commandeleven
SECURING YOUR SIX

United States Hospital Threat Assessment

Threat Assessment - April 2025
https://commandeleven.com

info@commandeleven.com
https://twitter.com/commandeleven

Report Author

"United States Hospitals Threat Assessment" was written and researched by CommandEleven.

About CommandEleven

CommandEleven is an intelligence and analysis firm, based in Pakistan, with assets, analysts, and researchers offering apolitical analysis on topics such as security, geopolitics, defense, and espionage. CommandEleven's intelligence includes Afghanistan, Pakistan, and Kashmir.

CommandEleven, founded in 2015 as a think tank and policy advisory, with the objective of democratizing intelligence, simplify its understanding and real-life application, while offering guidance to governments, agencies, media, and private organizations.

CommandEleven continues to inform and guide public policy and decision-makers in the government, business, and military through a rigorous program of publications, conferences, digital media, policy briefings, and recommendations.

Introduction

Topic: Hospital Attacks in the United States and Canada

Assessment Number: CMDELVN-THREATASSESS-2025-135

Summary & Purpose:

The threat assessment presented below is to advise and assist hospitals and trauma centers in preparing for an upcoming terrorist attack orchestrated by Islamic State Khorasan Province (ISKP), as a prelude to a secondary attack by al Qaeda.

This assessment has been reviewed and discussed by numerous individuals who are part of our intelligence advisory network, including Orange Diamond Consulting Group, Transatlantic Intelligence Consortium, Sarah Adams, and Ron Jost.

Bottom Line Up Front (BLUF):

Hospitals and Tier 1 trauma centers are being targeted for attack by the Islamic State Khorasan Province. The targeting is focused on mid-tier cities around the United States and Canada. The attacks will be multi-city and simultaneously carried out.

Intelligence Credibility: Credible - Highly Credible

This intelligence was gathered by CommandEleven human intelligence assets inside of Islamic State Khorasan Province training camps in both Afghanistan and Pakistan. These assets have been providing information since the end of January, but intelligence became more detailed starting in mid-February and continues to flow into our intelligence classification center.

This information was reviewed in detail, compared with additional intelligence gathered from other sources, classified based on credibility, and sorted into understandable information that was first passed to external analysts that

collaborate with CommandEleven, then passed to law enforcement and intelligence agencies in the United States.

Second, there are already numerous terrorist sleeper cells already inside the United States and Canada, as well as individuals actively being radicalized, whose identities are still unknown to any analyst.

Our estimation, based on the chatter within the camps, is roughly 30-50 operational sleeper cells within the United States and Canada at this time, with more cells being created weekly.

Therefore, it should be clear that **this attack will be carried out by terrorist who are already in the United States**, not individuals infiltrating the United States specifically for this attack.

SITREP:

- US internal security has been seriously compromised due to the Biden open borders policy, which facilitated the infiltration of terrorists from the northern and southern borders of the United States
- A second tier was also infiltrated into the United States via manufactured passports from the Sirajuddin Haqqani controlled Afghanistan Immigration department
- These terrorists have taken safe haven in predominantly high-Muslim population areas, university campuses, and suburbs of mid-tier cities, where movement can easily be made for reconnaissance and surveillance purposes
- The following links have been identified:
    - Hospitals that have been targeted via cyber-attacks or ransomware have also been targeted with surveillance and attempts to breach/test security protocols
    - Since our alert on March 18th, numerous reports have been received of suspicious individuals been seen, captured on video and interacted with hospital staff members inquiring about hospital security protocols
- On March 02, jihadi groups circulated a graphic with US hospitals circled in red with the title – “Soft flesh awaits”

Expected Tactics:

There have been a number of "tests" that have been carried out to test the following:

- First responder response time
- Which first responders respond
- Reaction of the general public in real-time to determine additional attack opportunities

One key item that we have been able to identify is that the hospitals that have been targeted with either cyber-attacks or ransomware attacks, have also been targeted for surveillance and reconnaissance. We have included a list of known cyber and ransomware attacks in an appendix.

We believe the New Orleans attack on January 1st was a test, using a method successful in European cities, with the addition of an explosive that was not detonated – IEDs were strategically placed around the accident location and on routes that would be used by first responders.

The methodology test was to penetrate the first layer of security and detonate a vehicle-based improvised explosive device (VBIED), causing mass casualties, when first responders entered into the attack area, the planted IEDs would be detonated delivering a second level of causalities.

