Information Analysis and Infrastructure Protection,
Department of Homeland Security

IAIP Analytic Red Cell Program

How Terrorists Might Exploit a Hurricane

LIMITED DISTRIBUTION: Any release, dissemination, or sharing of this document, or any information contained herein, is not authorized without approval from the Department of Homeland Security (DHS). Release to Intelligence Community is authorized. All requests for further dissemination outside of Intelligence Community entities must be approved by the DHS, Information Analysis - Requirements Division (IA-R) via DHS.IAIP@DHS.GOV.

September 15, 2004

Project Overview

This paper updates the results of a September 2003 analytic red cell session of more than 35 experts from intelligence, industry, military, and academia. That group was asked to speculate on possible terrorist exploitation of a high category hurricane.

Program Concept

The IAIP Analytic Red Cell program provides alternative assessments intended to provoke thought and stimulate discussion. Papers represent an assimilation of opinions, sources, and methodologies and are not necessarily derived from specific threat reporting. Papers are not meant to represent an IAIP, DHS, or U.S. Government corporate view.

Summary: *Terrorists are unlikely to exploit a hurricane, according to an independent group of governmental and nongovernmental experts asked to speculate on this issue. However, if terrorists were to do so, they would have several opportunities. One opportunity would be for a group like al-Qaida to capitalize on the hurricane—and its strain on emergency response and security personnel—to launch a strike elsewhere in the region or country. Moreover, organized groups, splinter cells, or lone wolf terrorists might observe security measures to help planning for a future event, target evacuation routes and emergency shelters, or even impersonate emergency responders to attempt to gain access and cause destruction. Possible mitigation strategies include maintaining vigilance and emergency response preparedness across the nation for a potential simultaneous terrorist attack. They also include increased security procedures at shelters, vigilance at evacuation chokepoints (tunnels, bridges), and reporting of unfamiliar vehicles and personnel.*

Exploiting Hurricane for a Simultaneous Attack

An independent group of nongovernmental and governmental experts concluded that organized terrorist groups are unlikely to capitalize on a hurricane. The planning these groups normally require would be complicated because hurricanes are unpredictable, their locations shift, and intensity varies.

However, it is conceivable that a terrorist group like al-Qaida, if it had plans in place for an attack elsewhere in the region or country, might attempt to time such an attack to a hurricane.

- Terrorists might hope that such an attack would capitalize on the deployment of security and emergency response resources to the area of the hurricane so as to increase chances for a successful strike and more difficult recovery.

- Terrorists might even hope that National Guard and other units are less able and well-equipped to respond to multiple events in the homeland because of deployments overseas.

Threats on Site and the Hurricane Lifecycle

Participants in the analytic red cell examined vulnerabilities that might arise during the life cycle of a hurricane, as well as potential threats to exploit these vulnerabilities at the hurricane site itself. The hurricane lifecycle was divided into three components: pre-event, during, and post-event.

The participants assessed that a splinter terrorist cell or a lone actor, rather than an established terrorist group, would be more likely to exploit a hurricane on site. This could include persons pursuing a political agenda, religious extremists, or other disgruntled individuals.

The following section provides charts breaking down the potential threat, impact and vulnerability for the entire life cycle, and the particular phases of a hurricane.

Entire Life Cycle Analysis: Several types of exploitation or attacks may potentially be conducted throughout the hurricane lifecycle — hostage situations or attacks on shelters, cyber attacks, or impersonation of emergency response officials and equipment to gain access. Hostage situations are particularly worrisome due to the recent events in Beslan, Russia, normally limited security in evacuation shelters, high density of people, and the high publicity for this type of attack.

Entire Hurricane Lifecycle

Threats	Impact	Vulnerabilities
Hostage Situation or Attack on 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 • Confusion through erroneous information	• 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	• Moderate Panic	• Lack of identity checks and increased willingness to leverage resources of other communities and welcome assistance

Pre-Event Analysis: The most likely exploitation of a hurricane 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. Terrorists could observe precautionary measures to gauge emergency response resources and continuity of operation plans at critical infrastructures.

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 (key choke points) • High profile nature • Clearly identified evacuation routes 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

Threats	Impact	Vulnerabilities
Targeting of a shopping mall, grocery store or home improvement center as public prepares	• Possible high casualties • Destabilization and fear • Panic • High media coverage	• Congregation of population • Low security

During Event Analysis: Physical attacks during an event are 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 security personnel will have initiated emergency operations. Emergency responders will have a greater presence in areas due to emergency shift schedule operations.

During Event

Threats	Impact	Vulnerabilities
Attack on Critical Infrastructure and Key Assets	• High shock value • Low panic since population is immobile	• Decreased security presence • Weakened infrastructure from a natural event • Hostage opportunities • Potential reduction of personnel
Cyber attack on 9-11 Call Centers Emergency Broadcast Network	• Moderate public panic	• Increased reliance on emergency communications during an event • Increased volume may impact system
Physical or Cyber Attack on 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
Increased Access, Ability to Attack via 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 • May provide access via water to critical sites, attacks on dams

Post-Event Analysis: After the event, terrorists may build on public panic to further destabilize the system by disseminating rumors of infectious diseases, or actually contaminating emergency food and water supplies.

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 CBW Hoax	• Panic • Stress public health system • Increase media coverage	• High alert of the public • Weakened emergency response capabilities • Overloading of hospitals and health care infrastructure

Recommendations

Based on the above speculation, several actions might help mitigate or prevent potential terrorist exploitation of a hurricane.

- Maintain nationwide security and emergency preparedness in the event of an attempted terrorist strike elsewhere in the region or country during the hurricane.

- Remind corporate security directors to observe and report casing of critical infrastructure by unfamiliar vehicles and personnel during the period of heightened hurricane security, as well as report missing personnel and equipment.

- Institute increased security procedures (e.g. identification checks) at evacuation centers and shelters.

- Increase patrols and vigilance of staff at key transportation and evacuation points (for instance, bridges and tunnels), including watching for unattended vehicles at these locations.

- Advise the first responder community, telecommunications personnel, and power restoration personnel to increase identification procedures to prevent imposters from gaining unauthorized access to targets.

- Ensure even reallocation of emergency response resources across the country to prevent regions adjacent to the hurricane being left uncovered by emergency response personnel.

- Ensure that food and other emergency relief supplies are secure.

Who Took Part in the Red Cell

- Senior corporate security representatives
- Academics and consultants
- U.S. Department of Homeland Security
- U.S. Marine Corps
- Sandia National Laboratory
- Central Intelligence Agency