The Cold War on Terrorism: Reevaluating Critical Infrastructure Facilities as Targets for Terrorist Attacks

by David Riedman

Portions of this article are excerpted from the author's Center for Homeland Defense and Security master's degree thesis "How Critical is Critical Infrastructure?" The full document is available in the Homeland Security Digital Library.[1]

> Countries are inverted pyramids that rest precariously on their strategic innards--their leadership, communications, key production, infrastructure, and population. If a country is paralyzed strategically, it is defeated and cannot sustain its fielded forces though they may be fully intact.
>
> — Colonel John Warden, Air Theory for the Twenty-First Century[2]

Abstract

Nationally significant infrastructure facilities whose loss can cripple the essential functions of the entire country would be attractive targets for an enemy nation-state to strike with ballistic missile and airpower capabilities during a strategically-planned campaign against the United States. Terrorists lack the intelligence, organizational coordination, manpower, and resources to conduct a strategic warfare campaign with the intent of crippling essential-to-life systems across the country. The strategic warfare approach, which hinges on identifying, understanding, and targeting the interdependencies across infrastructure systems, does not match the capabilities or previous target selection patterns of terrorist groups. The Department of Homeland Security's current infrastructure protection policies are rooted in the theories of strategic warfare and make the flawed assumption that critical infrastructure facilities are the same targets that terrorists would have the intention and capability of attacking.

Suggested Citation

David Riedman. "The Cold War on Terrorism: Reevaluating Critical Infrastructure Facilities as Targets for Terrorist Attacks." *Homeland Security Affairs* 13, Article 3 (June 2017). https://www.hsaj.org/articles/13976

Introduction

Infrastructure facilities which are essential for the continued functioning of the entire country would be attractive targets for an enemy nation-state to strike with ballistic missiles and aircraft during a strategically planned war against the United States. The current terrorist threat comes from homegrown violent extremists who are motivated to inflict mass casualties in locations that are visible and easily accessible. Examples of these types of attacks would be the recent ISIS-inspired shootings in Orlando and San Bernardino.[3] These terrorists lack the organizational intelligence, coordination, manpower, and resources to conduct a sustained series of precise attacks with the intent of crippling essential-to-life infrastructure systems across the country. Employing a strategic warfare approach hinges on identifying, understanding, and targeting the interdependencies across infrastructure

systems. Terrorists are not capable of waging strategic warfare, and conducting attacks against infrastructure systems would be a radical departure from their previous target selection patterns across the world. The Department of Homeland Security's infrastructure protection policies are rooted in the theories of strategic warfare, and they make the flawed assumption that terrorists have the intention and capability of attacking critical infrastructure facilities.

Military Theory and Target Selection

> We must not start our thinking on war with the tools of war—with the airplanes, tanks, ships, and those who crew them. These tools are important and have their place, but they cannot be our starting point, nor can we allow ourselves to see them as the essence of war. Fighting is not the essence of war, nor even a desirable part of it. The real essence is doing what is necessary to make the enemy accept our objectives as his objectives.
>
> — Colonel John A. Warden, The Enemy as a System[4]

The primary component of the DHS critical infrastructure protection mission stems from the PPD-21 requirement to "reduce the risks to critical infrastructure [from] intrusions, attacks, or the effects of natural or man-made disasters."[5] To create a plan for the protection of critical facilities, the intentions of the enemy must first be understood. It is unlikely that a terrorist group operating in the United States has the capability to destroy a significant infrastructure target that provides life-sustaining services at the national level. A RAND terrorism risk modeling report, using a 10-ton explosive as the least likely type of bombing attack, found negligible terrorism risk outside of the top eight Urban Areas Security Initiative (UASI) cities, meaning that terrorists are not interested in targeting, and are not capable of destroying, the majority of infrastructure facilities across the country.[6]

The current terrorist threat comes from homegrown militants and members of violent extremist groups who are motivated to inflict mass casualties by killing and injuring as many people as possible in a location that is accessible to the public.[7] These individuals or small groups lack the intelligence, organizational coordination, manpower, and resources to conduct a strategic war campaign against nationally significant infrastructure targets.

Methods of Attack

Different military strategies have been taught and utilized by the United States and other modern militaries throughout history. The method of attack used is based on the strategic objectives, the ability to gather intelligence, military capabilities, and available resources. The Air Corps Tactical School theory[8] states that targeted strikes to specific facilities or functions can result in economic destruction which would lead to social collapse and defeat of the enemy. Lt. Col. Peter Faber, an expert in strategic aerial warfare, theorizes that targeted strikes provide the means to win a war in the following manner:

1. Modern nations rely on industrial and economic systems for production of weapons and supplies for their armed forces, for manufacture of products, and provision of services to sustain life. Disruption or paralysis of these systems undermines both the enemy's *capability* and *will* to fight.

2. Industrial and economic systems contain critical points, the destruction of which will break down these systems if bombs can be delivered with adequate accuracy to do this.

3. Air strike forces can penetrate air defenses without unacceptable losses and destroy selected targets.

4. Proper selection of vital targets in the industrial/economic/social structure of an industrialized nation, and their subsequent destruction by air attack, can lead to fatal weakening of an industrialized enemy nation and to victory through air power.[9]

Winning a war by employing targeted strikes requires knowledge of the enemy's key systems, intelligence to understand and select the critical points, having forces capable of making the attack, and avoiding unacceptable losses.[10]

Colonel Warden's *The Enemy as a System*[11] addresses infrastructure as the systems that are so important that "even minor damage to essential industries may lead the command element to make concessions."[12] The concessions may come because:

- Damage to organic essentials/essential systems (CI) leads to the collapse of the system.[13]

- Damage to organic essentials/essential systems (CI) makes it physically difficult or impossible to maintain a certain policy or to fight.[14]

- Damage to organic essentials/essential systems (CI) has internal political or economic repercussions that are too costly to bear."[15]

The homeland security definition of Critical Infrastructure (CI) is very similar to Warden's concept of organic essentials. DHS defines CI as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[16] Warden states that organic essentials cause a collapse of the system, which is the same as saying "debilitating effects." The systems that make it impossible to maintain a fight are the systems "vital to security, national public health, and safety." The organic essentials that cause great political and economic repercussions are the same as those that endanger the "national economic security." Thus, the current definition that DHS uses to describe CI closely aligns with Warden's organic essentials to target during strategic warfare.

The 2013 *National Infrastructure Protection Plan* operates under the assumption that "both domestic and international critical infrastructure assets represent potential prime targets for adversaries. Given the deeply rooted nature of these goals and motivations, critical infrastructure likely will remain highly attractive targets for state and non-state actors and others with ill intent."[17] Based on this research, infrastructure protection (IP) efforts are framed under an inaccurate assumption of the terrorist threat to them. CI protection policies should not focus on large-scale attacks to facilities when they have not been the target of the largest domestic terrorist attacks and have rarely been the target of the 130,000 terrorist

attacks across the world over the last 50 years. Terrorists have not previously targeted infrastructure and are unlikely to change their intentions in the future, which means that the way DHS views protecting infrastructure and preventing terrorism needs to be reformed.

