Fortress America – An Outdated Concept

Carl A. Singer

MSHS 6604 – Professor Gazman Xhudo

Abstract

This paper develops a hybrid approach for assessing and coping with infrastructure vulnerability. The author believes that the current concepts characterized as "Fortress America" and "passive response" are no longer valid and are not an appropriate basis for strategic and tactical planning as regards to infrastructure. This paper briefly explores the historical roots and reasoning behind both the "Fortress America" concept and "passive response", and then reviews current U.S. Army doctrine regarding assessing infrastructure vulnerability. A more aggressive approach that is suitable for today's strategic environment is then developed.

Introduction

Given that infrastructure is a key terrorist target, assessing and coping with the vulnerability of our infrastructure is a vital component in dealing with terrorism. The author continues to propose the following strategic objective:

> **To assure the security of the United States and its citizens at whatever cost to the United States and to others.** [1]

This objective is an *existential imperative* if the nation is to survive. This objective so stated loosens the reins for policy makers, and broadens their choice of military alternatives. Areas relevant to infrastructure security including site hardening, rapid recovery and infrastructure redundancy are important but outside the scope of this paper.

History – Fortress America / Passive Response

The concept of Fortress America (also referred to as "Fortress North America") has its roots in World War II and was a major strategic concept during the cold war. An example of this thinking is a statement by U.S. Secretary of Defense, Robert McNamara, in discussing the "Chinese threat." (Art & Waltz 1971: 503)

> ….The cornerstone of our strategic policy continues to be to deter deliberate nuclear attack upon the United States, or its allies, by maintaining a highly reliable ability to inflict an unacceptable degree of damage upon a single aggressor, or combination of aggressors, at any time during the course of a strategic nuclear exchange -- even after our absorbing a surprise first strike.[2]

[1] This objective was formulated in the author's term paper for HIST 7868 and is based on work by Yechezkel Dror.
[2] Excerpts of speech to editors of United Press International, San Francisco, California, September 18, 1967.

Why Fortress America is an Outdated and Flawed Approach

The key flaw with this approach in today's terrorist centric security environment is that "an unacceptable degree of damage" is meaningless to many of our terrorist enemies. Concepts such as MAD (Mutually Assured Destruction) have no relevance to an apocalyptic terrorist. This type of enemy may relish martyrdom, the likely result of our focus on retaliation and / or escalation. In both his book and in related papers, Ralph Peters discusses the mentalities of the two basic terrorist categories: the practical and the apocalyptic. The practical terrorists "[are] 'traditional,' politically-oriented terrorists with specific goals" whereas "the far more dangerous religious terrorists [are] irreconcilably hostile to the United States and the West." (Peters 2002: 58-59) Today we are dealing not with nation-states but with apocalyptic terrorists, both "lone wolves" (or independent small bands) and complex terrorist organizations (or networks) such as Al Qaeda. Our old national strategy, "fortress America" no longer fits our new national enemies!

Why a "Passive Response" Model Alone is not Optimal.

A second flaw specific to infrastructure vulnerability is our historic mindset which the author calls a "passive response" or weather-oriented model. FEMA (the Federal Emergency Management Agency) and similar agencies have their roots in dealing with natural disasters. This heritage subscribes to the adage that "Everybody talks about the weather but nobody does anything about it.[3]" Consider for example a pending hurricane. Weather forecasters will track the path of the hurricane and predict its severity and the time and place of its landfall. FEMA correctly poses two alternatives to those who may be impacted by severe weather: "Batten Down the Hatches" or evacuate to safety. This passive model reflects the impossibility of doing anything to deter the hurricane, only to live through it and recover afterwards. The FEMA

[3] This adage is variously attributed to Mark Twain or to his friend Charles Dudley Warner.

planning focus was thus build better post-incident responses.[4] Unlike the weather, terrorism is not inevitable – we must do more than just talk about it. We must in a sense halt the hurricanes, terminate the tornadoes.

By extension, the weather oriented approach yields a passive model in dealing with attacks upon our infrastructure. This passive model spawns two sets of responses: (1) Efforts to make us less vulnerable to the impact of attacks via such technical means as target hardening, redundancy, self-healing networks, etc. (2) Efforts to guard against attacks via both traditional security measures and by employing better intelligence to detect would-be plotters and plans.

A Better Approach.

Consider adding a more aggressive attack component to the above in order to build a hybrid active / passive model. This model recognizes that vulnerability is two-sided, both the target, our infrastructure, and the attacking agent, the terrorist, have vulnerabilities. At the risk of a cliché, "The best defense is a good offense." More on point an anti-terrorist offensive is a vital component for dealing with (or reducing) infrastructure vulnerability. We can and must deter human agents (aka terrorists) who may threaten our infrastructure.

