



GOVERNMENT FACILITIES SECTOR SNAPSHOT: MILITARY

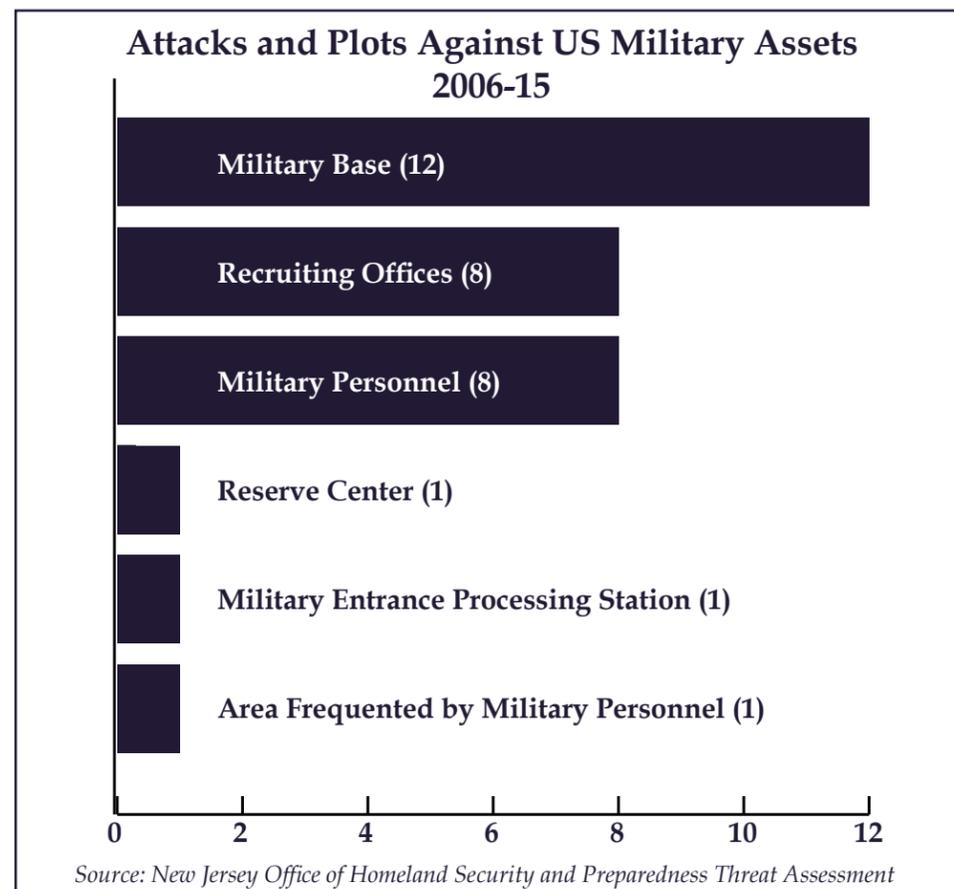


Sector Information

Military bases, recruiting offices, personnel, reserve centers, and entrance processing stations comprise the military component of the Government Facilities Sector. This includes Department of Defense facilities owned and leased by the federal government, and National Guard facilities controlled by their respective states.

New Jersey is home to four military bases: Joint Base McGuire-Dix-Lakehurst (Burlington and Ocean Counties), Picatinny Arsenal (Morris County), Naval Weapons Station Earle (Monmouth County), and US Coast Guard Training Center Cape May (Cape May County). The State is also home to the New Jersey National Guard, multiple reserve and Coast Guard units, and 31 recruiting stations.

Military facilities are attractive targets for terror attacks and plots by violent extremists. Between 2006-15, 19 of the 31 attacks against military assets in the United States – 61 percent – targeted those with less security than military bases.



Threat

Terrorism: Moderate

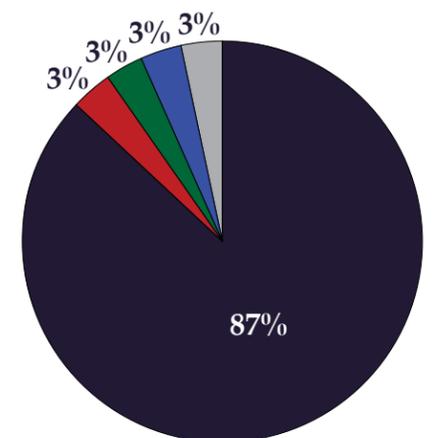
In September 2014, the Islamic State of Iraq and Syria (ISIS) released a message calling for lone offenders in the West to target the military. Since then, ISIS-inspired homegrown violent extremists have conducted two attacks and four plots targeting military assets in New York, Ohio, Illinois, Kansas, South Carolina, and Tennessee – including a July 2015 attack on military facilities in Chattanooga.

In 2015, sovereign citizen Thomas Deegan plotted to overthrow West Virginia's government by targeting state sites and National Guard facilities. Domestic extremists have plotted against the US military twice since 2012. The militia extremist group Forever Enduring Always Ready planned to attack Fort Stewart, Georgia in 2012.

Cyber: High

The cyber threat to the military is high because politically-motivated hackers and extremists, operating on behalf of terrorist groups, are persistently targeting the sub-sector. Military personnel are targets of state-sponsored cyber espionage actors seeking access to restricted data. In July 2015, Russian-based hackers infiltrated the Pentagon's e-mail system. Other cyber threats include the collection and release of personally identifiable information or "doxing," social engineering, distributed denial-of-service (DDoS) attacks, web application attacks, website defacements, network intrusion, exploiting unpatched system vulnerabilities, and theft of sensitive data and credentials.

Perpetrator of Attacks and Plots Against US Military Assets 2006-15



- Homegrown Violent Extremists (27)
- Militia Extremists (1)
- Sovereign Citizen Extremists (1)
- Anarchists (1)
- Unknown Actors (1)

Preparedness

Following the Chattanooga attack in 2015, military officials are developing new security measures to better protect recruiting stations. These include:

- Surveillance cameras
- Remote-locking doors
- Ballistic protection, such as shields and desk partitions

US military recruiters are also [undergoing training in active shooter exercises](#).

[Military policy](#) regarding social media is critical for operational security. Military personnel and their families are instructed to not reveal information on social media, such as unit locations or deployment dates. They are also reminded to enable privacy settings on all social media platforms and to disable automatic geo-tagging settings on devices to prevent accidental disclosure of sensitive information.

Intelligence Gaps

- What exercises would attract the attention of terrorist groups looking to target military establishments or personnel?
- What terrorist groups are actively plotting to attack US military facilities?
- What methods are terrorist groups using to compromise data of US military members?

Contact Information

For more information, please contact NJOHSP's Preparedness Bureau at preparedness@njohsp.gov.