Much of the current IP analysis conducted by DHS focuses on the attributes of individual facilities within separate functional sectors or subsectors of infrastructure. Military warfare strategies hinge on understanding the entire system that allows an enemy to function and then targeting the weaknesses that cause failures across the system. The focus on individual facilities that provide separate functions lacks the network-wide viewpoint necessary to understand criticalities and assign priorities within the entire infrastructure system, which prevents DHS from accomplishing the statutory protection mission.

Series Warfare

Unlike targeted strikes that are carried out with aircraft, in series warfare,

> a commander concentrates forces in order to prevail against a single vulnerable part of the enemy's forces. If the commander prevails, the army regroups forces and moves on to attack another point in the enemy's defense. While the attacking army regroups, the enemy army may counterattack or move to defend another position.[18]

This back and forth process is termed "serial warfare" because of the "subsequent maneuver and counter-maneuver, attack and counterattack, and movement and pause."[19] Series warfare continues until either army does not have the capabilities or will to continue fighting.

Parallel Attack

Combining multiple waves of targeted attacks and series warfare is at the core of the concept of parallel attacks which destroy a wide array of essential systems. The most important element of the parallel attack is understanding the targets that hold the highest value to the enemy system. Once the system is understood, a strategy must be developed to damage or paralyze it. A nation is likely to have a "small number of vital targets at the strategic level because most systems only cause localized disruptions if damaged."[20] The nationally significant targets "tend to be small, very expensive, have few backups, and are hard to repair."[21] These targets align with the same concept as DHS's definition of CI, which are interdependent systems that cause system-wide failures.

Figure 1: Process of Actions during Strategic Warfare

If a significant percentage of key targets are struck in parallel, the damage becomes insurmountable. The enemy can mitigate the effects of serial attacks by "dispersing the location of critical targets, by increasing the defenses of targets that are likely to be attacked, concentrating resources to repair damage to single targets, or conducting a counteroffensive."[22] The purpose of the parallel attack is to target the attacks in a manner that deprives the enemy of the ability to respond effectively to mitigate the impacts. The higher the number of significant targets destroyed during each set of strikes, the higher the likelihood of debilitating the enemy.[23] The current DHS strategy of protecting CI by adding redundancies and hardening targets directly relates to the concept of identifying and protecting key targets from the parallel attack.

Mass Casualty Attacks

Online publications, such as The Islamic State's *Dabiq* and Al Qaeda's *Inspire*, have provided instructions for supporters to carry out small-scale attacks with homemade conventional explosive and small arms. The intent of these attacks is to inflict as many deaths and injuries as possible by targeting crowded public areas and special events. An example of this tactic was the April 15, 2013 Boston Marathon bombing attack where two radicalized individuals produced small homemade explosives that were detonated at the crowded finish line area of the city's annual marathon.

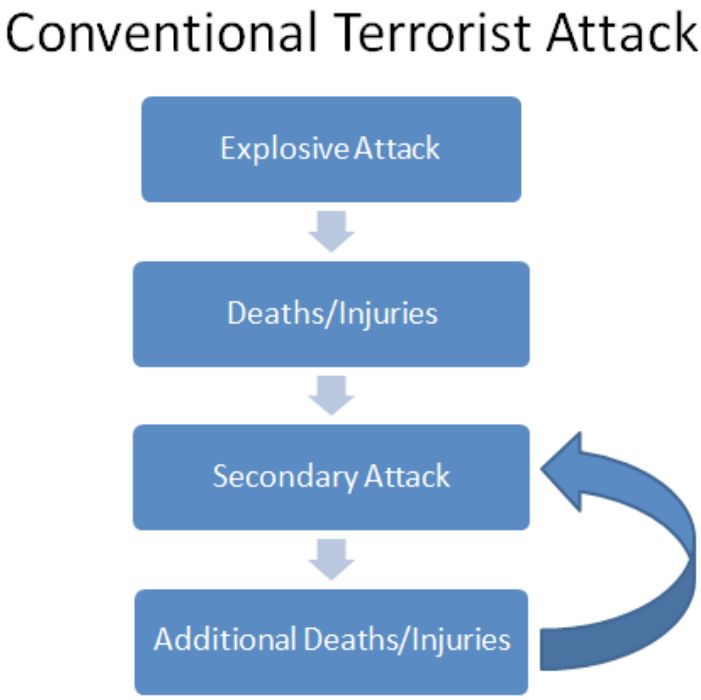

Figure 2: Process of Actions Occurring During Conventional Terrorist Attacks

The likely purpose of these attacks on the general public was to kill and injure people to cause fear. A terrorist attack of this manner on infrastructure would serve a different purpose than a focused military strike on infrastructure intended to cause cascading impacts to the systems that underpin the functions of the United States.

Mutually Assured Destruction

The underlying theory of nuclear war between multiple super-power nations is that if a nuclear weapon were detonated, mutually assured destruction would occur to all nations involved due to nuclear counterattacks. In the end, nobody would win the nuclear war because the casualties and damage on every side would be catastrophic.

The mutually assured destruction concept is applicable to planning critical infrastructure protection based on the size of an attack that would be required to damage a critical system. If a terrorist group were to obtain and use the massive amount of explosives (a theoretical 10,000 pounds or more of explosives exceeding the size of the Oklahoma City federal building attack) that would be needed to destroy a large dam, that group would be assuring its own destruction because the full power of the country's military and law enforcement agencies would be focused on responding. It is unrealistic to plan for, or protect against, attacks of this scope at infrastructure facilities because it is unlikely that terrorist groups could obtain, utilize, or even be motivated to possess such a large quantity of explosives. Increasing physical security at a facility with taller fences and stricter identification checks designed to stop a small-scale attack would also not deter the large-scale attacker who has already accepted that mutually assured destruction.

Warden's Five Ring System Theory

Warden's five-ring system theory is a concentric ring concept, as shown in Figure 3, of targeting the central rings that hold the highest strategic value (the central ring is also the smallest target). In the rings beyond the highest value targets, the targets become larger but have less strategic significance. Warden selected five general systems that he believed were key centers of gravity to exploit against any enemy (leadership, organic essentials,[24] infrastructure, population, and fielded military forces).

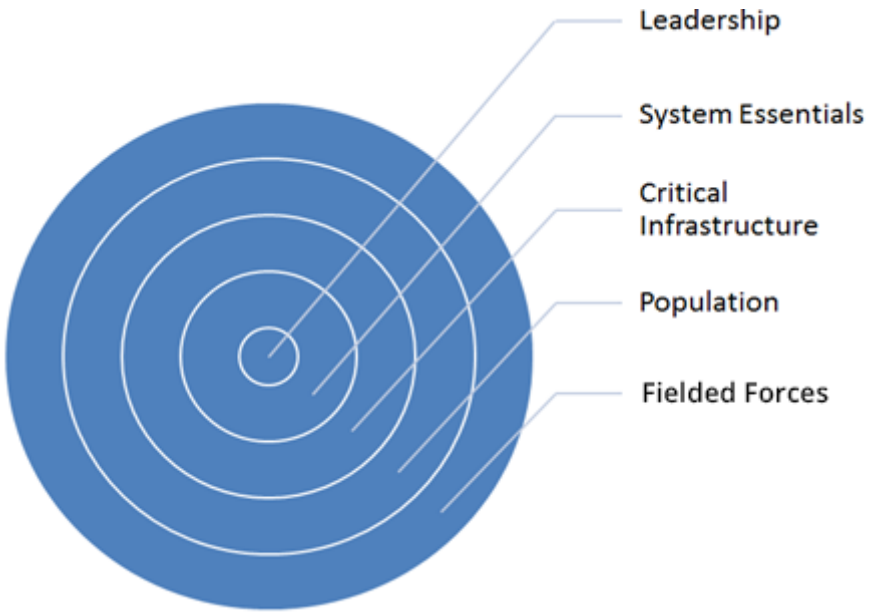

Figure 3: Warden's Five-Ring System Theory[25]

Warden's model provides a framework for how to defeat an enemy through destruction of critical components instead of engaging in combat with a conventional army.[26] This strategy is only effective if the attacker has the ability to identify and plan strategically how to destroy each of those systems in a specific order.[27] If military theorists trained in Warden's approach looked at how to identify and protect domestic infrastructure, they would likely think of it in terms of a concentric ring-based system. Warden's theory aligns with DHS's tiered approach to infrastructure protection as demonstrated by the target capabilities list, the national asset database, and annual mandatory threat, hazard, and risk assessments (THIRA) for states, counties, and local jurisdictions.

