Part I

Understanding the Dark Side: Malicious Intent

In This Part

Chapter 1: Analyzing the Malicious Individual
Chapter 2: Analyzing the Malicious Group
Chapter 3: Analyzing Country-Level Threats
Chapter 4: Threats and Security Nightmares: Our Current Reactive State of Security
Chapter 5: Current Network Security
Chapter 6: Future Threats to Our National Security

CHAPTER 1

Analyzing the Malicious Individual

We are all as unique as our fingerprints. No two of us are alike. Even identical twins exhibit different behavior under different circumstances. We are born with a genetic design that dictates our eye and hair color, height, weight, temperament, musical ability, and an immense number of other attributes. However, through life's experiences we are molded by a combination of biology and environment to be who we are and to behave the way we do.

We all respond continuously to events and situations in our environment that precede our behavior. We continually respond to any environmental context in which we find ourselves. As stated in the Introduction, a behavioral perspective considers these preceding events and situations to be *antecedents*. When we do exhibit behavior in the presence of precursor events, our behavior has *consequences*. Antecedents prompt behavior to occur, and consequences maintain it, increase it, or decrease it in the future, based on the desirability of the consequences. I refer to the antecedent-behavior-consequence sequence as *ABC* simply to use a less wordy term. In this chapter, you will learn to use ABC principles to help analyze malicious behavior. In later chapters you will learn how to use the concepts along with new methods to accurately anticipate malicious behavior.

Analyzing the Unique Individual

The method of behavior analysis presented in this book may be used to analyze and anticipate the behavior of an individual or group. When you compare the two, perhaps surprisingly, the individual often exhibits more behavioral variety than a group. Members of a group typically share common beliefs or are united for a common cause. The commonality among the members means that the group may act as a single entity, at least in some ways. They may respond to similar antecedent conditions with similar behaviors and are reinforced by similar consequences of their actions. Street gang members may dress alike, use the same slang, target the same individuals for harm, and remain in the gang because of bonded similarities. Although there are individual differences even within the members of a group, the commonalities simplify group analysis.

To ensure adequate analysis of the individual, the following are two of the most important principles to follow:

- First, we need to ensure that we have adequate and multiple observations of behavior under various conditions.
- Second, observations must include adequate descriptions so that we can identify the who, what, when, where, and how of past behaviors.

In the absence of observation we can use subject matter expert (SME) descriptions, but it is essential that the SMEs are knowledgeable.

DEFINITION **A *subject matter expert* is someone who maintains knowledge and details of a specific topic at a level that is more extensive than that of others. For example, a cardiologist attains and maintains knowledge of the functioning of the heart that is much deeper than that possessed by other individuals.**

We want to identify the antecedents, behavior, and consequences of past behavior (see Chapter 7 for details). Therefore, we seek to identify what environmental conditions serve as antecedents that precede the behavior of interest, as well as what follows the behavior — the consequences. Multiple examples of all three components — antecedents, behavior, and consequences, in that order — allow us to predict the person's future behavior when similar antecedents and the promise of similar consequences are present.

As a simple example to demonstrate the concepts, if we observe pedestrians crossing a busy intersection, we know that the crosswalk light will flash that it is okay to cross. The antecedents in this case are the flashing crosswalk light, followed immediately by the behavior of interest — pedestrians crossing the intersection. The consequence is that pedestrians cross successfully without injury and with minimal risk. If the crossing light is not on and cross traffic is

occurring, we can predict that pedestrians will not try to cross the intersection. Not crossing when the flashing crosswalk sign is not on with oncoming traffic again ensures safety at the intersection as a consequence. Therefore, we can predict with a high probability of success that when there is oncoming traffic, pedestrians will cross when the flashing crosswalk signal is on and will not cross when the signal is off. The antecedent controls the behavior.

However, with continued observation we are likely to determine that if the crosswalk light is not on and there is no oncoming traffic, pedestrians will likely cross quickly. This is a more complex and more accurate analysis. The behavior of crossing the intersection can be predicted accurately under two antecedent conditions: (1) the flashing crosswalk signal is on and traffic is stopped, and (2) the crosswalk signal is flashing or not flashing, but there is no oncoming traffic. Therefore, the two methods of crossing are likely to occur in the future because both lead to successful consequences — a safe crossing of the intersection.

Malicious behavior is very similar to this oversimplified example. Such behavior does not just happen. It occurs in response to environmental antecedents and is reinforced by the consequences of the behavior. For example, the presence of an abortion clinic and the comings and goings of the staff serve as antecedents (A) to an abortion clinic bomber. Committing a bombing is the behavior (B) that we are interested in predicting. The consequences (C) of the bombing, such as disruption of abortions stemming from physical damage, injury, or even death of the workers, reinforces the act of bombing. This ABC sequence forms the basis of behavioral modeling that has been shown to be predictive. The ability to predict future behavior is not based on a specific type of statistical method or detailed study of the behavior of interest. Prediction of behavior is based on the underlying antecedents and consequences associated with past behavior.

NOTE **The ability to predict future behavior is not based on a specific type of statistical method or calculation. Accurate anticipation of behavior is based on the underlying model and the components of behavior used to develop the predictive model.**

Interestingly, the ability to predict behavior does not rely on the individual to be rational or sane. In many of our past clinical cases, we used applied behavior analysis to help treat psychotic episodes, hallucinations, delusional talk, and other forms of abnormal behavior. Even in cases where a person is considered mentally ill or deficient, his or her behavior may still be predicted accurately if ABC behavior principles are applied diligently. In short, everyone responds to the environment from their own perspective, regardless of whether the antecedent conditions are present, or valid, from their perspective. Whether the target of the analysis is a world leader, a terrorist, or the criminally insane, the ABC components help us analyze and predict their behavior.

NOTE **We don't have to thoroughly understand *why* a person commits a specific type of malicious act to predict its occurrence in the future. We do, however, need to identify the precipitating antecedent events and the desired consequences that followed each occasion of the malicious behavior in the past.**

As a real example, Jeffrey Dahmer was a serial killer who targeted young males. Therefore, young males, their activities, and the locations they frequented became antecedents to Dahmer's behavior of visiting these same locations. Once a victim was targeted in one of these locations, the victim himself became an antecedent that prompted Dahmer's next step, which was to approach the victim. During Dahmer's interaction with the potential victim, that person's responses served as antecedents to Dahmer's approach of inviting the victim to his home, where subsequent molestation and death were waiting. If the sequence of behaviors was successful, we can predict with some certainty that the murders would continue.

Dahmer murdered 17 males over 13 years, one at a time. The antecedents to the multiple attacks, the actual behavior of murder, and the sexual molestation after death were all highly similar to each other. Dahmer's actions were an example of how malicious, fatalistic behavior may be patterned. His serial murders were also examples of behavior increasing in frequency because of the consequences (his not being apprehended and his ability to engage in sexual molestation). Until he was caught, he was free to continue his murders at an increasing pace. Finally, he was apprehended after a victim narrowly escaped and brought police to Dahmer's house. When the police arrived, they discovered pictures of young murdered men, a head in the refrigerator, and disintegrating bodies in a container of flesh-eating and bone-dissolving chemicals.

An analysis of the behavior across many individuals indicates that antecedents, behavior, and consequences are specific to the individual. The more bizarre the case example, the more assured we can be that the individual is responding to conditions in ways that are very different from our normal behavior.

The following sections present analyses of three persons with malicious intent as examples of the many and varied malicious cases:

- Richard Reid, the infamous shoe bomber
- Ted Bundy, the infamous serial killer
- The general, anonymous individual cyber attacker

These examples are purposely very different — for example, in the case of Ted Bundy, the subject could be considered to be mentally disturbed. Still, in each case the behaviors described in the examples, however repulsive, can be analyzed for

predictive patterns using the methods presented in this book. The latter case, the cyber attacker, is meant to be unidentifiable to demonstrate that the identity of an individual is not a requirement to conduct a behavior-based analysis.

