning analyses is when all the evidence available on the case is not examined closely; or, if an I&W problem is never established, as it appears was the situation in 9/11.

Policy-Marketing Analysis

Policy marketing refers to the "selling" of policy actions. Security policy analysts must develop a marketing plan to convince policy makers to adopt and support the policy recommendations resulting from the interpretation and inference element (Chapter 9) and implications and consequences element (this chapter). The consequences of not considering the needs and inclinations of policy makers could result in rejection of a recommended policy option. Policy analysts must keep in mind how the opportunities and limitations surrounding both politics and resources determine the acceptance or rejection of their recommendations. There may be resistance to changing existing policies, especially if the existing policies have been in place for a lengthy time and developed a strong supporting constituency. The ability of security analysts to present new or controversial material to policy makers is often called "speaking truth to power" and, when not handled properly, has been the downfall of many an analysis.[25] The key to marketing policy recommendations is to ensure the policy analysis is based on the latest intelligence analysis (even if the policy analyst also must act as the intelligence analyst); verify that the policy analysis is grounded in facts, logic, and reasoning; consider the politics and resources of the issue; and prepare verbal and written reports with strong arguments that support the recommendations.

Security policy analysis may involve single or multiple issues. A single-issue policy analysis usually is limited to one policy action and addresses a single goal,

including revising or implementing a new program to address a specific problem. A multi-issue policy analysis usually addresses a number of policy actions or programs with multiple goals, and is packaged under an overarching strategy. Security policy analysts face several major challenges in marketing their recommendations for both single-issue policies and multi-issue strategies. The challenges include:[26]

1. Assessing the tradeoffs posed when the goals of competing policies or strategies are incompatible.
2. Measuring the costs and effectiveness of policies and strategies when the actions recommended are so different that they are not easily compared.
3. Developing the program components—the action agenda—for policies and strategies in enough detail so policy makers know what they are approving and will support further planning and eventual implementation.

Below are three analytic techniques for assisting policy analysts to help ensure the policy analysis is complete and to develop sufficient details to convince policy makers to approve their recommendations—**How-How Analysis**, **SWOT Analysis** (Strengths, Weaknesses, Opportunities, Threats), and **Acceptance Analysis.** At times, the analyst may need only one or two of these techniques; at other times, all three techniques may be required. Depending on the policy analysis situation, these techniques provide systematic procedures for ensuring the analyst's briefing or written report contains sufficient details to obtain policy maker approval and/or support for recommended policies.

How-How analysis. The purpose of a How-How analysis is to generate initial steps toward planning and implementing recommended policy options. The How-How analysis begins with the results of the interpretation and inference element (Chapter 9) and completion of a cascading threat analysis (see above).