A flaw in applying Warden's theory to domestic infrastructure protection is that the strategic values of the targets within each ring are not static. Leadership can be adaptive and resilient, the relationships between systems can be too complex to understand completely, and most adversaries lack the resources necessary to conduct parallel attacks across a vast array of domestic targets.[28] These same problems are also evident in current critical infrastructure protection policies because as facilities are hardened, demand for services changes, populations shift, different technologies are developed, and the criticality of infrastructure facilities also changes. Compounding the problem, the concentric ring system is ineffective if the wrong facilities are identified as being the key targets. Placing non-essential systems

into the central rings creates a large core rather than concentric rings that delineate the importance of different assets.

Warden's theory depends on taking a snapshot of the enemy system and carefully analyzing it to understand the weaknesses in the system. This same strategy is not an effective method for analyzing vulnerabilities to domestic infrastructure over an extended period of time. Conducting assessments of infrastructure and creating tiered lists of resources would provide strategic planners with snapshots of the critical systems. But because the systems are not static, the value of targets changes over time and the target list becomes less and less useful. The effectiveness of the target list would also be contingent on how completely it captured the entirety of the system. Identifying individual facilities would only be useful if their destruction caused the cascading impacts that could cripple the essential functions of the enemy. The process of identifying these interdependencies would require an analysis of the entire system to determine the points of failure and then tracing the failures back to identify individual facilities as key targets. The current DHS policy identifies sectors of infrastructure and then identifies individual facilities within the separate sectors. This approach lacks the key "enemy as a system" concept of understanding the interdependencies and identifying the specific points of failure in the system. These points of failure are not broad sets of infrastructure systems; they are small areas of high strategic value in the center of the concentric rings.

Terrorism Differs from Strategic Warfare

The September 11, 2001 attacks on New York City and the Pentagon, the March 11, 2004 train bombings in Madrid, the July 7, 2005 London transit bombings, the 2010 attempted Atlantic airline bombings with ink cartridges concealing explosives, the 2015 Paris attacks, and the 2016 Brussels airport bombing are all examples of how the most sophisticated terrorist attacks in recent history are different from strategic warfare.

These attacks were not targeted strikes against essential systems intended to cripple an enemy population. The Madrid[29] and London[30] attacks targeted transportation systems and occurred along busy transit pathways. However, the attacks did not target the key hubs of the system or cause cascading outages throughout the transportation system. The same attacks carried out in more carefully selected locations could have caused wider impacts to the transportation system and inflicted a greater number of casualities. The Brussels airport bombing targeted the most accessible area of the facility rather than an essential part of the system required to direct, land, load, or fuel aircraft. If these attacks were strategically targeted strikes intended to cripple transportation system, they would have occurred in a different manner.

These major terrorist attacks also did not follow the concepts of series warfare in which an attack is mounted, resources are regrouped, and a subsequent attack occurs. Following the plane crashes at the WTC and the Pentagon, no plan or operation was in place for a second wave of attacks. If the 9/11 attacks were part of a series warfare strategy, a second operation would have already been underway but was not.[31] The same was true of the European transit bombings and the Paris bombings where coordinated attacks occurred, but no second or third wave of subsequent attacks were prepared to occur in quick succession.

While the 9/11 attacks and the European transit bombings targeted multiple locations, these attacks were not examples of a parallel attack strategy either. A parallel attack simultaneously strikes the key facilities in an area causing a crippling effect across the entire system. These significant terrorist attacks did not cripple the individual systems that they targeted (e.g., striking the Pentagon did not shut down the U.S. military) or cause cascading impacts that crippled other essential systems. Each attack caused isolated impacts to a single component of the infrastructure system.

The timing and location of the 9/11 and Madrid transit attacks also demonstrate that the attacks were not intended to cause the maximum number of casualities possible. While 50,000 people worked in the original WTC towers, the attack occurred before 9:00 a.m. when most people get to work.[32] Instead of potentially killing 50,000 people, 2,977 people died when the plane struck at 8:46 a.m.[33] Al Qaeda operatives spent years planning the 9/11 attack so it seems unlikely that they would have chosen to strike before 9:00 a.m. if the intent was to carry out a mass causality attack that would kill as many people as possible.

