Attack on AMERICA:

The First War of the 21st Century

David J. Shaughnessy and Lieutenant Colonel Thomas M. Cowan, U.S. Army

The terrorist attacks of 11 September 2001 rocked the nation in ways that will reverberate for years. The authors discuss how these attacks signal shifts in the modus operandi of international terrorism—shifts in purpose, organization, weapons, and capability.

Today, our fellow citizens, our way of life, our very freedom came under attack in a series of deliberate and deadly terrorist acts.

—President George W. Bush in his address to the nation, 11 September 2001

AS THE SOLE SUPERPOWER in a world increasingly defined by global markets, economic institutions, and societal norms, the United States is involved in world affairs to a degree unprecedented in its history. Its national success and prolific engagement, enacted within a framework of personal freedom, human rights, and Christian morals, have created resentment among other nations as well as religious, ethnic, and political factions in the world. Its national strengths—strategic location, economic strength, and military power—have served to protect it from conventional attacks resulting from these hostile views. However, its national character—democratic principles, individual freedom, and human rights—serve to increase its vulnerability to asymmetric, unconventional, or indirect actions. It remains clear that any campaign conducted against the United States, today or in the foreseeable future, will be a mix of asymmetric, adaptive, and conventional operations against the nation's vulnerabilities.

The 11 September 2001 terrorist attacks on the World Trade Center and the Pentagon, and the 2000 attack on the USS *Cole* are examples of asymmetric or asynchronous acts carried out by an adaptive and thinking opponent who continually studies the strengths and weaknesses of his perceived enemy and adapts his operations accordingly. These attacks were not without a larger purpose. They are part of an ongoing campaign that is likely to continue and expand.

The Nature of the Act

Terrorism is a tactical action that is designed to generate an operational or strategic effect. It is the creation of an event that has broader consequences than that created by the event alone. By its very nature, terrorism is asymmetric. It seeks to employ a capability that affords no defense or effective counteraction. This makes terrorism a viable means for less capable organizations to attack more capable opponents. At its very root, terrorism strikes at the will of the people, the credibility of the government, and the effectiveness of national security.

Terrorist acts can be linked together in the form of a campaign but will be more effective when employed as part of a strategy employing other elements of power in a more conventional framework.

This permits consistent operations that are continuous and complementary. The application of other elements of power need not be overt and in fact might be more effective when employed covertly. They could involve information operations, diplomacy, or economic leverage as well as more conventional military operations. For example, a state or organization that knows in advance that a significant event is going to occur could conceivably set economic conditions so as to profit from that event. It is the asymmetric nature of these tactics that affords the greatest opportunity for success against more powerful opponents, but it is their effect on conventional institutions that generates opportunity as a consequence of the event.

Terrorist tactics are normally employed in an asynchronous framework. It is their asynchronous character that gains the initiative for the terrorist. The terrorist picks the time and place of the event rather than having the time and place defined by its relationship to other operations. This represents an offensive framework that is driven by vulnerability, opportunity, and tailored capability rather than by fixed capability employed in a conventional construct. Because these events are asynchronous, however, does not mean that they are not part of a larger, more synchronized effort. In fact, it is becoming increasingly more likely that future terrorist tactics will be employed in a more synchronous operational framework. The ability to continuously choose the time and place of events allows the threat to control the operations tempo, thereby always retaining the initiative. To U.S. opponents, it is apparent that these tactics, planned and prepared in advance, allow a regional actor to keep a more capable adversary off balance without significant investment in visible and costly capabilities.

Terrorist tactics are normally employed in an asynchronous framework. It is their asynchronous character that gains the initiative for the terrorist. . . . Because these events are asynchronous, however, does not mean that they are not part of a larger, more synchronized effort. In fact, it is becoming increasingly more likely that future terrorist tactics will be employed in a more synchronous operational framework.

A Campaign Framework

History has demonstrated that single, isolated acts of terrorism may have profound effects on perceptions, policy, national strategy, or even national will; however, lasting effects involving significant change in the nature of government or long-term national goals have been unattainable through single acts. A long-term campaign with multiple lines of operation is required. This could be a campaign of asynchronous events to wear down and shape outcomes, such as the former Soviet Union sponsored events during the Cold War, or a campaign employing all elements of power in conjunction with and complementing terrorist acts.

As an accepted mode of operation, state-sponsored terrorism came of age during the Cold War when the Soviet Union guaranteed the survival of states that supported or conducted acts of terror against the United States and it allies. While today there are still states that sponsor terrorism, none do so overtly.