Richard Reid: The Shoe Bomber

On December 22, 2001, Richard Reid boarded American Airlines flight 63 bound for Miami, Florida, from Paris, France. It was less than 14 weeks after the devastating al-Qaeda 9/11 attacks against the World Trade Center in New York City and the Pentagon and an aborted airliner attack downed in the fields of Pennsylvania when passengers intervened. En route, Reid took his seat like all the other passengers, but he wasn't like the other passengers. He was reportedly intent on killing everyone aboard the flight before the plane would reach Miami. Perhaps encouraged by the events just 14 weeks earlier (the infamous al-Qaeda 9/11 attack) and his self-proclaimed identification with al-Qaeda, Reid was serious, was prepared, and would kill himself along with the other passengers in the attempt. His chosen weapon was 10 ounces of pentaerythritol tetranitrate (PETN), a powerful explosive that, if detonated, would bring down the plane into the depths of the Atlantic Ocean.

Reid had received terrorist and explosives training in Pakistan and Afghanistan. He considered the United States the enemy, and he was on a quest to attack the evil country. Consistent with past terrorist attacks, the plan was to commit a horrific attack that would cause shock and despair.

The Event

The actual event that transpired was apparently different from what was planned. On the day before the incident, Reid attempted to board the same American Airlines flight but was prevented from doing so. His appearance was unkempt, and he had no luggage. This was enough to raise suspicion among cautious security personnel. Questioned but not held, Reid missed the flight. He successfully boarded the same flight the next day, December 22. During the flight, Reid attempted to light a fuse with a match. The short fuse led to explosives hidden in his shoe. Alert passengers smelled the match and reported it. Confronted by an alert flight attendant, Reid tried twice to light the fuse in his shoe, and it did not start. Restrained and then arrested, he eventually pleaded guilty to all eight counts brought against him, including attempted murder and attempted use of a weapon of mass destruction. Reportedly defiant and displaying no remorse, Reid proclaimed during his trial that he was the enemy of the United States and expressed allegiance to al-Qaeda. He was sentenced to life imprisonment with no chance of parole.

The Motivation

Using applied behavior analysis, motivation is seen as identified antecedents and consequences of specific behavior. We can't see inside the person, but we can see what antecedents he responds to and what follows the behavior that is desirable to him. We can only infer inner motivation, but we can actually measure the observable ABC components. For example, antecedents can include reported U.S. actions and past terrorist events, as well as receiving training, being provided with a bomb, having a plan for using the bomb, arranging a flight, and boarding the plane. These events can be counted, measured in length of time, and, as such, form the basis of a scientific analysis.

Reid's bombing attempt can be viewed as a behavioral chain. Such a chain occurs as a series of antecedents (A), behavior (B), and consequences (C). In a behavioral chain, consequences of the first behavior, if successful, serve as antecedents to the second behavior, which then has consequences, as shown in Figure 1-1. These consequences then serve as antecedents to the third behavior in the sequence, followed by consequences of the third behavior, and so on, until the final behavior is completed. In this way, complex behavior can occur as a sequence of events. If an ABC sequence fails during one of the steps, the chain breaks down, and the ultimate event, even if planned, does not occur, unless there is a second behavior chain to follow if the first fails. If there is, the second plan occurs when failure at a step serves as an antecedent for initiating the second plan.

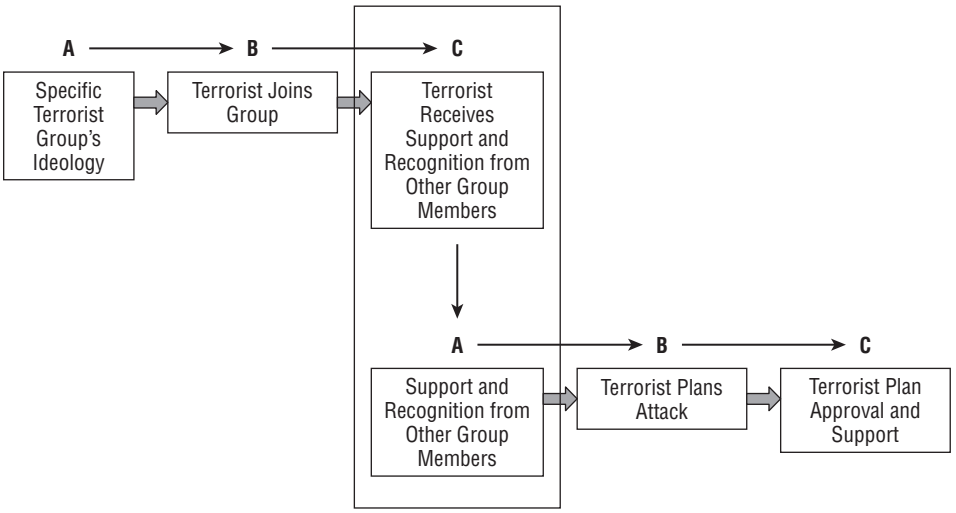


Figure 1-1: A behavioral chain in which a complex sequence of events may be described as consequences of one behavior becoming antecedents to a second behavior and so on until the entire chain is completed.

Reid either did not have a backup plan or was prevented from initiating it. The disruption of the plan came in the form of flight attendants who attempted to stop him from lighting a fuse on two occasions. Eventually, after the struggles with the flight attendants, Reid was subdued with the assistance of fellow passengers. For Reid, a series of chained events leading to the attempt was clear. Reid had planned the event for some time, had received training, was provided with bomb materials, and identified with al-Qaeda. He had followed a sequence of events that led to the end goal — attempting to light the fuse to explosives that, if detonated, would have brought down the flight.

Causes

The causes of terrorism are as varied as terrorist groups. However, Reid identified with al-Qaeda and, as such, incorporated the group's motivations, goals, and objectives. Targeting may be complex. Although primarily civilian, the World Trade center symbolized *towering* success and Western greatness and might. The vehicle for Reid's planned act was American Airlines containing civilians, bound for the United States. Combining this fact with the 9/11 attacks and the motivation, goals, and objectives of al-Qaeda, Reid's selection of the target and his subsequent actions are clear in retrospect. This was his chance to achieve infamy and to make his mark against a proclaimed enemy — the United States.

A Behavior Analysis

Analyzing Reid's behavior raises questions about his true purpose. On the day before the incident, Reid had tried boarding the same flight but with no luggage, and his appearance was sloppy enough to raise suspicion. Those intent on committing malicious behavior in public typically either attack immediately or attempt deceptive behavior by hiding in plain sight while they prepare for a malicious attack. It would be unusual for a terrorist with past training to attempt to board a flight with insufficient preparation, no backup plan, and an appearance so unusual as to raise suspicion. Terrorists often commit acts by blending in with the crowd. Reid did not blend.

During the flight, Reid attempted to light a fuse leading to the shoe that was then in his lap while passengers sat around him. It was obvious that the smell of a match would be noticed. For example, a lighter that would not have the sulfur odor of a match could have been used. The lighting of the shoe fuse could have been completed in the restroom, away from the passengers, with a gas lighter or an electric igniter so that Reid would not have been detected as easily. Last, the consequences of the detonation would likely have been the loss of a plane and lives in the Atlantic Ocean. Given the depth of the Atlantic, it may have never been retrieved properly and, therefore, difficult to determine the cause of the crash.

Given the *apparent* ineptness of the act, it is quite possible that the incident actually occurred as planned. When Reid was apprehended, the media produced a flurry of articles and television and radio reports about the incident. Media attention was heavy. Many articles dubbed Reid "the shoe bomber," and, as a result, we are still taking off our shoes at airport security lines 11 years later. The impact of the incident has been remarkable and exists only because Reid was apprehended and prevented from carrying out an actual bombing.

In my opinion, the Richard Reid incident was a success. He did not die in the process, and because of the detection of his overly obvious behavior, security practices have been affected at great cost for the past 11 years — with no end in sight. The media coverage of the incident provided consequences. Reid was allowed to make statements about his cause in court. His picture has been widely disseminated. His cause has been publicized. The incident has likely had more of an impact without bringing the plane down than if the explosion had actually occurred.