A sports analogy may be helpful here. Consider a goalie in either hockey or football (soccer.) By the rules of our game even a single goal scored against our team is intolerable – only a shutout is acceptable. A 10-1 "victory" is therefore unacceptable as the "1" is one too many. If we have no offense and rely only on our defense and our goalie, choosing to let the opposing team shoot as often as it wishes with no meaningful deterrent or consequences then sooner or later a goal will be scored despite our best efforts.

[4] FEMA representatives were participants in the U.S. Army War College's annual Strategic Crisis Exercise – the author commanded a military team in support of this training exercise. He highly respects FEMA's experience and professionalism.

In real world terms we cannot rely only on target hardening and increased security to protect our critical infrastructure. We must go beyond the passive model.

The U.S. Army's Analysis of Infrastructure Vulnerability

The Army Training and Doctrine Command, TRADOC understandably focuses on infrastructure as it impacts the Army and its ability to fight. Nonetheless, their approach is somewhat analogous to those of non-military government agencies. TRADOC Handbook No. 1.02, *Critical Infrastructure Threats and Terrorism* (TRADOC 2006: II-1) identifies nine "Critical Infrastructures at the National Level." These are: Agriculture & Food, Water, Public Health, Emergency Services, Government, Defense Industrial Base, Information and Telecommunications, Energy, Transportation, Banking and Finance, Chemical Industry and Hazardous Materials, Postal and Shipping. This list is similar to those from non-military government sources.

A Defense Critical Infrastructure Program (DCIP) is described and a Risk Management program is discussed in the TRADOC documentation. The Risk Management program has two phases: Risk Assessment and Risk Response. Risk Assessment incorporates an evaluation of the criticality of an asset, its vulnerability to attack, and the threats and hazards present. Risk Response similarly has three elements: Remediation, Mitigation, Reconstitution. Risk management is characterized as an on-going process.

TRADOC addresses the "Direct and Indirect Effects of Infrastructure Attacks". TRADOC also identifies a five-step process for identifying weaknesses in Critical Infrastructure. Additionally, TRADOC categorizes Critical Infrastructure assets as Physical, Human and Cyber (hardware, software, data and networks.)

Key physical assets are in the domains of agriculture, banking, energy and the economy. Physical assets include both tangible and intangible (information) property. Human assets include employees who need to be protected and personnel who may constitute a threat to systems. A discussion of Cyber-Terrorism is included as well. A key cyber asset is the defense department's own Global Information Grid (GIG) which even a decade ago consisted of over three million individual computers on 12,000 local Area Networks (TRADOC 2006: 2-3.)

TRADOC identifies Mission Essential Vulnerable Areas (MEVAs). The process for identifying these MEVAs begins by identifying all supported and service missions. Each mission is evaluated to determine if it is an essential requirement – in essence can our society go on without it. This is described as a five step process: (TRADOC 2006: III-4,III-5)

1. **Identifying critical assets** – an on-going review of assets and mission.

2. **Identifying and assessing vulnerabilities** – Identify potential areas of weakness and protective measures to mitigate vulnerabilities. Identify Interdependencies within and among infrastructures.

3. **Normalizing, analyzing, and prioritizing study results** – In a resource constrained environment prioritization is key.

4. **Implementing protective programs** – Target hardening, increased security, redundancy are among the measures that can protect or minimize.

5. **Measuring performance** – As with any useful program metrics need to be established.

The overarching goal is to assure that the organization's mission can be accomplished despite attack.

Learning from the TRADOC approach, "civilian" equivalents to Mission Essential Vulnerable Areas (MEVAs) can be developed. Consider for example, establishing Society Essential Vulnerable Areas and then adapting TRADOC's five step process accordingly. This

approach goes a step beyond the current "flat" listings of critical infrastructure by assigning priorities which can then lead to prioritizing avoidance and response measures.

Vulnerability is a Two-edged Sword.

Disappointingly, although the Department of Defense implementation guidance as described in the TRADOC document does include direction to "Identify …. protective measures to mitigate vulnerabilities" it maintains a strictly defensive posture and does not integrate an assessment of the threat actor's own vulnerabilities into its analysis. Perhaps these are out of scope for this document / organization.

Vulnerability should take into account threat assessment. In turn, threat assessment must consider the current and future strength and capabilities of the threat actor. Negatively impacting the threat actor's capabilities and freedom of action thus impacts our threat assessment and in turn our analysis of vulnerability. The author believes that an overlay of offense / and offensive countermeasures is essential both in analyzing the vulnerability of our infrastructure and in protecting our infrastructure from attack.