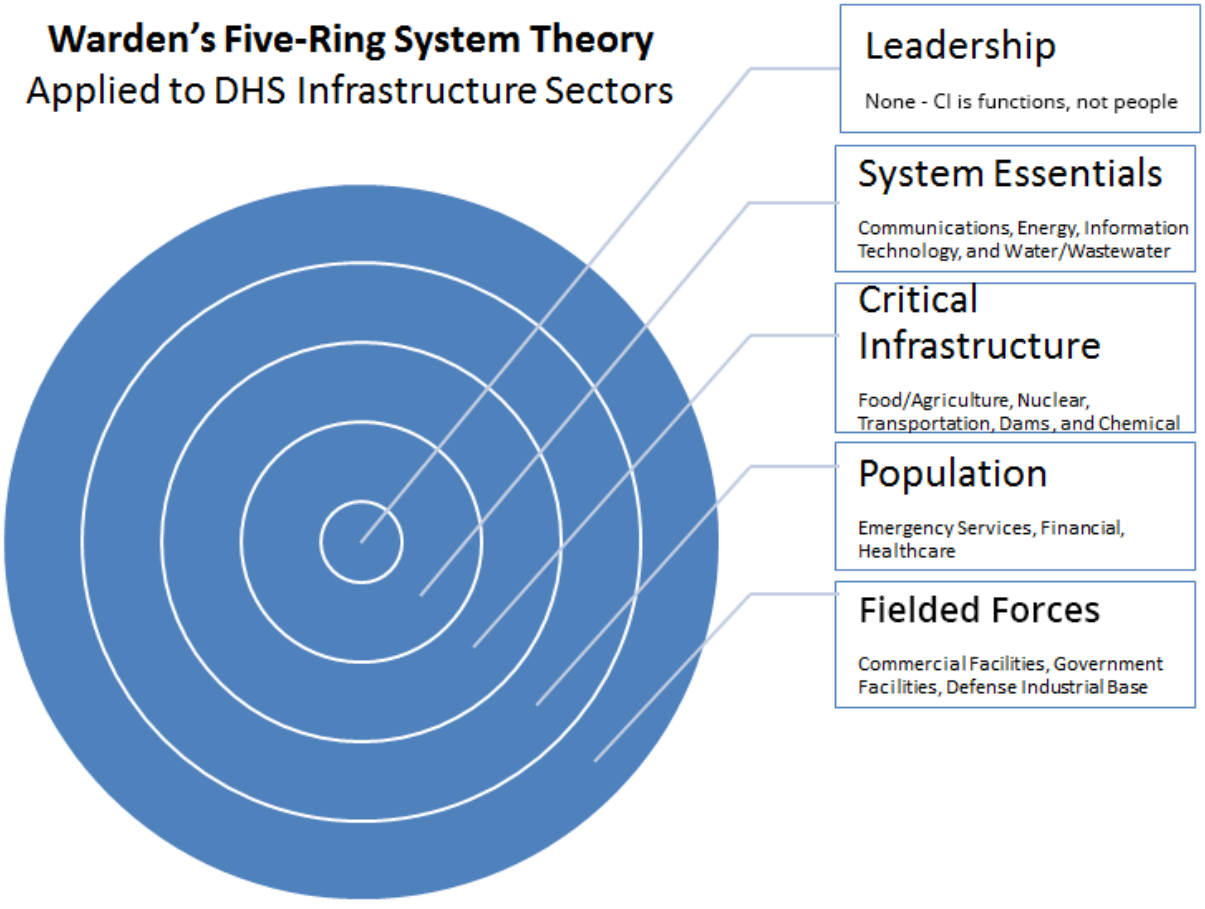

Figure 4: Warden's Five-Ring System Theory Applied to DHS Critical Infrastructure Sectors

Based on Warden's concentric rings theory, each of the terrorist attacks targeted the outermost rings that consist of the population and the fielded forces. If the terrorist attacks were strategic in nature, they would have likely tried to target the inner rings to cause more disruption across the entire country. Attacks targeting the inner rings could have been the New York Stock Exchange or the White House.[34]

Historically Terrorists do not Target Critical Infrastructure

Improvised explosives, vehicle borne explosives, and firearms were the primary weapons used in more than 99% of terrorist attacks according to the *Mineta Transportation Institute National Transportation Security Center of Excellence* study of multiple terrorism attack databases.[35] While these types of attacks have the power to kill people and cause damage to property, they do not have the destructive capability to cease the functions of most critical infrastructure facilities, such as power plants, telecommunications hubs, dams, water treatment facilities, regional transportation systems, and so on. Why is protection of facilities providing essential infrastructure functions a primary goal of DHS when these facilities are rarely targeted, and do not align with the motivation for terrorist groups?

Protecting critical infrastructure against terrorist attacks is a primary mission of DHS, but the execution of this mission is flawed in many ways. Current policies and procedures look at targets in a different way than how a terrorist would select a target for attack. The protection of potential targets is designed around methods of attack that are different from how the majority of terrorist attacks are carried out. The consequences of an attack on a target are assessed based on the number of deaths, injuries, and dollars rather than the public exposure or alignment with an ideology that the target represents. Following similar ideas as the book, *From the Terrorist's Point of View*, rather than refine the approach to identify threats, current practice is to cast a larger and larger net, which requires greater resources for smaller results.[36]

Fear—The Critical Strategy of Terrorism

Terrorism experts including Bruce Hoffman argue that large-scale terrorist attacks with weapons of mass destruction (which have never occurred) and large events like the 9/11 attacks on the WTC are counter-productive strategies for terrorist groups. Small-scale attacks cause "disproportionately enormous consequences, generate fear and alarm, and thus serve the terrorists' purposes just as well as a larger weapon or more ambitious attack."[37] According to Breckenridge and Zimbardo, "a heightened sense of crisis can lead to political disaffection and diminished confidence in the government,"[38] and the resulting fear and anxiety across the population from the attack aligns better with terrorists' goals of political or social changes than inflicting mass destruction or causalities. For example, Osama Bin Laden's attacks on the United States prior to September 11, 2001 were also attempting to erode public support and cause political pressure to remove U.S. forces from the Middle East. These attacks were intended to erode the general public's support of U.S. leaders, not to kill the entire American population. As Bruce Bonger argues,

> It is not surprising that fear and apprehension can have considerable political consequences. Affective influences on attention, memory, and judgment contribute to the widespread experience of disproportionate vulnerability and looming threat appraisal that make terrorism a more psychologically complex phenomenon.[39]

Osama Bin Laden's Strategy

While the conventional army wants to conquer territory at the lowest cost, Osama Bin Laden's strategy was the opposite. Instead of wanting to invade America and take over resources, his plan was to draw the United States into a prolonged and unwinnable military conflict in the Middle East that would eventually bankrupt this country. In 2004, Bin Laden delivered the message that:

> all that we have to do is to send two Mujahedin to the farthest point East to raise a piece of cloth on which is written al-Qa'ida in order to make the generals race there to cause America to suffer human economic and political losses without their achieving for it anything of note other than some benefits to their private companies. This is in addition to our having experience in using guerrilla warfare and the war of attrition to fight tyrannical superpowers as we alongside the Mujahedin bled Russia for 10 years until it went bankrupt and was forced to withdraw in defeat. So we are continuing this policy in bleeding America to the point of bankruptcy.[40]

Bid Laden's motivation for waging this style of war stemmed from his view of his territory as being under occupation and the strategy was designed to make the continued deployment of U.S. troops unsustainable. In his videotaped messages, Bin Laden states, "we fight you because we are free men who don't sleep under oppression. We want to restore freedom to our Nation and just as you lay waste to our Nation, so shall we lay waste to yours."[41] Bin Laden's message showed no interest in invading the United States or eradicating the entire American public.

This freedom fighter warfare strategy is problematic for a conventional military because of the imbalance between the extreme expense of a maintaining a remotely-deployed modern military force with the minimal expense of conducting guerilla operations with a small number of operatives and homemade explosives.

Homeland Security Enterprise versus Homegrown Violent Extremists

The same imbalances in the costs of waging warfare exist between the thousands of law enforcement agencies within the homeland security enterprise and their battle against individual homegrown violent extremists who self-radicalize to conduct jihad against domestic targets.

In 2010, Al Qaeda transitioned to a "death by a thousand cuts" strategy, which focused on a high volume of low cost attacks. An example was the plot to use bombs in printer cartridges

to destroy planes. This plot had an estimated cost of $4,200[42] but would have done hundreds of millions of dollars in damage to the aviation industry by destroying two Boeing 747 aircraft valued at more than $200 million each,[43] and causing subsequent groundings of other flights.[44] Similar to the problems that have resulted from prolonged military operations in Iraq and Afghanistan, the cost of maintaining thousands of intelligence analysts and law enforcement officers dedicated to counter-terrorism is unsustainably expensive, while the cost of conducting small-scale terrorist operations is a minimal expense for Al Qaeda or ISIS.