Because he was jailed, we will never know if Reid would have made another attempt. However, behavior principles also include modeling. We can review the extensive work of practitioners such as Albert Bandura to explore this interesting area in detail. Modeling basically refers to the process of one person's imitating the behavior of another. For example, if a person with malicious intent observes (including reading detailed accounts of) another's behavior that appeared to be successful, the second person may repeat the behavior. We typically call this *copycat* behavior, and we see its occurrence in criminal behavior.

To point to the possible reasoning that the Richard Reid incident was successful, a close repeat occurred 8 years later on Christmas Day. Umar Farouk Abdulmutallab boarded Northwest Airlines flight 253 from Amsterdam to Detroit — another flight leaving Europe for a destination in the United States. Abdulmutallab had the same chemicals in his underwear that Reid had in his shoe. No doubt they were in his underwear because of the potential to have shoes checked by security because of the Reid incident. Reportedly, Abdulmutallab returned from the restroom, placed a blanket over his lap, and lighted his pants. Again, there was no explosion, although the terrorist received burns. He too was apprehended. The incident received widespread media coverage, which contained the perpetrator's message.

Even if the underwear bombing was modeled after the shoe bombing, it is our experience that modeled behavior is just that — only the behavior is copied. The second person commits similar terrorist behavior but in reaction to antecedents that fit his cause and context. The consequences may be very different. In this way we can see similar terrorist attacks from different groups in response to different antecedents.

The direct and obvious success of both Reid and Abdulmutallab's *attempted* airliner bombings was that both terrorists evaded airport security and spawned

widespread media attention as a result of being apprehended. The latter incident raised considerable concern and new scrutiny of airport security. As is obvious with the Reid incident, the primary, typically reactive, security practice resulting from the attempt was inspection of shoes. This provided some cause for concern and fuel for late-night comedians when the underwear bombing attempt was reported. Would we be required to remove our underwear? Obviously not. However, because we can't remove our underwear, we have seen an increase in the use of body scanners.

What is the next step? Many security lines at airports now check belts and shoes and use scanners. The result will be that terrorists may simply alter their approach. Our security posture is not only reactive but also literal. In the examples given, the explosives simply moved from the shoe to the underwear. Given that terrorists alter their tactics based on our security policies, we may be approaching a body cavity bombing attempt if airliners remain a vehicle to support the incident. Because of the location of a body cavity bomb, it is not likely to be accidentally discovered. If the intent is truly to bring down an airliner full of innocent civilians, we are more likely to witness a suicide-bombing explosion in an airliner.

NOTE ***Automated behavior analysis*** **(AuBA) is the automation and extension of applied behavior analysis for the purpose of predicting malicious behavior. Patented tools assist in automating the formerly manual process to achieve rapid and accurate behavioral modeling on a global security basis. The accompanying DVD demonstrates how the AuBA tools and applications can work in real time.**

Ted Bundy: The Infamous Serial Murderer

Theodore ("Ted") Robert Bundy was one of the most brutal serial murderers in U.S. history. Bundy shattered many views of the serial murderer. He was a law student, was described as handsome and well mannered, and was interested in politics. Yet he was a cold-blooded killer who targeted attractive young women. He became an expert at attracting women, convincing them to go to a remote location, and then killing them, often violently. Although he admitted to 30 murders, new evidence has surfaced to indicate that he may have committed many more.

Bundy developed a skill for convincing selected targets to accompany him to remote locations, where he could kill them without being seen. He would have sex with the corpses. On occasion, he would behead the victim and keep the head in his house. He was a self-described despicable human being who would use a faked injury or need for assistance to lure his victims. He would wear a

cast, use crutches, and even fake police identification as a means to weaken the chosen victim's defenses and to allay her suspicions.

Bundy was brutal, often beyond words. He often bludgeoned his victims using a crowbar. His behavior occurred in three stages:

1. He would select and attract a victim.
2. He would transport and then kill her.
3. He would engage in sex with and desecrate the corpse.

Each stage was honed as a set of skills strengthened by continued success (desirable consequences for the perpetrator). On occasion he would alter the pattern, but the killings were notable more for their strong similarities than for their differences.

Similarities of Targets

Bundy selected his targets based on similarities. All the victims have been described as attractive young females. They all had long dark hair; the hair was parted down the middle; and many were associated with college. His selection of targets for his attacks was highly specific.

The Motivation

Motivations are complex and often difficult to identify. Richard Reid committed a public act that was highlighted by his apprehension. In contrast, Ted Bundy committed private acts with the objective of not being detected or apprehended. More similar to a Jeffrey Dahmer, serial murderers must plan carefully and hone their skills to separate a victim from others, isolate the person, and kill him or her while remaining undetected. Because the acts are committed by these individuals in private, it is fair to say that public attention, media exposure, and detection are not contributing factors to the cause of the repeated behaviors. It is clear that when such heinous crimes are committed, the person is deranged, with motivations that are likely never to be discovered. It is even possible that the perpetrator himself could not describe the reasons for his actions. The causes are complex and deeply seated.

However, a behavior analysis can provide insight in such serious cases of flagrant abuse against humanity. Although we don't know why Bundy committed such acts, we can determine observable antecedents for him that included young, attractive women. Antecedents for Jeffrey Dahmer included young males. Consequences were similar to some extent. The consequences of killing the victim in both cases were that sexual molestation and dismemberment could occur.

Behavior analysis can provide the types of insights that would otherwise be lost. Behavior analysis is crucial in cases where there is not the possibility to

observe the behavior we are trying to predict or influence. By studying past behaviors, we can gain a better understanding of how serial murderers operate. When we compare Dahmer and Bundy, we see the behaviors of luring a target to a private location and the brutal, sexually oriented behavior of the perpetrators are similar. In one case, the targets were exclusively male, and in the other case, they were exclusively female.

Today, we face many adversaries that target the United States, its citizens, and our national infrastructure. These adversaries, whether terrorists, insurgents, or cyber hackers, are usually not known to us until after the fact and, in many cases, never known. Often, all we have are examples of their behaviors. The examples may be in the form of reports, news articles describing past attacks, or SMEs who know extreme details about past behaviors. The lack of direct observation of behaviors poses problems for many forms of analysis. However, applied behavior analysis and automated behavior analysis, with their reliance on identifying preceding antecedents and following consequences, provide a means to better understanding not only adversary behavior but also in the case of the latter, a mechanism and set of tools to predict it.

Examples of past cases provide a mechanism by which we can learn and practice behavior analysis concepts and methods and not worry about passing along sensitive information from a current security-sensitive case.

Determining the Complexities Underlying Individual Malicious Behavior: A Behavior Analysis

The stages in the process in which Bundy started with victim selection and ended with post-death behavior had similarities to other cases, for example, Jeffrey Dahmer, as noted earlier in the chapter. In both cases the length of time between murders decreased over time; the killings started to occur more frequently. The ultimate consequence that ended the chain of events for each victim was the interaction with the corpse after death. In both serial cases, the process started with target selection and acquisition. In both cases, the victim had to have enough trust to join the killer and move to a location less likely to result in detection. In a recent documentary on serial killers, a former FBI profiler indicated that these different locations are referred to as *scenes*. Typically, the more scenes, the more complex the thinking of the perpetrator and the more careful the methods of selecting the target, of attracting the target, and of committing the murder. For Bundy, the stages described can be analyzed with the antecedents and consequences of the behavior defining each stage.

Table 1-1 is a high-level overview of an analysis of Bundy's serial killer behavior. The analysis depicts three sequential stages, leading from selection of the victim through corpse manipulation and sexual activity. Each stage is defined as a major behavior (target selection, transporting/killing the victim, and post-death

corpse desecration/sex). Each stage of behavior is associated with common antecedents and consequences.