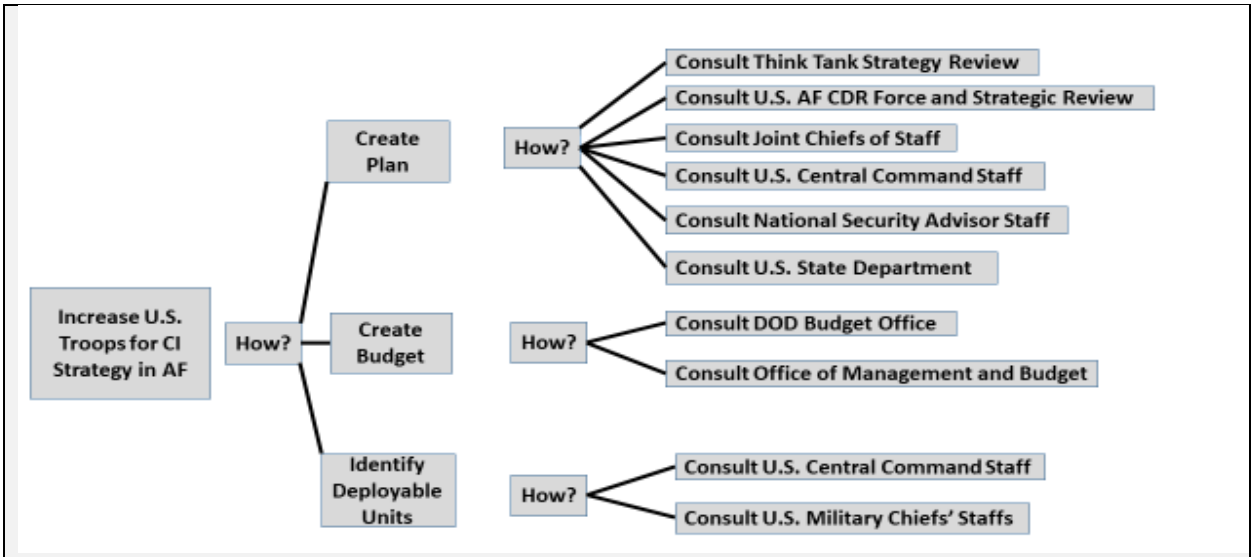
The technique follows a divergent-thinking approach to identify important general action steps. Depending on the situation, How-How analysis may be applied to the preferred, recommended policy option; several of the highest-priority options; or to all the policy options developed in the interpretation and inference element results. The goal is to develop detailed options for policy makers to approve one or more options. Once a recommended policy option is approved, the How-How analysis can be revisited to develop even more in-depth actions and activities for policy implementation. The How-How analysis proceeds as follows:

- Identify the recommended option.
- Ask the first "how" question and record responses.
- Ask "how' again and record responses.
- Continue to ask "how" questions until the level of required detail is achieved.[27]

To visualize a How-How analysis, an events tree diagram is provided in Box 10.5. This example is based on the outcome matrix analysis presented in Box 9.3 on President Obama's decision about troop deployments in the Afghanistan war.

Box 10.5 **How-How Analysis**: **Obama's War in Afghanistan**

Box 9.3 details the 2009 negotiations to decide on revised U.S. troop deployments in Afghanistan (AF). During these negotiations, the U.S. DOD offered the option of 45,000 additional troops with enablers (support units) to continue a counter-insurgency (CI) strategy. A How-How analysis could have been employed by DOD planners to develop this option.



From the above How-How analysis, DOD planners could generate the details of a plan to increase the number of U.S. troops in Afghanistan and pursue a CI strategy. Bob Woodward's book *Obama's Wars*[28] captures how much of the above planning took place. President Obama initiated an independent think tank review of U.S. strategy in Afghanistan in spring 2009. The U.S. Commander in Afghanistan completed a force review and second strategy review in late-summer and early-fall 2009. President Obama made his decision to increase troop deployments in Afghanistan on November 29, 2009. The main DOD actors in establishing the option for 45,000 troops plus enablers to conduct a CI strategy similar to the one successfully conducted earlier in the decade in Iraq were: Secretary of Defense, Joint Chiefs of Staff, U.S. Central Command, and the U.S. Commander in Afghanistan. Other actors in the above How-How analysis were peripheral to the DOD planning. The next step would be to take the details of an initial plan and place them through a SWOT analysis.

SWOT analysis. The strengths, weaknesses, opportunities, and threats (SWOT) analysis is a systematic assessment of a recommended option (policy, program, or strategy) and is widely used in government and corporate management circles.[29] Using their knowledge of the option under consideration,

combined with informed brainstorming, analysts develop a SWOT assessment for a recommended option. Strengths and weaknesses usually relate to the internal attributes of an option. Opportunities and threats usually relate to external conditions affecting the option.

The SWOT results should identify "**gold badges**" and "**red flags**." Gold badges are features of the option under assessment that would be attractive, necessary, or unavoidable; and would likely influence the policy maker to approve the option. Gold badges identify viable means to attain high-priority goals and protect vital interests. Red flags identify potential problems with the option, to include likely failure to achieve goals, payoffs too small, risks too high for the policy makers, or costs too high. Such red flags will usually result in the rejection of the option, irrespective of its strengths and opportunities.[30]

A SWOT analysis is facilitated through the use of a simple 2 X 2 matrix template as shown in Figure 10.2. Once the initial SWOT analysis is completed and gold badges and red flags identified, the policy analyst then may revise the option to make it more marketable to the policy makers.