Terrorism remains a viable and effective tactic, but its use is less and less acceptable to the international community when employed in an asynchronous framework short of declared hostilities. Under conditions of limited warfare or in time of peace, it is a heinous act unacceptable to most nations. However, within a framework of total war, terrorism would be retitled asymmetric operations and become accepted for achieving national objectives. For this reason, many states hostile to the United States covertly support transnational organizations capable of conducting terrorist acts. These organizations are employed for campaigns short of war and permit distance and deniability by the supporting states within the international community. At the same time, these states are developing capabilities for employing asymmetric means and

Judging from more recent attacks, however, it appears that new and less predictable patterns are emerging. Rather than a fixed capability looking for an opportunity, the threat appears to be designing the capability to attack assessed vulnerabilities. This presents a significant problem in that the characteristics of each event are likely to be different.

tactics should open warfare break out. Future operational environments will contain state as well as transnational organizations with the capability to conduct asymmetric operations both inside and outside the area of operations as part of an overall operational design.

As the nation grows stronger, the value of these operations increases, making them more likely to be a major part of any future military operation. Asymmetric operations are conducted within a campaign framework and strikes at the will of the American people, the perceived center of gravity of the United States, rather than at the fringes. Within the scope of unlimited war, all targets are justified: population centers, infrastructure, industry, and the military. The end state for the terrorist or asymmetric operation is achieving operational or strategic goals, including denial, exclusion, or defeat of the United States and its allies.

Adaptive operations. The decrease in numbers of terrorist acts over the past decade has more to do with the increasingly fixed mode or pattern of operation than desire or intent. While still difficult to detect, known actors, employing logical methods of operation and using recognizable capabilities, offer indicators that could be identified and targeted, which would reduce terrorists' opportunities significantly. Judging from more recent attacks, however, it appears that new and less predictable patterns are emerging. Rather than a fixed capability looking for an opportunity, the threat appears to be designing the capability to attack assessed vulnerabilities. This presents a significant problem in that the characteristics of each event are likely to be different. The pattern of operation is designed uniquely for the target that the terrorist plans to strike. A lack of predictability requires more resources for intelligence collection and analysis, and a broader range of protective measures to defend against a wider range of possibilities.

The attacks of 11 September represent a significant change in pattern and tactics, and fit the new emerging model. U.S. law enforcement has routinely and successfully monitored hazardous goods that may be employed as weapons, a practice strengthened by the Oklahoma City bombing. Recognizing this obstacle, terrorists adapted their attack means by smuggling explosives into the United States rather than attempting to obtain them from sources within the country. This approach met with only partial success and, in the process, increased border security and cooperation between the United States and its neighbors. Recognizing this new factor in the security environment, the methodology was again modified, this time creating the kinetic effect of explosives—a fully fueled, large aircraft—without the inherent intelligence indicators that could compromise the attack while bypassing personnel and vehicle control measures at the World Trade Center implemented after the 1993 attempt. In this instance, the organization leveraged U.S. resources to train pilots and provide the weapons. From air security protocols, terrorists devised a plan to smuggle low-metal-content weapons onto aircraft and used the pilot and crew training to cooperate with hijackers to gain control of the aircraft.

Leveraging sanctuary. Operating from dispersed locations in multiple countries provides a high degree of sanctuary from direct attack. Transnational terrorists rely on their strategically secure positions to deflect the conventional strengths the United States could otherwise employ to destroy their organizations. By seeking sanctuary in areas difficult to attack by using high-tech, precision standoff engagement, terrorist organizations protect themselves from forms of retaliation that they have limited means to counter symmetrically. In the case of Osama bin Laden's organization, it has embedded itself in a nation whose economic and physical infrastructure is too underdeveloped to threaten, yet

US Navy

The destroyer USS *Cole* positioned on the deck of the Norwegian heavy transport ship M/V *Blue Marlin* during its 5-week trip back to a U.S. drydock. The 11 October 2000 attack off the coast of Aden, Yemen, killed 17 crew members and injured 39 others.

The 11 September 2001 terrorist attacks on the World Trade Center and the Pentagon, and the 2000 attack on the USS Cole *are examples of asymmetric or asynchronous acts carried out by an adaptive and thinking opponent who continually studies the strengths and weaknesses of his perceived enemy and adapts his operations accordingly. These attacks were not without a larger purpose. They are part of an ongoing campaign that is likely to continue and expand.*

is still capable of mounting a formidable defense on rugged terrain. This has provided a nearly ideal sanctuary that poses more dilemmas to the United States than can be countered from standoff precision targeting. Even successful attacks against elements in sanctuary may not defeat the network, that extends over a wide number of nations and nonnations and carries substantial risks to U.S. forces conducting conventional operations. From this position of relative security, bin Laden's group has the flexibility and security to retain the initiative and remain on the strategic offensive.