Table 1-1: Dissecting Ted Bundy's Murders

STAGE	ANTECEDENTS	BEHAVIORS	CONSEQUENCES
Isolating the target as the victim	Age (youth), attractive, female, long hair, dark hair, straight hair	Approach target, fake injury or identity, wear cast, use crutches, request assistance	Victim in car
Transporting and killing the victim	Volkswagen Beetle, victim in passenger seat	Handcuff victim, hit victim with blunt-force object, render victim unconscious	Victim incapacitation complete
Post-death sex/corpse mutilation	Victim is dead, corpse	Sex with corpse, decapitation, mutilation, return to victim and repeat behaviors	Control over corpse, completion of sexual activity, corpse desecrated or decapitated

Each depicted stage in the behavioral chain was reinforced by the consequences of the behavior of that stage. Stage 1 began with selecting a target victim. Antecedents to the selection were age (young), gender (female), long dark straight hair, and attractiveness. The presence of these antecedents under the right conditions would prompt Bundy to fake an injury to attract the victim. Once the victim responded, Bundy would request assistance or otherwise try to get the target into his Volkswagen Beetle. (In one case he impersonated a police officer and asked the victim to go the station with him.) The act of the victim getting into his car reinforced Bundy's behaviors up to this point. The objective was to select the target and get her into his domain, where he had control and would be less likely to be identified.

Once the victim — not knowing that this would be her last voluntary act on Earth — accompanied Bundy in his car, Bundy moved to the next stage. This stage was to incapacitate the victim so that he could carry out his ultimate objectives. The form of incapacitation typically was violent and painful if the young lady was not rendered unconscious. It could include being handcuffed, being hit in the head with a crowbar, or suffering any other form of blunt-force trauma. What is important to realize in the Bundy cases is that victim's death was not the final objective. It was an interim objective to leave the victim in the ultimate state of submission. After the victim's death, Bundy could initiate his final objective. This included sex with the corpse, mutilation, and often repeated visits to the site to engage in the same behaviors until the disintegration of the body no longer supported the sexual degradation.

It is likely that if this chain of behaviors had been prevented from occurring at any stage, the behavior would have ceased for that time period and that target. It is more likely that Bundy would have waited for a new situation with a new victim. However, Bundy was successful in his repetition of behaviors. He had honed his skills to the point where he could rely on obtaining the assistance of an attractive and trusting young lady who fit his target profile.

Removing Subjectivity and Bias from the Behavior Analysis

Perhaps the most surprising fact of the Bundy case is that he received marriage proposals from young women while on death row. He orchestrated his own defense and even received positive comments from the judge upon his sentencing to death. The judge said that Bundy would have made a good attorney and that he had no animosity against him. This event is surprising given the path of destruction and devastation Bundy left, affecting not only his victims but also their families. It does demonstrate that Bundy was charismatic and used this trait as a tool to win over others.

Behavior analysis provides a method to remove subjectivity and bias. It provides a scientific set of methods that can identify key elements of behavior to help us understand better how behaviors occur over time. This is precisely why we need behavior analysis and its unbiased assessment of behavior. Again, the methods do not depend on a rational world.

We need behavior analysis to objectively analyze antecedents, behavior, and consequences of malicious intent so that we can avoid the seductions that Bundy was able to orchestrate all the way to the electric chair. Whether we are examining Jeffrey Dahmer, Ted Bundy, or anyone else who exhibits severe malicious intent, it is clear that behaviors are complex and must be dissected for us to understand them fully. Identifying antecedents and consequences does not depend on psychological, psychiatric, sociological, or family background — it focuses on the objective identification of key environmental events and situations that support the continued occurrence of the behavior. Last, the methods provide a mechanism to both predict and influence the occurrence of future behavior.

The Individual Cyber Attacker

The Internet is one of the most impressive technological advances of our lifetime. Humans exist by communicating, and the Internet provided a new, instantaneous method of doing so. It led to an evolution of communication that now includes intranets, social media sites, websites to meet anyone's needs and desires, webcams placed literally all over the globe, instant financial transactions, and instant news. But the new technology has also attracted malicious intent and

behavior that is moving as fast as, if not faster than, the actual technologies. More important, the Internet is rife with malicious intent, and we do not know the perpetrators. Again, this is a primary reason for using behavior analysis methods to better anticipate future cyber attacks.

The lone hacker has evolved from what is known as an ankle biter, script kiddie, or nuisance hacker to a sophisticated hacker capable of wide-ranging damage or theft. The situation is worsening, and both ankle biters and more sophisticated hackers remain. In total, their numbers and sophistication have increased. However, behavior principles can be used to understand how such behavior occurs. With such understanding, new technology can follow to intervene and prevent damage and theft.

Identifying the Threat from the Lone Cyber Attacker

In the early days of the Internet, the public simply did not understand the technology. Therefore, hackers of that era were granted the aura of *genius*, even though they could have been skipping school and avoiding education at the time. They typically were young, members of the hacker community, and learning by doing, sharing code, and seeking vulnerabilities to exploit. Hackers were divided into two groups: those who stated they were doing good, and *crackers*, who had malicious intent. However, a hacker who claims to do good by entering networks or applications uninvited to find their security vulnerabilities and then notify the owners is much like a stranger breaking into your house to check your security system. It is often a bogus justification. I don't want anyone getting into my computer network or any of my applications uninvited, no more than I want someone breaking into my house or car.

NOTE For simplicity, this book uses the term *hacker* to describe anyone who enters networks and applications uninvited.

As time passed from the 1980s and 1990s into a new century, it was clear that hacking had more rewards than simply recognition from peers. Money could be made by damaging or stealing information residing within protected networks; money could be made by stealing proprietary information and selling it to a competitor; and money could be made by stealing classified information and selling it to a foreign government. An organization might also pay a hacker to shut down a competitor's network with something as simple as a denial-of-service (DOS) attack. (Such an attack simply directs a waterfall of information or requests at a network so quickly and in such large amounts that the network cannot function.) More recently, credit card numbers, identities, and banks are being targeted at an increasing rate.

The individual attacker can show malicious behavior in a variety of ways. He or she has vast latitude with time, freedom of action, available code, and the high probability of not being caught. A new hacker might carry out his or her first attacks with some apprehension. The fear of being detected fades away as the individual learns how to be deceptive and realizes how difficult it is to be detected.

As stated, behavior principles indicate that if behavior is successful, it will continue. It may even increase in frequency. In short, it may escalate. There are many cases of beginning hackers becoming very good at what they do very quickly. Repeated acts followed by success as a consequence increases the behavior's occurrence over time. Success takes many forms for a hacker. Success in maliciously affecting sites, evading capture, or even avoiding detection, and perhaps identifying with the many movies and TV shows that depict hackers as the elite, work to bolster future hacking behavior. With practice come greater skill and greater knowledge.

NOTE **The more a hacker hacks, the better he or she becomes. Practice, and available hacking code, makes perfect.**

Catching a hacker takes excellent forensics, expensive investigation resources, and a solid reason to prosecute. As a result, until protection technology improves, effective hacking is here to stay and grow.

Hacking has become more sophisticated. In recent years, it has become apparent that advanced persistent threats (APTs) may be one of our most serious concerns. APTs can come from a foreign state-sponsored intelligence service that is always present and waiting to gain access. As pointed out by my SANS instructor friend and colleague, Dr. Eric B. Cole, when an unsuspecting user clicks a seemingly harmless link, the damage may already be done. One of many APT-vigilant programs may be installed on the user's hard drive by means of the innocent click and immediately begin monitoring the user's actions to capture user IDs and passwords. Of course, as soon as the hacker has the user ID and password, he or she can access the network at will as an approved user and can cause significant harm or steal restricted information.

In the past, we associated malicious intent with the person causing the damage. We now have to broaden this concept. The malicious intent may be part of an APT organized threat, but the innocent individual inside an organization may be the unwitting participant who unlocks the security doors for the malicious service. Malicious intent and behavior must now be broadened to include the behaviors of the inside innocent employee who simply does not know about or practice good security policy.

Recognizing the Power of Being Anonymous

It is easier to be malicious if the probability of being caught is small to nonexistent. Certain events and situations in the environment actually suppress behavior. For example, a yellow traffic light turning red as you approach suppresses your driving through the intersection. When the light turns green, the color serves as an antecedent to driving through the intersection. If you follow the antecedent rules, you may continue to drive through intersections with a low probability of an accident (successful consequences). The individual hacker encounters very few situations in which hacking behavior must be suppressed. Because hacking activity may be bounced through different servers (relays), it is difficult to impossible to conduct an actual traceback under normal circumstances. A person can remain anonymous in the midst of a flurry of hacking activity. Anonymity spawns the courage to attack. After all, the victim doesn't know who you are. This is even more true if networks or sites are attacked at random. The hacker simply continues attacking different sites until he or she is successful.