Vulnerability Assessment ← Threat Assessment ← Threat Actor Capabilities

This analysis is best done on two levels: micro (specific) and macro. At the micro level we address the specific vulnerabilities of a given infrastructure component, detailing the likely attack modes and then planning a (likely) preemptive tactical response. Further discussion at the tactical level is out of scope for this paper.

It is at the macro level that one needs to emphasize that just as our infrastructure is vulnerable, so, too, those who would attack our infrastructure have their own infrastructure vulnerabilities. Four complementary actions are recommended:

1. Discomfort and destroy the enemy in his refuge, staging and training areas.
2. Target enemy infrastructure – especially communications.
3. Ferret out the enemy among us.
4. Impede enemy funds flow.

1 - Discomfort and destroy the enemy in his refuge, staging and training areas.

The deployment of myriad troops in GWOT, the Global War on Terrorism, needs to be continuously examined regarding its aims and objectives, and of course its effectiveness. Our misadventure in Iraq is a case in point. To satisfy the post 9/11 political need to "do something" and strike back, we attacked the wrong target and at great cost brought down a regime thus upsetting the regional balance of power. Additionally, none of this significantly discomforted and destroyed the enemy.

The enemy must be more precisely identified, located and targeted. Recently the United States has pursued this to a limited extent by using drones to kill known terrorists. It must be noted that the use of drones to kill terrorist leadership has spawned controversy. There is ample justification for the killing of terrorists wherever they may reside. Even though the controversy may be for political gain it is worth noting that there is reasoned analysis justifying the use of drones. We are at war. In 1996 Osama bin Laden declared war on the United States via a fatwa. The United States declared war shortly after the 9/11 attack (September 14, 2001.) Those who join with al-Qaida should be considered enemy combatants and may be treated (attacked) as such. (Krauthammer 2013)

Vulnerability Assessment ← Threat Assessment ← Reduced Threat Actor Capabilities

2 - Target enemy infrastructure – especially communications.

TRADOC reviews "cyber support to terrorist organizations." A key component of terrorist infrastructure is the worldwide web. The web provides terrorists with intelligence and it's a communication vehicle well suited to their needs. That terrorists use the internet is verified by the following excerpt:

> Al-Qaeda "was using the Internet to do at least reconnaissance of American utilities and American facilities. If you put all the unclassified information together, sometimes it adds up to something that ought to be classified." Richard Clark, Former Chairman, President's Critical Infrastructure Protection Board, February 13, 2002 (TRADOC 2006: VI-1)

Terrorists also use the internet for planning, recruitment, research and propaganda. A dispersed organization consisting of many isolated cells depends on and can thrive only in a communication rich environment. As we assess the vulnerability of our infrastructure, one constant is the capability of relatively unsophisticated actors to obtain the knowledge needed make explosives, biological agents and chemical agents. This is coupled with the wherewithal to procure necessary supplies. If we can reduce these capabilities this will reflect as reduced vulnerability to our infrastructure.

Although cyber-terrorism is a ripe topic, a detailed discussion it is out of scope for this paper. Nonetheless, we must recognize that a cyber attack can inflict significant harm to our infrastructure. The author coined a term, the "MegaPole", to equate the damage that a line of faulty software could do to a long distance communications network with the destruction of telephone poles caused by a hurricane or tornado. (Singer 2003) We must use similar measures to assess the criticality of infrastructure assets, their vulnerability to terrorist actions then we must plan and act accordingly.

3 - Ferret out the enemy among us

We must seek out terrorists whether they are affiliated with a terrorist organization or are independent.

Individuals

To date the majority post of 9/11 terrorist attacks or attempts on domestic targets have originated from within the U.S. and have involved an individual or a small independent group. The terrorist(s) or would-be terrorist(s) does not "invade" per se. The terrorist arrives and stays in the U.S. or the benign U.S. resident becomes a terrorist. In either scenario we have people here in the U.S. who would do us harm and by dint of being here they have proximity to myriad targets.

As a free and open society there are limits. Per the U.S. Supreme Court ruling in Robinson *v* California (1962) someone cannot be arrested simply for their status. In other words one cannot be charged as a criminal unless they have committed a criminal act. By extension (having) the status of being a terrorist is not in itself a crime. However, plotting or conspiring to commit a terrorist or criminal act is.

We must locate would-be terrorists and keep close tabs on them. To profile based only on membership in a given community – or even all young males 18-35 is likely bias – and more importantly ineffective. However, to look within a target population and profile / search / filter based on relevant indicators is good police work. (Or good anti-terrorist work.)