Both Al Qaeda's *Inspire* magazine and the Islamic State's *Dabiq* offer similar guidance to future jihadists to conduct small attacks close to home. There are examples of this message in *Dabiq* No. 6 asserting that "the Muslims will continue to defy the kāfir war machine, flanking the crusaders on their own streets and bringing the war back to their own soil."[45] The Orlando Pulse nightclub shooting is a stark example of this low-cost warfare strategy because online videos and propaganda materials alone can provide enough motivation to draw vulnerable individuals to jihad and virtual affiliation with ISIS.[46]

Terrorist Target Selection—Maximum Exposure not Critical Functions

The use of fear as a tactic makes the target selection for a terrorist attack even more complicated to determine. As Bruce Bonger points out, "the potential for misplaced threat-related priorities may represent a particularly daunting challenge for the United States, which can anticipate a vast array of possible terrorist targets and methods, but relative to many areas of conflict, it has had little historical experience with terrorist attacks."[47]

Without a framework of past experience with terrorism, DHS likely used conventional military strategies to identify domestic infrastructure. One of these sources was likely Sun Tzu's war strategy, which centered on defeating the enemy with the least amount of effort possible. This same strategy has been utilized by the United States in the air bombing campaigns against Iraq. Using Warden's theory of concentric rings, the highest value targets (the leadership and most critical systems) are targeted to cripple the remainder of the country. Precise attacks to the strategic core leave the population mostly unharmed.

Terrorism is not about conquering the enemy or using strategic strikes. Since the objectives of a terrorist group are different from an army, critical facilities have lower value and are less likely to be targeted. The intent of the terrorist is to send a message and gain maximum exposure, but not necessarily cripple the functions of the target. Of the 125,087 incidents in the Global Terrorism Database, more than 74,000 had no injuries and 90% had fewer than 10 injuries from the attack. Nearly 63,000 incidents also had no fatalities and more than 90% of incidents also had fewer than 10 fatalities.[48] This small number of injuries and deaths occurred even though 59,982 of the incidents were bombings/explosions targeting primarily private citizens, businesses, military, and government. As shown in Figure 5, less than .5% of the attacks were against telecommunications systems, which would be a high value strategic target to cripple infrastructure.

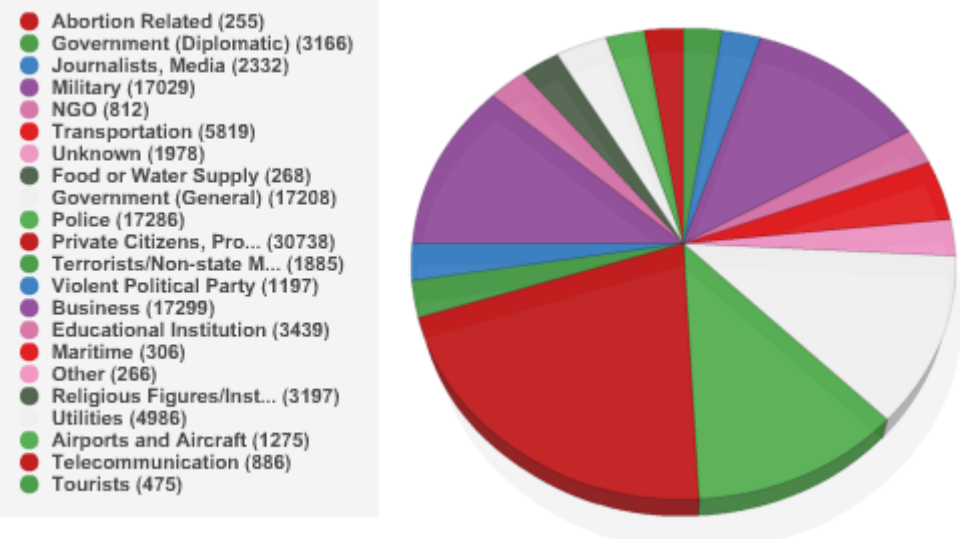

Figure 5: Terrorist Attack Targets by Type

From "Global Terrorism Database, Search Results: 141966 Incidents," accessed July 22, 2015, http://www.start.umd.edu/gtd/.

The 1995 Aum Shinrikyo attack on the Tokyo Subway using sarin is an example of a terrorist attack that occurred at a critical transportation facility, but the intent of the attack was not to disrupt operations or functions of the transportation system. The doomsday cult held a belief that the Japanese government was corrupt and responsible for a pending apocalypse, so they believed that a shocking attack would result in the people of Japan prescribing to the Aum Shinrikyo beliefs. This attack was deadly, but it did not cause any damage to an infrastructure system. It was an attack on a mass gathering of people inside a vulnerable area.[49]

Another terrorist group focused on the message of the attack rather than the death and destruction caused by it was the IRA. It was a standard practice of the IRA to call in and report bombings prior to the explosion because the intent of attack was not to harm civilians.[50] Based on the Global Terrorism Database, in 74,838 of 125,087 attacks (59.8%), no injuries occurred. Mass injuries harming more than 100 people occurred less than .08% of the time.[51] In the majority of cases, the goal of a terrorist attack has been to send a message rather than cause widespread harm.

In the video tape Osama Bin Laden released taking credit for the 9/11 attack, he said, "the Twin Towers were legitimate targets, they were supporting U.S. economic power. These events were great by all measurement. What was destroyed were not only the towers, but the towers of morale in that country."[52] Bin Laden's statement makes it clear that the attack was not intended to destroy the American economy or collapse the infrastructure of New York City; the purpose of the attack was to scare the American people and damage their morale. Like those conducted by the Irish Republic Army (IRA) and Aum Shinrikyo, the attack was a message, not a targeted strike on critical infrastructure systems.

When considering the facilities at risk for a terrorist attack, the DHS's infrastructure protection policies do not align to the most frequent targets for terrorist groups around the world. Shown in Figure 5, the most common targets are private citizens, police, military, and

government (general and diplomatic), accounting for 70% of all attacks. Facilities providing purely infrastructure functions, such as telecommunications and utilities, were targeted in 4.4% of attacks.

Terrorist's Motivation—Attention and Reward

Conventional thinking about terrorist tactics and targets would suggest that they want to inflict the most damage possible. For this reason, standard practices for protecting critical infrastructure include building fences, installing traffic bollards, monitoring security cameras, and screening visitors at locations such as government buildings, commercial offices, stadium, hotels, casinos, sports arenas, and museums. These measures are designed to prevent the terrorist from reaching the facility by building a fortress around it. Unfortunately, the motivation for terrorist attacks is also distinctly different from a targeted military strike designed to cripple the infrastructure systems of the enemy. The attack is not about destroying the function of the physical system; it is about sending a message to society. That message can be sent by detonating an explosive beyond the security perimeter at points where civilians must congregate to enter the facility as was the case with Brussels airport bombing.

The functions of a "terrorist attack can include:

- Showing that the authorities are weak and vulnerable to attacks
- Proving that the authorities are unable to control events
- Lowering allegiances to the authority institutions
- Creating a sense of instability and lawlessness in society
- Creating a sense of helplessness among the population
- Giving the impression of terrorist organizations as being very powerful
- Giving the impression that there will be no end to terrorist attacks until a final victory"[53]

These functions of a terrorist attack are not exclusive to Islamic extremists. The same fundamental goals motivated groups like the IRA, Aum Shinrikyo in the Tokyo Subway sarin attack, and domestic lone-wolf attacks like the Oklahoma City bombing. In each case, employing a strategy of protecting physical facilities does not deter attacks or prevent terrorists from accomplishing their functions.