Although there is only a slight chance that a hacker will be identified, precautions can still be taken. As the individual attempts to hack into sites, he acquires deceptive practices to maintain his anonymity. In studying hacking in detail, I have reduced the many factors that are associated with hacking to just two significant variables if we are concerned with external threats only. To be a successful hacker and be a significant threat, one needs only:

- To have the *expertise* to conduct effective hacking
- To be *deceptive* to ensure not being caught

Chapter 17 discusses in detail my patented CheckMate and InMate applications, produced by SAIC:

- **CheckMate** converts samples of network packets into the behavioral measures of the degree of *expertise* and *deception* present at any one time for every external user entering a network.
- **InMate**, similar in construction, converts users' network activities into *intent to engage in misuse* and *deception* for all insiders (employees, contractors, interns, and so on).

The hypothesis in conceptualizing CheckMate was that if expertise (E) and deception (D) are simultaneously higher than preset thresholds, malicious behavior is occurring or will occur in the very near future (in seconds). If high E and D occur at the same time and the option is set, CheckMate can intervene and block the potential offender's connection. InMate works in a similar manner, except that if an insider threat is identified, an alert is immediately forwarded to security. Most important, CheckMate (working to protect against external

threats) and InMate (working to protect against internal threats) provide a combined approach that is unparalleled. The dual external and internal threat protection that concentrates on true human behavior, as opposed to network activity, is a totally new security methodology.

CROSS-REFERENCE **AuBA applications to address both external and internal computer network threats are discussed in Chapters 11, 12, and 17 (CheckMate and InMate products). The DVD contains demonstrations of the applications working.**

CheckMate and InMate are constructed from automated behavior analysis (AuBA) technology. They are good examples of new, proactive security technology that is not based on signatures or anomaly detection. The differences between this new technology and signature and anomaly detection are explained in detail in Chapters 5 and 12. The new technology works on the basis of real-time behavior assessment methods presented in this book. By applying behavior principles and techniques and focusing on human malicious behavior, as opposed to network behavior, new proactive protection technology is surfacing. This new technology presents the case and the foundation for a new approach to security practices.

Recognizing When a Hacker Is Detached from the Target

Human behavior has suppressors. If suppressors are present, malicious behavior may not occur. But if the suppressors are removed, malicious behavior occurs. For example, criminal behavior is unlikely to occur to any great extent within one or two blocks of a police station. The risk of getting caught is just too high, and there are too many other places to commit a crime where the chances of detection are slim. In this example, the police station acts as an ever-present stimulus to suppress malicious behavior in that immediate vicinity. However, if the police station moved 5 miles away, crime levels would probably return to normal for the region after the suppressor stimuli are gone. Likewise, if you place a security system warning sticker in your front window, the potential breaking-and-entering criminal may pass your house in favor of one that doesn't appear to be protected. There are too many other houses to break into where there is less chance of setting off an alarm.

Although these are simple examples, they illustrate to some extent why hacking occurs at such a high rate and appears to be increasing. There are few suppressors. In other words, it is well known among hackers that if a known attack is modified using typical hacker evasion tactics, the new attack is not likely to be picked up by typical signature detection designed to catch only past attacks. Therefore, to the sophisticated hacker, signature detection is simply not a suppressor. Just change a known attack and send it back through,

and it is likely not to be detected. This is our primary network security flaw in existence today.

Being a hacker who approaches target networks remotely, and maybe even at random, means that the hacker has little or no investment in the target and may not even know anything about it. When one has malicious intent, it helps to not know the target if an act will be committed against that target. Being detached lessens guilt, remorse, and all the other psychological factors that can work to suppress the hacking behavior against that target. Certainly, a hacker does not attack targets who are friends or members of the accepted hacking culture. We don't see hacking wars to speak of, although there are a few exceptions between warring groups/countries. Even if the target is well known, such as a Fortune 500 company or a major financial institution, it is relatively easy to remain detached. After all, the hacker's perception is that the Fortune 500 companies are filthy rich and can absorb loss. At least, that is the reasoning to maintain the detachment.

At the time of writing this book, the *Occupy Wall Street* movement and its many derivatives show that Americans are protesting the corruption and unfairness that exists between mammoth-sized companies with rich staffs and the more common Americans. As the slogan goes, "We are the 99%." This means that 1% hold the wealth, while 99% do not. Therefore, there is likely little guilt in attacking these super-rich companies/organizations.

The detachment from a selected target, the potential for recognition from other hackers, and the sense of acting in a covert manner fuel the ankle biter/script kiddie, as well as more sophisticated hackers. Whether under the guise of helping by discovering security holes or pure intent to be a nuisance, the ankle biter is of concern, although mild. It is when we add significant motivation to inflict significant harm that the degree of malicious intent is of much greater concern.

Recognizing Motivation

Motivation for committing any individual malicious network attack is of serious concern because the perpetrator wants to inflict harm on others. The number of malicious acts that can be committed is limited only by the hacker's imagination. Severity of the behavior ranges from mild malicious behavior that creates a nuisance to significant theft or sabotage. Regardless of the number of malicious acts that can be directed at a network, there are only two ways to inflict harm on others.

1. The perpetrator can do something harmful to a person or group (for example, denial-of-service attack to disrupt the organization's normal business operations).
2. The perpetrator can take away something pleasant or something that a person or group owns (for example, classified or proprietary information).

Although we cannot determine someone's motivation with certainty, analyzing components of behavior can help us infer malicious intent.

It is important to realize that APT from a sponsor such as the Chinese is very important. As reported by many open source news articles, one of China's primary goals is to be the world's leader in technology within a decade. There are two ways to accomplish this: (1) to develop new technology that is superior to all other technology developed worldwide (not likely), and (2) to steal proprietary technology secrets from top private, commercial, and government sites. In my opinion, the primary reason for the many attacks and thefts of information we are experiencing that point to the Chinese clearly fit the latter category. If they enter a network and make copies of proprietary information, leaving the original information, they have engaged in theft that increases their technology and makes them more competitive. Let's not fool ourselves. This is happening. It doesn't matter that it is a copy — the secrets are gone and continue to leave. We desperately need new technology to stop this U.S. brain drain to coordinated and state-supported hacking, or we should take all proprietary and sensitive information off the networks!

Because no specific personality type commits malicious network attacks, and because profiles of individuals are as varied as the number of profilers, behavior analysis presented in this book provides a structure for studying the significant malicious behaviors in question. The structure provides us with reliable and valid ways to anticipate adversary behavior.

A set of antecedents serves as signals indicating that it is time for a specific behavior to occur. In a sense, the presence of a set of antecedents is like removing the safety on a gun; it is now ready to shoot. It is clear that we all act in response to the presence of antecedents. If you want to cross a busy street, the oncoming cars or a lack thereof serve as an antecedent for signaling when you can cross the street safely. You may stand on the corner with the motivation to cross, but you cross only when the antecedent conditions say the coast is clear. Regardless of the motivation, the conditions must be right for a specific behavior to occur. That is a key point — regardless of the internal motivation, the hacker's behavior is moderated by environmental antecedents and consequences of the hacking behavior.

Identifying the Power of Disruption

The focus of security practices is to maintain order and the presence of nonmalicious behavior, or to minimize damage if it should occur. Therefore, security has to be concerned with all forms of malicious activity. If we observe a protest on television, we notice the presence of law enforcement and security forces. Security personnel are often thrust into disruptive environments where either active malicious behavior is occurring or great potential for disruption is accelerating quickly into harmful conditions. This is also true of computer

networks, except that it is not quite so obvious as a public disruption on the street. Hackers embrace being anonymous to all but their friends. Disruption and the nature of how it plays out depend on the context.