Figure 10.2 SWOT Analysis Template[31]

Strengths	**Weaknesses**
List attributes of the option that are helpful in achieving the goal.	List attributes of the option that are detrimental to achieving the goal.
Opportunities	**Threats**
List external conditions that are helpful to achieving the goal.	List external conditions that could be detrimental to achieving the goal.

Box 10.6 provides an example of a SWOT analysis based on the Box 9.3 decisions surrounding President Obama's decision on troop deployments in the war in Afghanistan.

Box 10.6 SWOT Analysis: Obama's War in Afghanistan

During the 2009 decision process on increasing U.S. troops in Afghanistan, there were three main options considered (see Box 9.3 for more details):

Option 1: 10,000 additional troops to train the Afghan Security Forces (police and military). No additional U.S. combat troops.
Option 2: 30,000 additional troops plus up to 3,000 additional enablers. Troops would train Afghan Security Forces and conduct counterterrorism (CT) operations.
Option 3: 45,000 additional troops with unspecified number of enablers. Troops would train Afghan Security Forces and conduct CI operations.

Option 3 was created and supported by the U.S. DOD. This option is the subject of the below SWOT analysis.

Strengths	**Weaknesses** (All Red Flags)
• Trains Afghan Security Forces (Gold Badge). • Conducts CI similar to Afghanistan (DOD perspective).	• No plan to end war. • Not politically acceptable to U.S. Congress. • Cost was additional $10 billion per year (most of 3 options). • Does not send political message U.S. will not stay in AF long-term. • Does not address a primary CT mission with presidential support.
Opportunities	**Threats**
• Build size, capabilities, and combat experience of U.S. forces.	• May not be supported by President, National Security Advisor's staff, U.S. Congress, and public.

If DOD planners had completed a SWOT analysis, they would have found their option for 45,000 additional troops, plus enablers, likely would not be approved. All the weaknesses listed are red flags because the concerns of President Obama were not given necessary attention in the DOD option. The above SWOT analysis would have indicated that DOD needed to adjust its planning. The only gold badge in this option concerned the training of Afghan Security Forces, which also was part of the other two options and had support from all sides. DOD planning appeared to be based on two false assumptions. First, over the past several decades, U.S. presidents had readily approved ("rubber-stamped") all DOD recommendations on troop levels and military strategies—but that was not the case with President Obama. Second, similar to Iraq, they assumed a CI strategy was best for continuing the war; this assumption was not shared by President Obama, Vice President Biden, and the National Security Advisor's staff who preferred a CT strategy. Thus, without adjustments to their option for 45,000 additional troops, and the support of key "stakeholders" in the decision process, this DOD option likely would be rejected. A plan to gain acceptance would require an Acceptance Analysis, discussed below.

Acceptance analysis. With a SWOT analysis completed and necessary revisions under consideration, an acceptance analysis allows the determination of conditions that might help or hinder an option's final approval and implementation. Here **contextual thinking** is injected into the analytic process to develop an understanding of the decision's implications, consequences, and overall environmental conditions. The analyst must be sensitive to the physical and psychological factors of **stakeholders** involved in the decision process. Stakeholders are individuals, groups, or organizations that have a vested interest in the approval or rejection of recommended policy options.

Acceptance analysis should begin with a 5Ws + 1H analysis (Chapter 8). As part of this analysis a table is created with two columns: one for sources likely to assist the approval or implementation of an option and one for those likely to resist the approval or implementation of an option. Then under each column, list the 5Ws + 1H results about the option from the perspective of those assisting or resisting the approval or implementation of that option. The next step is to use the results of the 5Ws + 1H to conduct an acceptance analysis by creating a table that lists stakeholders, their level of support for an option, and potential actions to gain support where it is lacking or to improve existing support. An acceptance analysis proceeds as follows:[32]

- Generate a list of all stakeholders.
- Identify each stakeholder's existing level of support for the option.
- Estimate each stakeholder's level of support required for the option's approval.
- Generate action items to achieve the level of support required for the option's approval.