Difference Between Critical and Targetable Infrastructure

A potential point of confusion in the infrastructure protection mission is the difference between facilities that are part of an infrastructure system and locations that are attractive targets for terrorism. While a water treatment plant might be a critical infrastructure facility, its remote location, inaccessibility to the general public, and lack of people at the site would

make it an unattractive target for a terrorist. Inversely, an outdoor concert might not serve any infrastructure function, but due to the large crowds and open access to the area, it could be an attractive location for terrorist attack.

By looking at the types of facilities attacked in the Global Terrorism Database, a difference can be seen between a "targetable" facility and a "critical infrastructure" facility. Looking more specifically at domestic terrorist attacks that have caused 1–10 fatalities or injuries (Figure 6), the Global Terrorism Database includes 149 incidents from 1973 to 2014.[54] The two attacks targeting utilities include the 2012 attempted bombing of a gas pipeline by a sovereign citizen in Plano City, Texas,[55] and the utility targeted by the New World Liberation Front in 1976.[56] The majority of attacks target government, police, private citizens, educational institutions, and businesses. Infrastructure systems including airports, transportation, and utilities are seldom the target. During the recent attack in Brussels, even though the main terminal of the Zaventem International Airport was targeted by terrorists during the April 2016 bombing, the location was chosen because it was publicly accessible, not because it was a critical node in the overall operations of the airport. The Brussels attack targeted a vulnerable location where civilians congregated outside of the security perimeter.[57] If the attack was against the airport as a component of the transportation infrastructure, the terrorists would have targeted the fuel storage system, power substation, air traffic control tower, radar system, baggage-screening area, or another key node upon which the entire airport was dependent. The seven airport and aircraft attacks cited within the START data represent similar circumstances to the recent Brussels attack. When airports had minimal security, they were vulnerable to attacks in which terrorists could hijack a plane and take the defenseless passengers hostage. Today the vulnerable point beyond airport security is now an attractive target.[58]

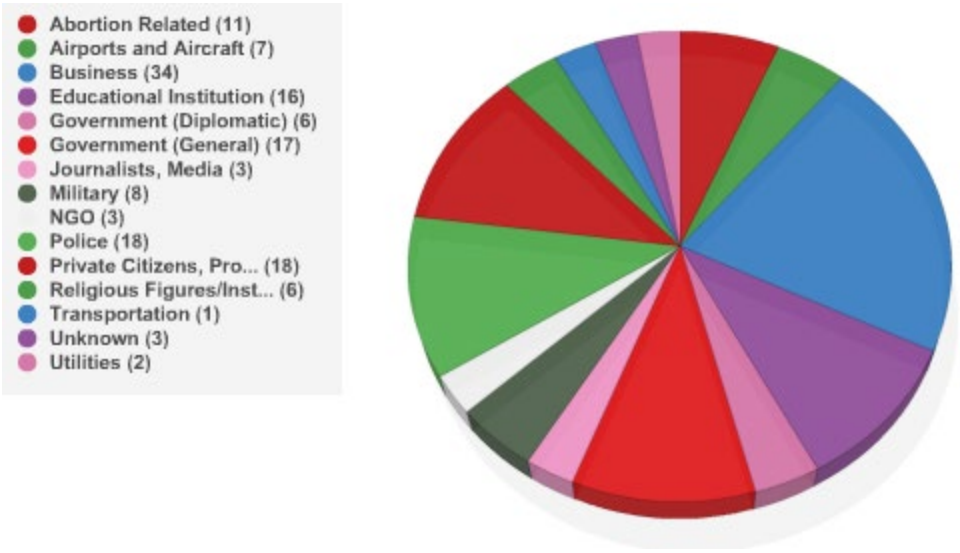

Figure 6: Domestic Attacks Causing 1–10 Fatalities/Injuries

From "Global Terrorism Database, Search Results: 141966 Incidents," accessed July 22, 2015, http://www.start.umd.edu/gtd/.

Since 1970, eight terrorist attacks have occurred in the United States that have killed or injured more than 101 people, as shown in Table 1. These incidents include: the 2016 Orlando, FL Nightclub Shooting; the 2013 Boston, MA Marathon Bombing; the 9/11 attack at the Pentagon in Arlington, VA; the 9/11 attack at the WTC in New York, NY; the 9/11 plane crash in Shanksville, PA; the 1996 Olympic bombing in Atlanta, GA; the Oklahoma City federal building bombing in 1995; and the 1984 biological (salmonella) attack in The Dalles, Oregon.[59] The target of each attack was selected to send a specific message from the group responsible. In each case, the attack did not cause a significant disruption to infrastructure or the functions of the facility attacked, the surrounding facilities, or government (local, state, or federal).

Table 1: Terrorist Attacks Causing more than 101 Deaths or Injuries in the United States [60] [61] [62]

Attack	Purpose/Intent	Consequence	Disruption to CI	Success?
Orlando Pulse Nightclub Shooting	Establishment of Islamic Caliphate; acceptance in radical Islamist communities[60]	49 fatalities, 53 injuries, minor damage to commercial building	None	No—other than killing/injuring people at the site of the attack, the goals were not accomplished
Boston Marathon Bombing	Establishment of Islamic Caliphate; acceptance in radical Islamist communities; wage war against the United States[61]	Two fatalities, 132 injuries, marathon stopped, minor damage to surrounding buildings	Localized closures at site of explosion (7–10 days), city-wide closures due to law enforcement operations while searching for suspects, no disruption to infrastructure systems	Partial—Attack did not harm US military or overseas military operations; Tsarnaev brothers gained acceptance in radical communities
9/11 Attack—Pentagon	Remove U.S. military forces from countries in the Middle East by striking domestic US target with a high profile attack	189 fatalities, 106 injuries, significant damage to a portion of the Pentagon	U.S. Military command functions and US government functions had minimal disruptions to critical operations	No—other than killing/injuring people at the site of the attack, the goals were not accomplished
9/11 Attack—World Trade Center	Remove U.S. military forces from countries in the Middle East by striking domestic U.S. target with a high profile attack; cause widespread fear in public and erode support for government	2,996 fatalities, +6,000 injuries, total destruction of multiple buildings	Localized disruptions to infrastructure functions at the site of the attack and immediate surrounding areas; regional infrastructure functions experienced minimal disruption	No—other than killing/injuring people at the site of the attack, the goals were not accomplished

Attack	Purpose/Intent	Consequence	Disruption to CI	Success?
9/11 Attack—Shanksville, PA	Remove U.S. military forces from countries in the Middle East by striking domestic US target with a high profile attack; final target unknown	40 fatalities (crew and passengers of AA Flight 77)	None	No—plane crashed prior to reaching intended target
Atlanta Olympic Games Bombing	Force cancellation of Olympic Games to protest the U.S. government's allowing abortions	1 fatality, 110 injuries	Olympic Games continued with minimal disruptions; no disruptions to infrastructure functions	No—other than killing/injuring people at the site of the attack, the goals were not accomplished
Oklahoma City Bombing (Murrah Federal Building)	Retaliation against the federal government for gun control and Waco, TX Branch Davidian standoff (attack occurred on 2-year anniversary)[62]	168 fatalities, 650 injuries, significant damage to targeted building	Localized disruptions at site of attack; local, state, and federal government continued to function; minimal impacts to infrastructure functions	No—attack did not change government policies
The Dalles, Oregon Salmonella Attack	Sicken the local population prior to election to allow Rajneeshee Group candidate to win election	0 fatalities, 751 injured, no damage to buildings	No disruption to infrastructure or government functions	No

As these eight attacks demonstrate, targeting and injuring a large number of people does not align with attacking a facility that provides essential infrastructure functions to the nation or region. In each case, the disruptions to essential infrastructure services were nonexistent or minimal in even the immediate areas adjacent to where the attacks occurred.