Disruption by an individual in public is intended to cause a public effect. Recently I saw on the evening news the apprehension of an overweight man running and frolicking through a parking lot naked. You may wonder why someone would do this. You may also assume that this would not be considered normal behavior — something that most people observe frequently. It would be a very interesting world indeed if this were the norm, based on who decided to be the perpetrator! However, it is clear that such behavior resulted in a public disruption. The behavior literally stopped traffic, the smartphones were out in a second, and the behavior was recorded for posterity. The person committing the act responded to public antecedents. Many people were present to ensure an audience, and his being subdued by security was public and recorded. We may not know his inner reason for the behavior, but it occurred in public, and he succeeded in his objective of disrupting events and saying, "Look at me."

This is an example of disruption on one end of the spectrum. It is an example of being public, in public, to gain public attention, perhaps at all costs. Being apprehended and cuffed while on his stomach on the hot blacktop may have been an undesired consequence. Being apprehended and handcuffed this way should, according to behavioral principles, decrease the probability of the same behavior occurring under the same circumstances in the future. Perhaps joining a nudist colony would be a sound backup plan.

On the other end of the spectrum is computer network hacking. This extreme includes behavior that is not public, and the hacker does not necessarily want to be known, discovered, or apprehended. The hacker embraces anonymity, except for seeking the adoration of the select few with whom he or she may share the exploit. The key to many hacking attacks may simply be profit from theft of credit card information, financial data, or other personal information, such as social security numbers that can be sold. To a lesser extent, disruption may be the goal. This objective is simple: interfere with the normal operations of a specific organization by disrupting network operations. Why? Disruption is easy — very easy! It requires far less expertise than covertly entering a network and stealing and actually achieving financial gain. Disruption can be caused by almost anyone and, with a minimum of planning, can be conducted with little worry about being caught.

There has been expressed concern about a dual terrorist attack — one that is conventional with multiple coordinated bombings but backed up by disrupting all networks to stop first responder communication. This is a nightmare scenario that has not happened yet. However, we should be aware that it is relatively

easy to shut down network communication at the time of a coordinated but conventional terrorist attack.

To seriously disrupt an organization, the hacker may use any number of possible denial-of-service (DOS) activities. A relatively simple DOS attack is fueled by malicious intent to cause harm. The objective is to disrupt an organization's activities by paralyzing its network. The basic DOS attack may result in a total loss of normal communication within the network temporarily. Hackers learn quickly that a DOS attack can be fairly simple to initiate. Protection from DOS attacks has improved, and today's high-speed networks are more difficult to clog. However, a disruptive DOS attack remains a serious threat from a hacker who targets that organization or from a hacker who simply wants to disrupt the operation of any network.

It's sad, but true. A large set of hackers is content to simply be mischievous and cause disruption. This type of hacker achieves desirable consequences by sharing the success with peers. He or she also feels a sense of success simply from achieving his or her disruption objective. If the hacker fails, he or she is off to the next network. The second type of disruption is when hackers target an organization for a specific purpose. In this case they have a reason why they want to hurt the organization. If at first they don't succeed, they may try again until they do succeed. Regardless of the motivation, the acts of both types of hackers have the same effect. However, the random act of DOS versus the repeated attempts represents different levels of threat. The hacker who targets an organization is often a more serious threat, because he or she might keep trying until he or she succeeds, and his or her success begets even more attempts.

Recognizing the Need for Theft

Theft is an act fueled by motivation as old as humankind itself. Theft has been around as long as humans have recognized and valued possessions. Someone gains a possession, and someone else wants to take it.

NOTE **For a hacker, theft on a network can bring the thrill of achieving financial gain with little effort and little concern for getting caught.**

Theft using a computer network of multiple servers joining multiple bank branches as targets is much like robbing multiple banks. The interconnected target with an accumulation of assets or valuable objects is a significant target. It is one-stop shopping. Penetrating a physical bank or network of banks that hold great wealth and the possibility of achieving gains financially by stealing some of that wealth is an increasing objective. However, today, stealing credit card

numbers, committing identity theft, and selling stolen restricted information may be just as valuable.

Theft is perceived as being easy. The criminal looks at theft as a means to an end. It is a way to obtain money for whatever reason money is desired. In the field of applied behavior analysis, money is a powerful conditioned, or secondary, reinforcer. This is a fancy way of saying that money has secondary value because it can obtain an almost infinite number of primary desired objects and services in our world. Instead of obtaining a flat-screen television as a reinforcer, obtaining money means that you can purchase anything you want. This feature is what makes money so attractive. Secondary, or conditioned, reinforcers are extremely powerful. By stealing credit card numbers or identities, a person only needs to sell them quickly to obtain money. There is a large market for credit card numbers and identities. If someone can steal numerous numbers or identities at one time from within a network and sell them to a bidder who wants such information, significant financial gain is ensured.

Information is also a conditioned reinforcer. It is a two-step process, much like selling credit card numbers or social security numbers. Aldrich Ames and Robert Hanssen were notorious and very damaging spies working against the U.S. government from inside. They stole classified information of great value to Russia, their customer. Ames worked for the CIA in an impressive position of trust. He then violated that trust and sold classified information to the Russians. Hanssen, a key counterintelligence head at the FBI, sold trusted inside and strictly held information to the Russians as well. Although their motivations for conducting espionage against their own country occurred as the result of a complicated set of internal motivations, a behavior analysis simplifies what they did over the years they operated as spies for a U.S. adversary. Obtaining classified information and then selling it is the same two-step process as obtaining and selling proprietary information. However, their disgruntled feelings toward the CIA and FBI added to their reasons for committing espionage against our country, not just their chances of financial gain.

Regardless of the target — obtaining classified or restricted proprietary information, identities in the form of social security numbers, or credit card numbers — the objective is to obtain valuable information. The theft then can be converted into money by selling it to a customer who seeks such information. Theft can be complicated because of a number of motivations fueling the theft. However, a behavior analysis makes such theft more understandable and predictable. If a constellation of indicators suggests extreme disgruntlement, a need for revenge against supervisors, or a need for recognition, even if from a foreign government, the stage may be set for insider theft. And if the individual

is in debt and needs money, and he or she has a low sense of ethics and loyalty to his or her country, the probability of theft rises sharply for that individual.

A Behavior Analysis

The behavior analysis of theft and disruption depends on the specific perpetrator and the context in which he or she operates. To conduct a predictive analysis, we would need to isolate the specific examples of theft or disruption and capture/identify the precursor antecedents that preceded the behaviors of concern and the consequences that followed. It is important to first define exactly the behavior of concern. For example, is it the act of stealing information or the act of selling information to an adversary that marks the behavior of concern? Is it the act of breaking into a network or the behavior of stealing information? Once the behavior has been defined, antecedents that precede that specific behavior and the consequences that follow are more clear. We then repeat this process across examples. Last, we try to find the common antecedents across all the examples. These common antecedents can then become predictors if we use them with the procedures outlined in this book and the DVD walkthrough.

Modeling the Individual: Advantages and Disadvantages

As noted earlier in the chapter, it is my experience that modeling the behavior of a group is easier than modeling an individual. All members of the group are individuals, but if we were to model an individual of that group, the antecedents and consequences would be remarkably similar across members. The individual represents the freedom to be different. Therefore, we focus on specific environmental influences affecting only the individual.

Table 1-2 shows the advantages and disadvantages of predictive modeling of the individual (such as a foreign leader) compared to predictive modeling of a group (such as a terrorist group). This table is the result of operational lessons learned across numerous models developed from clinical cases and cases across foreign adversaries. Furthermore, the table displays true advantages and disadvantages of behavior modeling of individuals using manual applied behavior analysis and patented automated behavior analysis modeling.

NOTE **I was awarded one of my patents on *methods and tools to automate the process of predicting human behavior*. This was the foundation of automated behavior analysis, or AuBA, described in this book for behavior-based predictive modeling of malicious behavior.**

Table 1-2: Advantages and Disadvantages of Modeling Individual Malicious Behavior

ADVANTAGES	DISADVANTAGES
The specific antecedents and consequences for one person allow prediction of specific behaviors.	The unique set of antecedents and consequences must be identified for each person modeled — one person, one model.
Data collection often takes less time than data collection for a group, because only the antecedents, behaviors, and consequences for that person are required.	It is more challenging to identify antecedents and consequences for the individual as compared to a group.
Unusual behavior of a person can be modeled.	You must be sure that a sufficient number and variety of behaviors for the person are captured.
Uncommon combinations of antecedents can be used to predict behavior under new conditions.	The predictive model for one individual is unlikely to generalize to another individual. We all are different.
If the person modeled has been covered sufficiently by the press, news articles may be used to extract antecedents, behaviors, and consequences.	Sufficient and multiple examples of behaviors under a variety of conditions are required.