The six factors cited by Gartenstein-Ross & Grossman are: (Gartenstein-Ross & Grossman 2009: 12-13)

1 – Adopting a legalistic interpretation of Islam
2 – Trusting only select religious authorities
3 – Perceived schism between Islam and the West
4 – Low tolerance for perceived theological deviance
5 – Attempt to impose religious belief on others
6 – Political radicalization – Jihad

Add to the above an obvious indicator such as extended stays in certain overseas destinations. Additionally, we need to clamp down on persons who have entered the U.S. legally, say as students or visitors or green card workers and who have overstayed their legal "welcome." It seems that many of the 9/11 terrorists fit this profile. Caution is indicated as we may be "throwing out the baby with the bathwater." Many "innocents" may fit this expired visa profile.

Another key commonality among these terrorists is that although they may have been inspired by, trained by and / or taught by Al Qaeda, they have essentially acted independently. They may have learned how to make bombs from a terrorist "how-to" website, but they were on their own in purchasing components, obtaining vehicles for transport and in recruiting team members. This degree of independence can be viewed as both a positive and a negative.

Since this paper focuses on protecting our infrastructure it must be noted the majority of the plots which have received public (unclassified) notice have focused on killing people as opposed to attacking infrastructure. This may be because critical infrastructure is a harder target and in many cases is wrapped in greater security, or because killing people is a more direct, vengeful act in concert with the mentality of the newly spawned terrorist.

Organizations

Primary among the organizations we must ferret out is Al Qaeda[5]. Even when not directly acting with domestic terrorists or attacking in the United States Al Qaeda has caused us to alter our lifestyle, expend billions of dollars and our most precious resource – the lives of our soldiers. A most troublesome aspect is that Al Qaeda might be considered a franchise. General Stanley MCChrystal former Commander of the International Security Assistance Force (ISAF) and Commander, U.S. Forces Afghanistan (USFOR-A) first refers to Al Qaeda as a brand but later provides a precise description of Al Qaeda as a franchise. "Beginning in 2003, this decentralization forced Al Qaeda to rely on what became known as its franchises" – in Algeria, Libya, Saudi Arabia, Yemen, Somoalia, and Iraq." (McChrystal 2013: 115) This results in a more diverse enemy (enemies) that is harder to identify, locate and thwart (and / or kill.)

4 -Impede enemy funds flow

Although external funds and tangible resources as opposed to training and "how-to's" have not played a significant role in domestic post 9/11 terrorist plots the flow of funds to would-be terrorists has a strong potential for escalating terrorist capabilities. The old adage of "follow the money!" still applies.

Money is the lifeblood of any organization. There is a well entrenched "hawala" system within the Arab community which is likely immune to intervention. But Swiss banks and other similar offshore banks provide additional facilities for funds flow and these must be addressed. Similarly, certain "charities" have been instrumental in funding terrorist activities. The diversion of U.S. foreign aid and U.S. war zones expenditures into terrorist coffers also needs to be further

[5] While this paper does not focus on Al Qaeda, it is important to briefly examine its role.

addressed. For example, there are various news reports claiming that Yasir Arafat diverted over a billion dollars to his personal account.

Summary

In conjunction with conventional assessments of infrastructure vulnerabilities a more offense minded approach is needed to exploit the vulnerabilities of would be terrorist actors. This in turn impacts the original infrastructure vulnerability assessments. It is recommended then that an aggressive program specifically targeting terrorists be implemented.

Bibliography

Art, R.J. & Waltz, K.N., (1971), *The use of force – International politics and foreign policy*, Boston, MA, Little, Brown and Company.

Gartenstein-Ross, Daveed & Grossman, Laura. (2009), "Homegrown Terrorists in the U.S. and U.K. FDD Press, Foundation For Defense of Democracies, Washington, D.C.

Krauthammer, Charles. "In defense of the president's drone war against al-Qaida" The Washington Post 13 February 2013:

McChrystal, Stanley A., (2013), *My Share of the Task: a Memoir*, New York, NY, Penguin Group.

Peters, R., (2002), *Beyond Terror*, Mechanicsburg, PA, Stackpole Books.

Singer, Carl A., (2003) The MegaPole, retrieved March 24, 2013, from author's website: http://www.ProcessMakesPerfect.net/The MegaPole.pdf

TRADOC, DCSINT Handbook No. 1.02, Critical Infrastructure Threats and Terrorism, *US Army Training and Doctrine Command, Deputy Chief of Staff for Intelligence. Assistant Deputy Chief of Staff for Intelligence – Threats Fort Leavenworth, Kansas ,10 August 2006*