Potential Attack Scenarios:

Based on the human intelligence (HUMINT) that has been gathered and confirmed, we have been able to identify 3 different potential attack models:

- 11/26 Mumbai attack
- 10/07 Israel attack
- 03/03 Mannheim, Germany attack

Again, based on the conversations in the terror camps in Afghanistan and Pakistan, the attack scenario will start with:

- a VBIED breaching the main level of the building and detonating
- followed by small assault teams taking control of the hospital, with hostages, including high ground for snipers against any law enforcement and first responders
- this will be a multi-city, coordinated attacks designed to hit the US at its weakest security point with the highest psychological impact – hospitals

We believe, based on the intelligence chatter that we are receiving, the attack will be a mixture of both the Mumbai and Mannheim attacks.

IMPACTS:

For an intelligence and terrorism official, mid-tier cities present the hardest targets to protect and identify potential threats. A mid-tier city is defined as those cities whose population falls between 100,000 and 500,000 residents, making them large enough to maintain LEVEL ONE trauma centers, but lacking the security of metropolitan cities, such as New York City, Los Angeles, Chicago, Washington, DC.

The selection of a mid-tier city is made based on specific criteria:

- large enough to get media attention, but small enough to be vulnerable
- all infrastructure of major cities exists without the same security presence as top-tier cities
- law enforcement will most likely not have advanced counter-terrorism training, meaning the attack can be sustained while reinforcements with advanced training are able to reach the location - slowing emergency response
- significantly lower surveillance allowing terrorists more freedom of movement without detection

Mid-Tier Cities Believed to be Vulnerable

The list provide below is based on numerous criteria, as defined above:

- Birmingham, Alabama
- Tempe, Arizona
- Pasadena, California
- Modesto, California
- San Diego, California
- Colorado Springs, Colorado
- Bradenton/Sarasota, Florida
- Fort Myers, Florida
- St. Petersburg, Florida
- Boise, Idaho
- Wichita, Kansas
- Louisville, Kentucky
- Grand Rapids, Michigan
- Rochester, Minnesota
- Omaha, Nebraska
- Trenton, New Jersey
- Raleigh, North Carolina
- Albuquerque, New Mexico
- Albany, New York
- Buffalo, New York
- Syracuse, New York
- Dayton, Ohio
- Columbus, Ohio
- Toledo, Ohio
- Tulsa, Oklahoma
- Harrisburg, Pennsylvania
- Pittsburgh, Pennsylvania
- York, Pennsylvania
- Providence, Rhode Island
- Knoxville, Tennessee
- Nashville, Tennessee
- Austin, Texas
- College Station, Texas

- Houston, Texas
- Arlington, Virginia
- Richmond, Virginia
- Madison, Wisconsin
- Milwaukee, Wisconsin
- Marshfield, Washington
- Spokane, Washington

We are also closely reviewing areas where there is a large population of recently immigrated Muslims from Afghanistan, Syria and Iraq, who we believe could have terrorist ties and used manufactured (fake) passports to enter the United States during the Biden administration, when there was no vetting or security check. This is not a warning against all Afghans, but those whose passports are questionable, meaning carrying the birthdate of 01/01, 06/01 and 12/31/xxxx, which we have found many matches to this characteristic to avoid detection by immigration officials.

We have learned that there are many new employees from the above mentioned countries with passports that match the date sequences given that should be given special attention and review.

WHY MID-TIER CITIES:

We have determined mid-tier cities are being targeted for the following reasons.

Soft Targets

Major cities often have heightened security, greater counter-terrorism resources, and more robust surveillance systems, mid-tier cities, while still populous and symbolically important, usually lack the same level of protection, making them more vulnerable.

Maximized Disruption

Attacks in these cities can still generate significant media coverage and public fear. By striking locations that are not typically seen as likely targets, terrorists can amplify the psychological impact and spread anxiety across a wider region.

Symbolic Impact

Mid-Tier cities often represent the "heartland" or more everyday aspects of society. Attacking these locations may be aimed at demonstrating that no place is immune from violence, thereby undermining the sense of security in communities that might otherwise feel overlooked by national security priorities.

Operational Logistics

These cities may have infrastructure and transportation hubs that can be exploited for logistical support or as targets that cause broader disruption without the need for the high-profile elements of larger urban centers.