Why does critical infrastructure protection policy focus on large-scale attacks to infrastructure facilities when they have not been the target of the largest domestic terrorist attacks, and were rarely the target of the 130,000 terrorist attacks across the world over the last 50 years?

Terrorists are interested in attacking locations that are accessible, crowded with people, have minimal security, and will draw the interest of the general public and the media. The eight major terrorist attacks on the United States fit these criteria. For example, the Olympic Park in Atlanta, Georgia was accessible to the general public and had no security screenings. On the local scale, the 10 restaurant salad bars targeted in the 1984 salmonella attacks were easily accessible to the terrorist group, frequented by the public, and the consequences were intended to be widespread across the community.[63] The attack at the Boston Marathon targeted an event that was open to the general public, did not have security screenings, drew large crowds, and would draw international media attention. The Boston Marathon attack did not directly target transportation or specific infrastructure functions in Boston with the intent of crippling the city's essential functions.

The November 13, 2015 coordinated terrorist attacks in Paris, France further highlight the selection of accessible targets over those that provide critical functions. The simultaneous terrorist attacks in Paris targeted Le Bataclan (concert venue), Le Petit Cambodge (restaurant), Le Carillon (restaurant), Stade de France (stadium), Les Halles (shopping center), The Louvre (museum), and La Belle Equipe (restaurant).[64] Each of these targets were areas likely to contain a large number of people on a Friday night, but none of these locations included a critical infrastructure system that would have a cascading impact on the essential-to-life functions of the city. Seven groups of terrorists armed with automatic weapons and explosives could have likely damaged bridges, power distribution equipment, water treatment facilities, transportation hubs, or other infrastructure systems but their intent was not to attack infrastructure systems.

A terrorist's interest lies not in the functions that a facility provides, such as a high demand electrical substation responsible for regional power distribution, but instead focuses on publicly accessible areas that are high-visibility locations for attacks. Targetability is the primary motivation of the terrorist over the criticality of the facility to the interconnected infrastructure system.

Conclusion

Modern military theories provide a potential explanation for the focus of DHS's efforts because the threats from terrorism have likely been evaluated by senior officials who draw on their education and experiences with the principles of strategic warfare. Nationally significant infrastructure facilities that can cripple the essential functions of the entire country if destroyed would be attractive targets for an enemy nation-state to strike with ballistic missile and airpower capabilities during a war. The current terrorist threat comes from homegrown violent extremists and members of terrorist groups who are motivated to inflict mass casualties in the locations that are most visible and easily accessible.[65] An individual terrorist or a small group of terrorists most likely lack the intelligence, organizational coordination, manpower, and resources to conduct a strategic warfare campaign against nationally significant infrastructure targets with the intent of crippling essential-to-life systems across the country. The strategic warfare approach of developing a static list of vulnerable assets does not match the unpredictable and dynamic threat from terrorism. The current IP policies identify the likely targets of a nation-state military and assume them to be the same targets that terrorists would have the intention and capability of attacking.

The 2013 *National Infrastructure Protection Plan* operates under the assumption that "both domestic and international critical infrastructure assets represent potential prime targets for adversaries. Given the deeply rooted nature of these goals and motivations, critical infrastructure likely will remain highly attractive targets for state and non-state actors and others with ill intent."[66] Based on this research, infrastructure protection efforts are framed under an inaccurate assumption of the terrorist threat to them. Protection policies should not focus on large-scale attacks to facilities when they have not been the target of the largest domestic terrorist attacks and have rarely been the target of the 130,000 terrorist attacks across the world over the last 50 years. A possible solution in the mission of protecting critical infrastructure can be refined through a psychological approach to evaluate why a terrorist attacks, the likely method of attack, and the type of target that would align with the desired results. Unlike conventional warfare, terrorists view their tactics as a driver for social

change, making their highest value targets different from those chosen by a conventional army commander.

The flaw in using a strategy that aims to prevent all types of attacks is compounded by the extreme difficulty of identifying individuals who are terrorists.[67] The focus on protecting critical infrastructure has been identifying all possible targets then building better barriers, installing more security and surveillance systems, and gathering large amounts of real time intelligence. Unfortunately, it is impossible to determine who will become a terrorist before they strike, and it is impractical to fortify every potential target to withstand every possible type of attack. Protection policies should focus instead on determining the most likely targets and the most realistic forms of attack based on goals and capabilities of the terrorist groups. In most cases, the most likely targets are not the most critical facilities to the infrastructure system.

Terrorists have not previously targeted infrastructure and are unlikely to change their intentions in the future. The most recent terrorist attack on U.S. soil, which also was the most deadly shooting in the country's history, targeted a nightclub that served no infrastructure function and had no interconnectivity to any type of infrastructure systems or facilities. Based on the historical and current targets of terrorists, the way DHS views protecting infrastructure and preventing terrorism needs to be reformed to remove the focus on the facilities that hold strategic value in a war between nation-states.

About the Author

David Riedman is a Captain in the Montgomery County, MD Fire and Rescue Service and an expert in emergency and disaster preparedness, planning, and response. Mr. Riedman is a graduate of the Center for Homeland Defense and Security master's degree program at the Naval Postgraduate School and received his undergraduate degree from Georgetown University. He is currently an associate at the Cadmus Group and supports federal clients with strategic planning, policy development, and organizational improvement. He may be reached at dariedman@gmail.com .

Notes

1 David A. Riedman, "How Critical is Critical Infrastructure?" Homeland Security Digital Library, September 2015, http://hdl.handle.net/10945/47320.

2 Anthony B. Carr, "America's Conditional Advantage: Airpower, Countering Urgency, and the Theory of John Warden," Homeland Security Digital Library, June 1, 2009, https://www.hsdl.org/?view&did=697900.

3 "Countering Violent Extremism," July 20, 2015, http://www.dhs.gov/topic/countering-violent-extremism.

4 John A. Warden, "The Enemy As a System," *AirPower Journal*, Spring 1995, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm.

5 "What is Security and Resilience?" August 24, 2015, http://www.dhs.gov/what-security-and-resilience.

6 Henry Willis, *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection* (Santa Monica, CA: RAND Corporation, 2006), http://www.rand.org/content/dam/rand/pubs/technical_reports/2007/RAND_TR386.pdf.

7 "Countering Violent Extremism," July 20, 2015, http://www.dhs.gov/topic/countering-violent-extremism.

8 Howard D. Belote, "Warden and the Air Corps Tactical School–What Goes Around Comes Around," *AirPower Journal*, Fall 1999, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj99/fal99/belote.html.

9 Peter Faber, "Competing Theories of Airpower: A Language for Analysis," *AirPower Journal*, April 30, 1996, http://www.airpower.maxwell.af.mil/%20airchronicles/presentation/faber.html.

10 Ibid.

11 John A. Warden, "The Enemy As a System," *AirPower Journal*, Spring 1995, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm.

12 Ibid.

13 Ibid.

14 Ibid.

15 Ibid.

16 "What is Critical Infrastructure?" August 26, 2015, http://www.dhs.gov/what-critical-infrastructure.