The employment of sanctuary also uses international law and trade practices against the United States. Transnational organizations use international banking processes designed to encourage free trade to receive and disburse the funds needed to attack various targets while remaining nearly undetected. Transnational groups also hide behind international law, protecting themselves and their sponsors by

Chicago firefighters join the rescue effort at the World Trade Center site.

Federal Emergency Management Agency

Asymmetric operations are conducted within a campaign framework and strikes at the will of the American people, the perceived center of gravity of the United States, rather than at the fringes. Within the scope of unlimited war, all targets are justified: population centers, infrastructure, industry, and the military. The end state for the terrorist or asymmetric operation is achieving operational or strategic goals, including denial, exclusion, or defeat of the United States and its allies.

demanding legally admissible evidence. This level of proof does not normally exist because of the manner in which terrorists are organized and operate; when it is available, it often cannot be presented to the public without compromising intelligence sources or methods.

If the United States elects to attack, transnational terrorists frustrate targeting by having a signature undetectable to high-tech collection systems, by dispersing into complex terrain, or blending into the civilian population. All these techniques are designed to defeat the United States' undisputed asymmetric advantage in high-tech, precision standoff weapons. U.S. security procedures have been designed primarily to detect, rather than to defend against, a determined attacker.

Information Operations

Regardless of whether he is responsible, the 11 September attacks raise bin Laden's prestige in the Muslim extremist world and attract additional followers and money to his cause. It also gives other organizations and states insights into U.S. vulnerabilities. The United States may appear weak to opponents if it is unable to respond to the attack effectively. The visibility of this event and its dominance in the media provide opportunities for a wide range of actors to take advantage of this act.

Photo not available

Transnational terrorists rely on their strategically secure positions to deflect the conventional strengths the United States could otherwise employ to destroy their organizations. By seeking sanctuary in areas difficult to attack by using high-tech, precision standoff engagement, terrorist organizations protect themselves from forms of retaliation that they have limited means to counter symmetrically.

Carefully planned and executed adaptive campaigns of terror attempt to demoralize the nation, frustrate U.S. policies for reaction and retaliation, reduce U.S. regional presence, and paralyze the national will by exploiting the vast U.S. information system. Information systems expand the impact of the event and create strategic effects. On the international scene, well-publicized, effective events may serve to fracture coalitions by focusing other nations inwardly.

Furthermore, consistent denial of responsibility is a new tack taken by transnational terrorists. It counters the information and diplomatic superiority of the United States and creates doubt. It allows nations to support terrorism without international repercussions.

A successful attack on the United States must be conducted against the systems upon which it relies for its dominance. This consists in large part of military and economic complexes that have formed pillars of U.S. foreign policy. The attacks on 11 September were more than symbolic; they targeted the command and control of the nation's economy and military. Normally, isolated attacks not part of a conventional campaign can be expected to focus on symbolic targets for their media value and strategic

The 11 September attack raises bin Laden's prestige in the Muslim extremist world and attracts additional followers and money to his cause. It also gives other organizations and states insights into U.S. vulnerabilities. . . . The visibility of this event and its dominance in the media provide opportunities for a wide range of actors to take advantage of this act.

implications. When asymmetric or terrorist attacks are conducted as part of a more conventional campaign, they will more likely target operational or strategic capabilities. Within the framework of a terrorist campaign, terrorists understand that defeating the United States is not a matter of winning battles but rather of continuously applying psychological and physical pressure to damage the political, economic, and military foundations of power.

Access denial. Strategic preclusion attempts to deter or reduce the deployment of U.S. forces. Sympathetic or supporting nation states lend support to strategic preclusion efforts by calling for the use of diplomacy, citing the absence of proof that links the group to the act and imposing economic measures that threaten coalition partners' interests. These actions are often disguised as respect for international law or a desire for a peaceful resolution.

Operational exclusion attempts to prevent regional neighbors from allowing or assisting the deployment of U.S. forces. Adversaries have long recognized the United States' need for significant staging areas. The adaptive transnational terrorist threatens regional neighbors with attacks and terror in the event they cooperate with or provide staging areas for U.S. forces. State sponsors of transnational terrorism conduct diplomatic and information campaigns to persuade regional states that the United States is an unreliable partner and that cooperation will lead to regional economic and diplomatic isolation.

