Information Analysis and Infrastructure Protection

Competitive Analysis and Evaluation Office

16 September 2003

Strategic Red Cell: How Terrorists Might Exploit a Hurricane

A key component of the IAIP/Competitive Analysis and Evaluation Office's mission is convening a diverse range of governmental and nongovernmental experts who adopt a terrorist mindset to challenge traditional or existing assumptions about how terrorists might attack some aspect of our critical infrastructure. The ideas generated by these "red cells" contribute insights on potential terrorist threats to the homeland for state and local governments, law enforcement, and industry.

An ad hoc IAIP/CAEO red cell of more than 35 experts from intelligence, industry, military, and academia on 16 September 2003 provided insights as to possible terrorist exploitation of a hurricane. Respondents assumed the threat was a high category hurricane that would strike the US East Coast. Participants indicated that the probability of a terrorist attack during a hurricane was low. However, they outlined the three most likely methods by which terrorist could potentially exploit the opportunity:

- Observe security measures to plan for a future event
- Target evacuation routes and emergency shelters
- Cyber attacks

Most Likely Actors and Motivations

Respondents identified a lone actor or small terrorist splinter cell, rather than an established terrorist group, as most likely to exploit a hurricane. The profile would be a person or small group that could operate with ease domestically, be opportunistic and possibly disenfranchised. A lone actor or small group would be seeking attention rather than pursuing a political agenda, and would retain the capability to act without extensive planning.

Network-based groups such as Hamas, Al Qaeda and Hezbollah were discounted because of their traditional long-range planning processes. However, members noted as an option a group that might already have an attack plan in place, ready for an opportunistic moment where infrastructure and emergency responder resources are already stressed due to a natural disaster. Members considered this a low probability, because of the unpredictable nature of hurricanes, the inability to determine location, and the varying intensity. Additional information on the profiles of the participants include:

- Religious extremist groups may seek to leverage the natural disaster as a sign from God and take it as a signal to attack. Washington D.C. being the target of a major disaster could be interpreted as a sign of God condemning the United States.

- The Y2K event provides historical evidence of terrorist groups trying to exploit circumstances that threatened infrastructures and may provide a planning precedent. Terrorists unsuccessfully planned to capitalize on the resulting confusion and chaos if Y2K had created panic or destabilization in the United States.

Threats and the Hurricane Lifecycle

Red Cell respondents examined vulnerabilities that might arise during the life cycle of a hurricane, as well as potential threats to exploit these vulnerabilities. The hurricane lifecycle was divided into three components: pre-event, during, and post-event. Physical threats during the event were considered highly unlikely, due to the logistical complexities involved in preparing and mobilizing assets in extreme weather. However, participants noted that a natural disaster could be used as a diversion or a way to capitalize on the concentration of Federal resources in one area of the country while an attack is staged. A cyber attack could be utilized throughout the hurricane life cycle to cause increased confusion and panic while avoiding the logistical issues of mounting an operation in an unstable environment. The following chart breaks down each threat, impact and vulnerability identified by red cell respondents.

Pre-Event

Threats	Impact	Vulnerabilities
Targeting of Evacuation Routes	• Mass panic • Possible high casualties • Destabilization • Loss of public confidence in the government • Immobile population • Increased media coverage	• Soft target • Mass of population along the transportation infrastructure (e.g. Chesapeake Bay Bridge or Bridge-Tunnel, North Carolina bridges, tunnels, key choke points) • High profile nature (thousands stranded along an evacuation route) • Clearly identified evacuation routes make them susceptible to attack • Could lead to a failure to evacuate
Critical Infrastructure Surveillance	• Low initial value; yet useful information for future attacks • Detailed reconnaissance opportunity	• Preparation procedures may be easily observed • Terrorists adapt strategically not tactically
Targeting of a shopping mall, grocery store or home improvement center as public prepares for a hurricane	• Possible high casualties • Destabilization and fear • Panic • High media coverage	• Congregation of population • Low security

Pre-Event Summary: The most likely exploitation of the hurricane identified by respondents in the pre-event period is surveillance by terrorist individuals or groups to understand security measures of hard targets—such as nuclear or government facilities. Terrorist could observe precautionary measures to gauge emergency response resources and continuity of operation plans at critical infrastructures.

Event

Threats	Impact	Vulnerabilities
Critical Infrastructure and Key assets	• High shock value • Low panic since population is immobile	• Decreased security presence • Weakened infrastructure from a natural event may provide opportunities for terrorists • Hostage opportunities • Potential reduction of personnel due to emergency
Communication Centers	• Panic	• Increased reliance upon communications during an event
9-11 Call Centers Emergency Broadcast Network	• Moderate public panic	• Increased reliance on emergency communications during an event • Increased volume may already impact the system
Communication towers and infrastructures	• Confusion • Hamper ability to respond • Loss of life • Incite panic	• Communication is critical to respond to an attack, but is potentially vulnerable to a target attack, either cyber or physical
Tidal Surge	• Variable depending on what target and the method of attack	• May utilize flooding to access infrastructure • Tidal surge may destroy key security measures at facilities and terrorists may leverage this weakness and attack • May provide access via water to critical sites • Potential attacks on dams

Event Summary: Physical attacks during an event were considered less likely due to the severe weather, unpredictability of the storm path and the difficulty of mobilizing resources. Hard targets such as critical infrastructures may be more difficult to attack during the storm since they will have initiated emergency operations. In addition emergency responders will have a greater presence in areas due to emergency shift schedule operations.

Post-Event

Threats	Impact	Vulnerabilities
Contamination in distribution chain of emergency relief	• Stress public health system • Increase media coverage • Further destabilization	• Low security • New distribution mechanisms without clarified roles
Bomb threats or anthrax hoax type of attack	• Panic • Stress public health system • Increase media coverage	• High alert of the public • Weakened emergency response capabilities • Overloading of hospitals and health care infrastructure

Post-Event Summary: In the post-event, terrorists may build on public panic to further destabilize the system by disseminating rumors of infectious diseases or water supply contamination.

Entire Hurricane Lifecycle

Threats	Impact	Vulnerabilities
Evacuation Shelters	• High value target to incite panic • Destroying a place of refuge will cause a loss of confidence in the government's ability to protect its citizens	• Mass of population along transportation infrastructure (e.g. bridges, tunnels) • Minimal security, numerous bags and suitcases, concentrated population • Manned by volunteers (e.g-lax security)
Cyber attacks	• Confusion • Economic impact • Public agitation	• Terrorists may exploit key web sites to pass erroneous information • May seek to gain control of key assets (e.g water dam, SCADA systems) during an event to create havoc • Denial of service, network intrusions, release of malicious codes
Impersonation of first responder personnel (e.g.-fire rescue, electric restoration)	• Moderate Hysteria	• Lack of identity checks and increased willingness to leverage resources of other communities and welcome assistance

Entire Life Cycle Summary: Experts felt that cyber terrorism may be the most likely and potentially dangerous attack that could be mounted easily – locally or internationally – during all phases of the storm. A cyber attack could produce erroneous information on the storm to confuse the population, hamper critical infrastructures during the storm thereby increasing instability and response efforts. Denial of service attacks on infrastructures such as the 911 system could be widespread and impact communication between first responders and the public.

In addition, attacks on soft targets or disaster areas by persons or groups disguised as first responders or infrastructure repair personnel were considered a potential vulnerability, especially considering the mobilization agreements in place. Such an attack would likely cause panic and frustrate efforts by emergency management personnel to respond to the effects of the hurricane. Natural disaster sites have less security than terrorism disaster sites and it may be easy to manipulate the confusion and chaos to access high value targets.