The automated behavior analysis described in this book consists of a set of patented tools and methods proven to predict malicious adversarial behavior. AuBA automates much of the manual process required to conduct predictive modeling using elements of applied behavior analysis and adds numerous enhancements. Lessons learned have been incorporated into the new technology.

How Individuals May Vary

We are individuals. Like fingerprints, we are unique. Even if we observe identical twins, differences in behavior are readily apparent. These individual differences are developed from birth and maintained throughout life. The experiences within our environment tend to shape what we react to and how we react. The effects of our actions encourage us either to act the same way in the future when followed by desirable consequences or to change if the behavior is followed by undesirable consequences. Each experience is associated with a unique set of antecedents for the behavior we exhibit, and each behavior is followed by the effects of that behavior within the environment.

Our behavior within any context will receive immediate feedback from other individuals or from the physical environment itself. This ongoing and continuous environmental interaction adds to our innate biological and genetic design to make us who we are. The analysis of malicious behavior at the individual

level must take this into consideration. Identifying different behaviors of individuals to the same or similar antecedents indicates that the antecedent-behavior-consequence sequence across individuals is specific to the individual. For example, two children may grow up in the same neighborhood under similar family conditions. One attends college, and the other becomes a drug addict and becomes a murderer. The environments and family situations were highly similar, but the behaviors were entirely different. Why? If you read this book in its entirety, you will know the answer.

To highlight how individuals can be so different, the following types are presented as examples of malicious behaviors that are familiar to everyone. In these cases, something went wrong. More than likely the person's complex inner motivations interacted with the environment. However, we can understand the behavior and even predict it without knowing the inner mechanisms operating.

The Loner

Theodore ("Ted") John Kaczynski, known as the Unabomber, was a brilliant PhD mathematician. He was the youngest faculty member ever hired by the prestigious Berkeley University after skipping grades, starting Harvard at age 16, and earning his master's and PhD degrees in mathematics from the University of Michigan. It was obvious that Kaczynski was different very early in his life. First, he was brilliant, with a talent for math. Second, he did not socialize well, preferred not to interact with others, and appeared to prefer math to people. Both characteristics continued throughout his life; he excelled in mathematics and became increasingly focused on being alone. After teaching only a few years at Berkeley, with less than stellar performance, he resigned. At 29 years of age, he moved to a 10-by-12-foot one-room cabin in Montana, about the size of two queen-size beds put together. With no amenities, he lived an austere life as a recluse.

While a recluse, Kaczynski sent a total of 16 bombs over 17 years that killed 3 people and injured 23. Antecedents to his attacks included individuals associated with technology — universities and airlines in particular. In fact, the term *Unabomber* is derived from the terms *un*iversity and *a*irlines. The primary consequence of his bombing behavior was success. For many years he evaded detection and capture — at least until his suspicious brother notified the FBI. Needless to say, Kaczynski has not acknowledged his brother David's attempts to communicate with him since his imprisonment.

The Chameleon

As described earlier in this chapter, Ted Bundy was one of the most violent serial killers in American history. Bundy was, by all accounts, a brilliant law student with a long-term girlfriend. He obscured his serial-murder lifestyle by

posing as a socially acceptable person liked by many. Bundy was a chameleon. He drastically altered his behavior to match the existing conditions, much like a chameleon lizard changes its color to match the background so that it will not be detected. He existed as a nice young man in public and was one of the worst serial murderers in our country's history in private. Interestingly, both sets of behavior, public and private, were associated with their own sets of antecedents and consequences. Ted Bundy is a good example of how a person can live a double life.

The Social Misfit

On April 26, 2007, Seung-Hui Cho shot and killed 27 fellow students and 5 faculty members and injured 25 others at Virginia Tech University. Cho committed his shootings in two attacks separated by only a few hours. The threat exhibited by the first set of killings was not communicated throughout the campus. Cho then came back and continued killing and injuring staff and students.

Cho had a mental-health-troubled youth that included a series of psychiatric diagnoses. The details of this troubled past were withheld from the university. Cho simply did not fit in. His behavior was tainted with violent overtones, stalking, and handguns. As a child he was occasionally bullied at school, which was an unpleasant, painful experience for him. Monday morning quarterbacking suggests this was a key to his later attacks. The antecedents to these two attacks were clear — students and faculty. Likely representing Cho's school problems over many years, the unfortunate victims may have been stand-ins for all his past problems.

As part of the violent theme that plagued Cho, he chose hollow-point rounds for his shootings. As part of my orientation to the U.S. Secret Service as a research psychologist, I observed a special agent demonstrate the power of a hollow-point round at the firing range. Using a typical pointed round, he first shot a gallon jug of water at a distance of about 75 feet with his 9-millimeter pistol. The bullet cleanly went in the front of the jug, traveled through, and exited the back. Water streamed out of the entrance and exit holes. It was obvious that this type of bullet could go through a body. Then, using the same type of bullet but with a hollow-point head, the agent shot another water-filled jug. This jug literally exploded, with water spewing in every direction, like a water balloon dropped from a tall building onto the pavement. It was a chilling exercise. Given the same firepower and an identical shell, the simple fact that the bullet's head had an indentation made the projectile much more deadly. The only reason to shoot someone with a hollow-point round is to minimize the victim's chances of survival.

Cho was a social misfit with a great deal of internal rage. Unfortunately, he did not surface as a concern even in the midst of many danger signals. He had exhibited severe mental issue since childhood, as recognized by school staff from elementary school and high school. His choice of the type of bullet used

is significant. A hollow-point bullet is meant to kill, not to wound. Armed with extremely lethal firepower, he clearly meant to kill. In addition, not only did he engage in a shooting, he came back a second time to complete more lethal acts. Combining Cho's very troubled background with the selection of firepower with hollow-point ammunition indicates that he was deadly serious.

The Individual versus the Group

This chapter has focused on the behavior analysis of the individual versus the group. In summary, the group is often easier to model than the individual. The primary considerations in predicting the behavior of the individual versus the group are identifying the following:

- The antecedents leading to the defined behavior of interest that are specific to the individual
- The consequences of malicious behavior, the desirable consequences that maintain or increase the frequency of occurrence of the behavior, or the undesirable consequences that result in a decrease in the occurrence of the behavior in the future

The next chapter focuses on the group versus the individual. The methods are similar, but the differences are significant. The focus will be on these differences. The group works to keep members similar in terms of beliefs and behaviors to maintain the group's integrity and identity. Because a group acts more as one entity, in some ways analyzing the group is easier than analyzing an individual. It is true that the individual is loosely tied to usual ways of behaving and can change behavior quickly. However, individuals are still creatures of habit. As humans, we all exhibit patterned behavior, and that makes our behavior predictable.

NOTE **AuBA exists as the only patented automation and extension of applied behavior analysis. Compared with manual modeling methods, the AuBA methodologies and tools have numerous advantages. At the end of each chapter a key advantage of this new technology will be presented.**

Advantages of AuBA #1: Automated Summarization

This chapter describes basic behavioral principles for analyzing individual behavior. These principles are very important because they provide a way to analyze behavior when the perpetrator is or is not known. Many psychological methods depend heavily on direct observation of the person being analyzed. Over the course of two decades, my teams and I have moved the basic applied behavior analysis approach to the use of text accounts of past behavior as a

corpus to replace direct observation. This is important because in comparison to clinical settings, where the person is available for observations and environments are constrained, text accounts of past behaviors may be used to replace direct observation. Figure 1-2 shows the basic AuBA process. Basically, text-based documents are presented to the first automated tool, ThemeMate. The output of ThemeMate is then forwarded to AutoAnalyzer, and the completed predictive engine is then embedded in the predictive application.