17 Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach, Washington, DC: Department of Homeland Security, 2013, http://www.dhs.gov/sites/default/files/publications/NIPP%202013%20Supplement_Executing%20a%20CI%20Risk%20Mgmt%20Approach_508.pdf.

18 Ibid.

19 John A. Warden, "The Enemy As a System," *AirPower Journal*, Spring 1995, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm.

20 Ibid

21 Ibid.

22 Ibid.

23 Ibid.

24 Defined as "the facilities or processes without which the state or organization cannot maintain itself. It is not necessarily directly related to combat." Warden, "The Enemy As a System."

25 Adapted from Clayton Chun, "John Warden's Five Ring Model and the Indirect Approach to War," ETH Zurich, June 1, 2008, http://www.isn.ethz.ch/Digital-Library/Publications/.

26 Clayton Chun, "John Warden's Five Ring Model and the Indirect Approach to War," ETH Zurich, June 1, 2008, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=57408.

27 Ibid., 301.

28 Ibid., 306.

29 "Madrid Train Attacks: How the Attacks Happened," *BBC News,* http://news.bbc.co.uk/2/shared/spl/hi/guides/457000/457031/html/default.stm.

30 "London Bombings Toll Rises to 37," *BBC News*, July 7, 2005, http://news.bbc.co.uk/2/hi/uk/4661059.stm.

31 David Stout, "Original Plan for 9/11 Attacks Involved 10 Planes, Panel Says," *The New York Times*, June 16, 2004, http://www.nytimes.com/2004/06/16/politics/16CND-REPORT.html.

32 "The World Trade Center—Facts and Figures," accessed July 22, 2015, https://www.nysm.nysed.gov/wtc/about/facts.html.

33 "September 11th Fast Facts," March 27, 2015, *CNN*, http://www.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/.

34 It should be noted that the White House was a possible target of United Flight 93 on September 11, 2001, but the President was away from Washington, DC on a public trip to Sarasota, FL. The building was also evacuated prior to the possible arrival of the aircraft meaning that leadership would not have been incapacitated by the attack even if it occurred at the White House while the President was there.

35 "Explosives and Incendiaries Used in Terrorist Attacks on Public Surface Transportation: A Preliminary Empirical Examination," March 1, 2010, http://transweb.sjsu.edu/MTIportal/research/publications/documents/2875-IED-Support-Research.pdf.

36 Fathali M. Moghaddam, *From the Terrorists' Point of View: What They Experience and Why They Come to Destroy,* (Westport, CT: Praeger Security International, 2006).

37 Bruce Hoffman, *Inside Terrorism*, (New York: Columbia University Press, 2006).

38 Bruce Bongar, *Psychology of Terrorism*, (Oxford: Oxford University Press, 2007).

39 Ibid., 118.

40 Osama Bin Laden, "Transcript: Translation of Bin Laden's Videotaped Message," *The Washington Post*, November 1, 2004, http://www.washingtonpost.com/wp-dyn/articles/A16990-2004Nov1.html.

41 Bin Laden, "Transcript: Translation of Bin Laden's Videotaped Message."

42 Matthew Cole, "Al Qaeda Promises U.S. Death by a 'Thousand Cuts,'" *ABC News*, November 21, 2010, http://abcnews.go.com/Blotter/al-qaeda-promises-us-death-thousand-cuts/story?id=12204726.

43 "Boeing 747-400 Freighter Commercial Cargo Jet," http://planes.axlegeeks.com/l/279/Boeing-747-400-Freighter.

44 Saad Abedine, "Yemen-based Al Qaeda Group Claims Responsibility for Parcel Bomb Plot," *CNN*, November 5, 2010, http://www.cnn.com/2010/WORLD/meast/11/05/yemen.security.concern/.

45 "ISIS Releases Issue 6 of Dabiq Magazine," December 30, 2014, http://www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq#.

46 Bearak, Max. "When ISIS Claims Terrorist Attacks, It's Worth Reading Closely," The Washington Post, July 26, 2016, https://www.washingtonpost.com/news/worldviews/wp/2016/07/26/when-isis-claims-terrorist-attacks-its-worth-reading-closely/.

47 Bongar, *Psychology of Terrorism*.

48 "Global Terrorism Database, Search Results: 141966 Incidents," accessed July 22, 2015, http://www.start.umd.edu/gtd/.

49 Nicholas Kristof, "A Guru's Journey—A Special Report; The Seer among the Blind: Japanese Sect Leader's Rise," *The New York Times*, March 25, 1995, http://www.nytimes.com/1995/03/26/world/guru-s-journey-special-report-seer-among-blind-japanese-sect-leader-s-rise.html.

50 David Sharrock, "IRA Is Not So Ruthless and Always Gives Bomb Warnings," *The Telegraph*, September 19, 2001, http://www.telegraph.co.uk/news/uknews/1340995/IRA-is-not-so-ruthless-and-always-gives-bomb-warnings.html.

51 "Global Terrorism Database, Search Results: 141966 Incidents," accessed July 22, 2015, http://www.start.umd.edu/gtd/.

52 David Bamber, "Bin Laden: Yes, I Did It," *The Telegraph*, November 11, 2001, http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/1362113/Bin-Laden-Yes-I-did-it.html.

53 Fathali M. Moghaddam, *From the Terrorists' Point of View: What They Experience and Why They Come to Destroy,* (Westport, CT: Praeger Security International, 2006), 85.

54 "Global Terrorism Database, Search Results: 141966 Incidents," accessed July 22, 2015, http://www.start.umd.edu/gtd/.

55 Ibid.

56 Ibid.

57 BBC News, "Brussels Explosions: What We Know About Airport and Metro Attacks," April 9, 2016, http://www.bbc.com/news/world-europe-35869985.

58 Nicola Clark, "Why Airline Hijackings Became Relatively Rare," *The New York Times*, March, 29, 2016, http://www.nytimes.com/2016/03/30/world/middleeast/airline-hijacking-history.html?_r=0.

59 Ibid.

60 Federal Bureau of Investigation, "Update Regarding Pulse Nightclub Shooting," June 20, 2016, https://www.fbi.gov/contact-us/field-offices/tampa/news/press-releases/investigative-update-regarding-pulse-nightclub-shooting.

61 National Public Radio, "The Brothers' Examines Motivation Behind Boston Marathon Bombing," April 3, 2015, http://www.npr.org/2015/04/03/397213144/-the-brothers-examines-motivation-behind-boston-marathon-bombing.

62 History.com, "Oklahoma City Bombing," A&E Television Networks, accessed July 22, 2015, http://www.history.com/topics/oklahoma-city-bombing.

63 Public Broadcasting Service, "History of Biowarfare," 2002, http://www.pbs.org/wgbh/nova/bioterror/hist_nf.html#cult.

64 Matt Ferner, "Locations of the Paris Attacks," *The Huffington Post*, November 13, 2015, Accessed November 30, 2015, http://www.huffingtonpost.com/entry/locations-paris-attacks_5646789ee4b08cda3488e867.

65 "Countering Violent Extremism," July 20, 2015, http://www.dhs.gov/topic/countering-violent-extremism.

66 Ibid.

67 Jeh Johnson, "Remarks By Secretary Jeh Charles Johnson On "The New Realities of Homeland Security," As Part of the Landon Lecture Series on Public Issues—As Prepared For Delivery.