Box 10.7 provides an example of an acceptance analysis surrounding President Obama's 2009 decisions on troop deployments in Afghanistan (Boxes 9.3, 10.5, 10.6 provide details).

Box 10.7 Acceptance Analysis: Obama's War in Afghanistan

Option 3: 45,000 additional troops with unspecified number of enablers. Troops would train Afghan Security Forces and conduct CI operations.

Stakeholder	SO	MO	N	MS	SS	Actions to Gain/Improve Support
President Obama		X →	→	→	O	Specify war end date, plan would send political message to AF govt, reduce costs, adopt CT strategy
VP Biden	X →	→	→	O		Same as President Obama
Secy Def				X →	O	Reduce costs
DOD Sr. Military					X	
Secy State			X →	O		Show training of AF Security Forces would deepen AF democracy
NSC Staff		X →	→	O		Make acceptable to Obama & Biden
U.S. Congress		X →	→	O		Specify war end date, reduce costs
U.S. Public		X →	→	O		Same as U.S. Congress

Legend: Strongly Oppose (SO), Moderately Oppose (MO), Neutral (N), Moderately Support (MS), Strongly Support (SS). X = Existing Level of Support, O = Required Level of Support

The above acceptance analysis would have further informed DOD that its Option 3 was in danger of rejection without several revisions. This analysis reveals they needed to reduce the cost of their recommended option, either by reducing the numbers of troops deployed or by shortening the deployment period. The DOD option needed a projected end date for U.S. troop deployments in AF, with the end date sending a political message to the AF government. DOD also needed to develop a plan for shifting from a CI strategy to a CT strategy.

Results: According to Bob Woodward's book *Obama's Wars,*[33] DOD appeared not to have generated a SWOT analysis (Box 10.6) nor an acceptance analysis, and entered the fall 2009 National Security Council meetings adamant that Option 3 was the best solution. With DOD failing to do a good job at contextual

thinking in their planning, Option 3 was not selected by the President, who decided on Option 2 as detailed in Box 9.3.

Key Concepts

Acceptance Analysis
Analysis of Competing Hypotheses
Capabilities
Cascading Threat Models
Consequences
Contextual Thinking
How-How Analysis
Implications
Indication & Warning Problem
Indicators Analysis
Indicators List
Intelligence Collection Plan
Intentions
Low Probability/High Impact Event
Policy Marketing
Positive Consequences
Stakeholders
SWOT Analysis
Threat Analysis
Unintended Consequences
Warning Analysis
What If? Analysis

Discussion Points

1. Using information in Boxes 6.3 and 7.1, conduct a cascading threat analysis of the implications and consequences from an Iraqi perspective of the 1980 Iraqi attack on Iran.
2. Using information in Boxes 6.3 and 7.1, develop an Indications & Warning Problem—indicators list, indicators analysis, and intelligence collection plan—from an Iranian perspective for a possible 1980 Iraqi attack on Iran.
3. Using information in Boxes 2.1 and 7.2, develop a How-How analysis, SWOT analysis, and Acceptance analysis for the end of the day-one ExCom discussions during the Cuban Missile Crisis (where President Kennedy's advisors

recommended surprise surgical airstrikes on Cuban air defenses and Soviet missile sites, followed by an invasion of Cuba).

Notes

[1] Richard Paul and Linda Elder, *Critical Thinking, Tools for Taking Charge of Your Professional and Personal Life,* 2nd ed. (Upper Saddle River, NY: Pearson Education, Inc., 2014), 93.

[2] Ibid.

[3] Ibid, 117.