Thwarting U.S. intelligence. Terrorist organizations rely on secrecy to plan and prepare attacks. Compartmented organization, brutal enforcement of loyalty, and recruiting criteria based on political and religious reliability allow better protection of information than is possible in the nation states that terrorists attack. In a strategic defensive posture, the United States is unable to force its opponent into an activity that might compromise locations and intentions. Not only does asynchronous timing lend security to terrorists, but it also necessitates vigilance by U.S. intelligence organizations to discern terrorist activities and intentions. Furthermore, to counter the ability of intelligence operations to detect plans and preparations, the terrorists employ deception. This includes deliberately leaking false information and statements to the media to mask the true plan and to desensitize and confuse intelligence analysis.

The vast U.S. intelligence system was designed to monitor the former Soviet Union and is built around technology. Human intelligence has been relegated to secondary importance and used largely to support diplomacy. This imbalance has created predictability and limited depth of collection. Also, the United States has focused on states rather than on transnational organizations, and U.S. analysis was designed to assess the conventional capabilities adversaries possess and employ. Last, the intelligence community functions well during times of crisis but lacks the analytical and human intelligence underpinnings to sustain the necessary level of effort this new operational environment requires. Success in the long term against an adaptive and determined transnational opponent demands a less predictable process, combined technical and human systems engaged against all threats, continuous operation at peak performance, and engagement well before a crisis.

Implications

Transnational organizations retain the strategic initiative and bring to bear the means of adaptive attack by controlling operations tempo. Acts of terror rely on surprise to magnify the psychological impact of each event. Unconstrained by the need to retain terrain or to follow one success with another, either of which would provide a predictable pattern of operations, the transnational terror organization

Strategic preclusion attempts to deter or reduce the deployment of U.S. forces. . . . Operational exclusion attempts prevent regional neighbors from allowing or assisting the deployment of U.S. forces. . . . The adaptive transnational terrorist threatens regional neighbors with attacks and terror in the event they cooperate with or provide staging areas for U.S. forces. State sponsors of transnational terrorism conduct diplomatic and information campaigns to persuade regional states that the United States is an unreliable partner.

can select times and targets that suit its resources, planning abilities, and the security environment. The 1993 attack on the World Trade Center and the 2000 attack on the USS *Cole* had no effect on the long-term success of the campaign that eventually led to the highly successful 11 September attacks, nor was the timing of the attack related to any other tactical event, which made it impossible to determine a pattern or predict the next attack.

Terrorist actions are likely to be continuous in nature but not continuous in rhythm or frequency. Adaptive terror actions are not simply isolated events but are linked to other goals and operations—economic, political, and even military, when feasible. They are also likely to take many forms and contain several lines of operation working simultaneously or orchestrated in space and time. Terrorist activities will range from nonlethal activities such as information operations, to lethal activities such as direct action using varied conventional low- to high-technology means and weapons. Future terrorist actions involving weapons of mass destruction or effects cannot be discounted. Collection against these activities requires an intelligence system as flexible, proactive, and adaptive as the organizations it targets.

Unconventional attacks against the U.S. homeland are part of every future opponent's strategy and will be part of its force design and capabilities. Repeated attacks against the U.S. homeland change social, economic, and political behavior; limit personal freedom; impede free trade; inflict psychological stresses; and damage the nation's international standing as a world economic and military power.

Terrorists stress adaptation and flexibility to preserve their organization and ensure their continued power. They conduct strategic operations to degrade U.S. national will, fracture alliances and coalitions, and limit the scope of U.S. involvement abroad. Their ability to adapt faster than defensive measures can complicate U.S. efforts to remain in the strategic defensive. Operations conducted without discernible frequency or patterns require the United States to maintain a socially, politically, and economically expensive posture of constant readiness, which itself does not guarantee success. Intelligence operations assist in reducing the need for constant readiness but are not infallible and must be flexible, adaptive, and broad in scope. Taking the strategic offensive can eliminate an opponent, but it requires exceptional intelligence and an adaptive force capable of fighting on a battlefield of unprecedented complexity, fluidity, and lethality. These challenges can only be met by creating an adaptable military force capable of dominating this environment. ***MR***

David J. Shaughnessy is the senior intelligence analyst for Headquarters, U.S. Army Training and Doctrine Command, Deputy Chief of Staff for Intelligence, Fort Monroe, Virginia. He has more than 34 years of federal service, including 8 years of Active Army service.

Lieutenant Colonel Thomas M. Cowan is a military intelligence officer, Headquarters, U.S. Army Training and Doctrine Command, Deputy Chief of Staff for Intelligence, Fort Monroe. He has served in a variety of intelligence positions from battalion to major command level. He is a graduate of the U.S. Army Command and General Staff College and has a Master's degree from Saint Mary College, Leavenworth, Kansas.