Additional Points

- Hospitals and trauma centers make high-casualty targets
- Smaller law enforcement budgets that large cities often prohibit funding for certain counter-terrorism measures including, but no limited to:
    - Advanced intelligence analysis
    - Surveillance technology
    - Tactical counter-measures
- Low federal presence = delayed counter-measures
- Disrupt daily American life with sustained panic
- Symbolic targets that strike fear nationwide but possibly avoid immediate military reprisal

RECOMMENDED SECURITY MEASURES:

1. Hospitals and trauma centres to complete full audits of their internal security protocols to limit the potential of a successful breach by ISKP terrorists
    a. Reviews of hospital security footage, attempting to identify any reconnaissance activities, repeat visitors, and suspicious activity.
        i. Perform a more comprehensive vetting of all newly hired (within the last 2 years) employees, contractors and their staff, service teams and vendors with building access

b. The restriction of specific vehicular access with barriers to allow for complete search of the vehicle by explosive sniffing dogs and questioning/identification checks of individuals.
    i. We are **highly concerned of the possibility of terrorists infiltrating hospitals in uniforms or hospital dress codes to avoid detection**. Hospital security must be heavily tightened to assure that modified identification credentials are not successfully used to gain entry.
    ii. Secure perimeter access – emergency rooms, loading docks and parking structures – where easy access can be used to infiltrate without alerting hospital security
c. Hospital security staff must be enhanced and perform practical drills to prepare for the potential of a breach attempt. This will require coordination with local law enforcement to gain strategic advantage over the terrorists.
d. Identification and access badges MUST be checked on a regular basis to assure that fake badges are not created to gain entry to secure areas of hospitals and trauma centers
e. Special attention must be paid to hospitals and trauma centers that have tunnels under their facilities. They must be heavily secured and searched to assure that no explosives have been planted there, nor can any unauthorized individuals gain access through those routes.

2. Law enforcement, intelligence and security agencies of the US and state governments actively identifying and arresting key operatives and disrupting the attack before it can be initiated
    a. Pre-emptive raids on known radicalised centres, where ISKP fighters could seek safe haven until the attacks are carried out
    b. Examination of storage facilities, locations close to, and within hospital premises, where weapons could be stored and easily accessed once the breach is achieved by terrorists.

Appendix A:

Known Cyber Attacks on Health Care Facilities 2025

- **Jan 02 - CYBER** - Connecticut - Community Health Center (CHC) USA breach which exposed the data of 1 million patients
- **Jan 24 - SWAT** - Loma Linda, California - Hoax call (swatting) of armed gunmen threatening to "shoot up" the Loma Linda University Medical Center triggered a massive police response, causing paediatric and surgical ward to be evacuated. News media speculated that it was a test of police response times
- **Jan 26 - CYBER** - Eden Prairie, Minnesota - Ransomware attack on Change Healthcare stealing approximately 190 million patient records - largest healthcare data breach in US history
- **Jan 29 - CYBER** - Fredrick, Maryland - Ransomware attack shuts down the entire Fredrick Health Medical Group
- **Jan 30 - CYBER** - New York, New York - New York Blood Center ransomware attack stops all blood donations
- **Feb 07 - CYBER** - Springfield, Illinois - Hospital Sisters Health Systems breached exposing over 882,000 patient records
- **Feb 24 - KINETIC** - Spokane, Washington - Fire outside regional hospital forces a full evacuation of the hospital
- **Feb 24 - KINETIC** - York, Pennsylvania - Gunman took staff hostage at University of Pennsylvania Medical Center Memorial Hospital, resulting in the death of a police officer and injuries to others. Gunman was killed on the spot.
- **Mar 14 - SWAT** - Pasadena, California - hoax call (swatting) at Huntington Hospital of an individual with a weapon, which caused the hospital to be placed on lock down.
- **Mar 14 - SWAT** - Marshfield, Wisconsin - Hoax call (swatting) of six bombs inside the hospital and an armed individual outside the hospital. Police called it a case of "domestic terrorism"
- **Mar 18 - CYBER** - Cyber Alert - FBI/CISA report a spike in Medusa ransomware attacks, including hospital
- **Mar 20 - KINETIC** - Troy, Michigan - Shooting in Corewell Health Beaumont Troy Hospital garage, 2 full access security key FOBs found in the hospital after the breach, suspect was arrested after a prolonged chase
- **March - CYBER** - Ohio State University Hospitals major cyber-attack that collapsed the entire system for almost 2 days

About the Author

"US Hospitals Threat Assessment" was written and researched by CommandEleven.

About CommandEleven

CommandEleven is a private intelligence firm, based in Pakistan, with assets, analysts, and researchers offering apolitical analysis on topics such as security, geopolitics, defense, and espionage. CommandEleven's intelligence includes Afghanistan, Pakistan, and Kashmir.

CommandEleven, founded in 2015 as a think tank and policy advisory, with the objective of democratizing intelligence, simplify its understanding and real-life application, while offering guidance to governments, agencies, media, and private organizations.

CommandEleven continues to inform and guide public policy and decision-makers in the government, business, and military through a rigorous program of publications, conferences, digital media, policy briefings, and recommendations.

Visit http://commandeleven.com for more information or contact info@commandeleven.com.