[4] Fred May, Cascading Disaster Models in Postburn Flash Flood," in *The Fire Environment—Innovations, Management, and Policy,* eds. Bret Butler and Wayne Cook, Proceedings RMRS-P-46CD, March 2007 (Fort Collins, CO: U.S. Department of Agriculture, Forest Service, Rocky Mountain Research Station, 2007) https://www.fs.fed.us/rm/pubs/rmrs_p046/rmrs_p046_443_464.pdf (accessed April 28, 2021).

[5] Cynthia Grabo, with Jan Goldman, *Handbook of Warning Intelligence, Complete and Declassified Edition* (Lanham, MD: Rowan & Littlefield, 2015), 2.

[6] Ibid, 381.

[7] Ibid (entire book).

[8] Arthur S. Hulnick, *Keeping Us Safe: Secret Intelligence and Homeland Security* (Westport, CT: Praeger, 2004).

[9] Richards J. Heuer Jr., *Psychology of Intelligence Analysis*, (Washington, DC: Central Intelligence Agency, Center for the Study or Intelligence, 1999), 95-110.

[10] Office of the Director of National Intelligence, "Intelligence Community Directive 203 Analytic Standards," (Washington, DC: Office of the Director of National Intelligence, 2015), 3. https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf (accessed July 20, 2018).

[11] Erik J. Dahl, *Intelligence and Surprise Attack, Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), 177.

[12] Sundri Khalsa, *Forecasting Terrorism, Indicators and Proven Analytic Techniques* (Lanham, MD: Scarecrow Press, 2004).

[13] Christopher Paul and Eric Landree, "Defining Terrorists' Information Requirements: The Modified Intelligence Preparation of the Battlefield (ModIPB) Framework," *Journal of Homeland*

Security and Emergency Management: 5, no. 1, (2008): 1-18. https://www.rand.org/pubs/external_publications/EP20080028.html (accessed April 14, 2021).

[14] Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis,* 2nd ed. (Thousand Oaks, CA: Sage/CQ Press, 2015), 250-254.

[15] Michael W. Collier, "Intelligence Analysis, A 9/11 Case Study," in *Homeland Security and Intelligence*, 2nd ed., ed. Keith Gregory Logan (Santa Barbara, CA: Praeger, 2018), 88.

[16] Robert M. Clark, *Intelligence Collection* (Los Angeles, CA: Sage/CQ Press, 2014), 451.

[17] The following discussion was edited from Collier, 88-92.

[18] Bill Gertz, *Breakdown, How America's Intelligence Failures Led to September 11* (Washington, D.C.: Regnery Publishing, 2002), 83–104.

[19] Bob Graham, *Intelligence Matters, The CIA, the FBI, Saudi Arabia, and the Failure of America's War on Terror*, with Jeff Nussbaum (New York: Random House, 2004), 75.

[20] Richard A. Clarke, *Against All Enemies, Inside America's War on Terror* (New York, Free Press, 2004), 236.

[21] 9/11 Commission, *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton & Company, 2004), 258.

[22] Peter Lance, *1000 Years for Revenge, International Terrorism and the FBI—The Untold Story* (New York: HarperCollins Publishers, 2003), 405.

[23] 9/11 Commission, 258.

[24] Ibid.

[25] Aaron Wildavsky, *Speaking Truth to Power: The Art and Craft of Policy Analysis* (Boston, MA: Little, Brown and Company, 1979).

[26] Richard L. Kugler, *Policy Analysis in National Security Affairs: New Methods for a New Era* (Washington, DC: National Defense University, Center for Technology and National Security Policy, 2006), 73.

[27] Gerard J. Puccio, Marie Mance, and Mary C. Murdock, *Creative Leadership, Skills That Drive Change,* 2nd ed. (Thousand Oaks, CA: SAGE, 2011), 230-232.

[28] Bob Woodward, *Obama's Wars* (New York, NY: Simon & Schuster, 2010).

[29] Heuer and Pherson, 308-310.

[30] Kugler, 47.

[31] Heuer and Pherson, 309.

[32] Puccio, Mance, and Murdock, 215-217.

[33] Woodward.