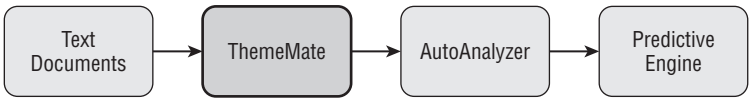


Figure 1-2: The AuBA process that processes textual accounts of past behavior to produce a predictive engine using two automated tools, ThemeMate and AutoAnalyzer

There are many advantages to AuBA. At the end of each chapter, a specific feature of the technology will be described. This chapter highlights one of the primary features of ThemeMate, and the following list highlights some of the primary features of ThemeMate that will be presented across chapters.

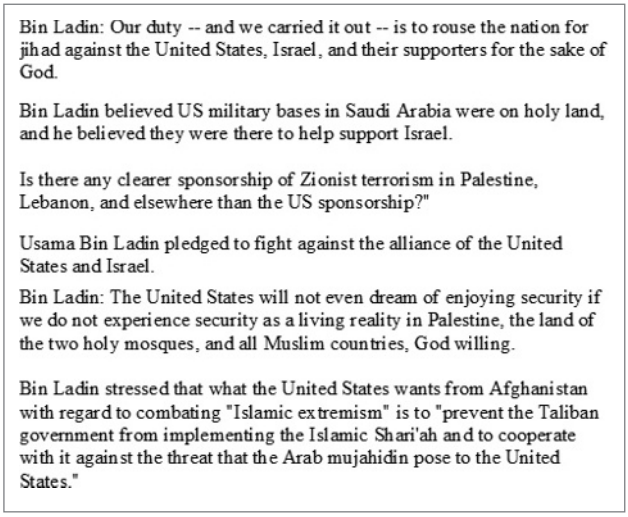
- The AuBA methodology includes automated methods to accurately identify antecedents and consequences of past behaviors in text-based reports and news articles describing past behaviors.
- ThemeMate summarizes large numbers of documents describing past behavior, identifies the most important features across all the documents, and presents salient features.
- ThemeMate automatically extracts antecedents associated with behaviors and constructs a data array, which is processed by AutoAnalyzer.
- AutoAnalyzer automatically conducts advanced behavior analytics to develop and validate predictive engines that may be used to accurately predict future behavior.

Although the accompanying DVD demonstrates these model-building tools, I will provide details in each chapter that demonstrate different advantages of AuBA. This chapter highlights a very useful feature — the automated identification of key points across all documents submitted for processing. This is a specific feature of ThemeMate. The feature enables us to submit a single document or collection of documents to ThemeMate to obtain the *x* number of key points embedded in the text. The user can specify how many key points are to be returned. This automated *CliffsNotes*-like feature is very valuable in summarizing all content very rapidly. Currently, ThemeMate provides this summarization in English or Arabic, but it can be readied to work with any new language in approximately two weeks. When I designed ThemeMate, it was based on the cognitive process

we use to extract key points and to extract antecedents associated with behavior. Comparing the automated ThemeMate extraction to human extraction of key points returns highly similar or the same summarization points.

To demonstrate this ThemeMate feature, I collected more than 150 separate open source documents of Osama bin Laden's statements, speeches, interviews, fatwas (declarations of war), and threats. I submitted all these text documents to ThemeMate and set the option to summarize all documents by providing the six most important points across all documents. There are two reasons for using ThemeMate to do this: (1) Such a summary has been shown to be highly similar to an analysis completed manually by a SME, and (2) ThemeMate can conduct the extraction and summarization across languages (for example, English and Arabic) and can provide key motivation points for an individual or group if it contains statements made by the individual or group, interviews, and authoritative articles about the individual or group. The primary difference between this AuBA automation and a manual analysis is that it took ThemeMate 90 seconds to complete its analysis for this demonstration, whereas it can take an SME many weeks to study and extract key features. Thus, the actual use of this feature is simply left to the imagination of the user.

Figure 1-3 presents the unedited results of the ThemeMate analysis of the more than 150 documents. As a manual comparison, it is followed with an expert assessment of Osama bin Laden's motivations. This assessment was produced by Michael Scheuer and extracted from a transcript video of an interview of Scheuer conducted by Alan Bock. This interview may be viewed at `www.youtube.com/watch?v=bYZizO0f0lk&feature=player_embedded#!`.



Bin Ladin: Our duty -- and we carried it out -- is to rouse the nation for jihad against the United States, Israel, and their supporters for the sake of God.

Bin Ladin believed US military bases in Saudi Arabia were on holy land, and he believed they were there to help support Israel.

Is there any clearer sponsorship of Zionist terrorism in Palestine, Lebanon, and elsewhere than the US sponsorship?"

Usama Bin Ladin pledged to fight against the alliance of the United States and Israel.

Bin Ladin: The United States will not even dream of enjoying security if we do not experience security as a living reality in Palestine, the land of the two holy mosques, and all Muslim countries, God willing.

Bin Ladin stressed that what the United States wants from Afghanistan with regard to combating "Islamic extremism" is to "prevent the Taliban government from implementing the Islamic Shari'ah and to cooperate with it against the threat that the Arab mujahidin pose to the United States."

Figure 1-3: The output of ThemeMate when set to return the five most important points contained in the more than 150 Osama bin Laden–focused documents presented for analysis.

As background, Scheuer headed the Osama bin Laden–focus team at the CIA from 1996 to 1999, as reported in open source reviews of his books and this taped interview. I was familiar with his work from inside the CIA, as well as his books, which were completed more recently. Scheuer is perhaps the world's authority on the motivations of Osama bin Laden and al-Qaeda. His assessment in the taped interview is the result of many years of studying Osama bin Laden's actual words in speeches, warnings, and so forth. His controversial views are the results of actually analyzing the content of bin Laden's words. Scheuer has drawn different conclusions based on actual study of bin Laden's words. Therefore, ThemeMate and Scheuer should agree, to some extent, as both are processing actual speeches, interviews, and so forth. We would not expect an exact match, because the documents are not identical, but we should see a strong similarity.

Scheuer's analysis of the true motivations of bin Laden presented in the recorded interview provided four key motivational points for Osama bin Laden. These points as presented in the interview were:

- The United States actively supports Israel.
- The United States occupies lands in the Arab peninsula.
- The United States supports tyrannies that govern most of the Arab world.
- The primary goal is to evict the United States from their lands.

A comparison between the careful analysis that Scheuer completed after years of study and the 90-second ThemeMate processing of documents reveals the close comparison between the separate analyses. Scheuer should be complimented on his objective analysis drawn from content analysis, not bias. ThemeMate automatically provides a rapid, nonbiased assessment that cannot be influenced by external or political pressures.

In Summary

This is an important introductory chapter on the topic of predicting individual adversarial threatening behavior that can impact our national security. The work, methods, and procedures I have discussed are a unique application and automation of applied behavior analysis — a field in psychology that emphasizes influencing and predicting individuals' behavior. AuBA is the SAIC-owned, author-invented, new set of tools and methods for security to help ensure our protection as a nation. AuBA is proactive, not reactive. Behavioral methods applied to terrorism, insurgency, war, network hacking attacks, and insider threats represent a paradigm shift in human predictive technology. They move from current reactive approaches to proactive methods that have been proven to predict threatening behavior in real time.

The methods described in this chapter have proven that antecedents to adversary behavior can be extended to the following:

- Network packets for computer network prediction
- Physical sensor output to serve as antecedents that convert sensor-based tracked movement of individuals into predictions of malicious intent
- Test extraction from past text accounts of adversarial behavior
- A unique way of capturing antecedent, behavior, and consequence information from SMEs when data is sparse or missing

Remember these key points:

- Adversarial behaviors on a global basis are associated with predictive antecedents and identifiable consequences.
- Behavior analysis principles can reliably predict adversary behavior.
- Following the principles and methods described in this book can allow us to move from a reactive security policy to a more proactive stance in which we can anticipate attacks before they happen.
- If you absorb and use the methods and procedures presented in this book, you can effectively predict future occurrences of malicious behavior.