



GOV. CHRIS CHRISTIE | LT. GOV. KIM GUADAGNO | DIR. CHRIS RODRIGUEZ

NJOHSP

OFFICE OF HOMELAND SECURITY AND PREPAREDNESS

Cyber-Terrorism: A Growing Threat

The cyber threat to New Jersey from terrorist groups is low despite their intent to target the United States. According to the FBI, terrorist organizations, including ISIS, al-Qa'ida, and Hizballah, are attempting to build offensive cyber capabilities, but to date they have had little to no success.



- In October, a media report citing federal sources indicated ISIS had attempted—unsuccessfully—to gain access to the US electric grid.

Terrorist groups are likely to continue developing cyber capabilities and will attempt disruptive or destructive cyber attacks as a means of intimidation and coercion. We assess ISIS is the most likely terrorist group to attempt cyber operations against US resources, but its capabilities remain limited to low-level activities such as socially engineered account compromises and website defacements.

- In August, Junaid Hussain, a British citizen reportedly responsible for leading cyber operations and recruitment for ISIS, was killed in Syria. Hussain allegedly released US service members' personal information last year—a tactic known as “doxing”—and used social media to inspire terrorist attacks in the West.

ISIS could leverage international hackers with more advanced cyber capabilities. These hackers often exploit targets of opportunity such as organizations with weak cybersecurity defenses. Large and thriving online black marketplaces, where off-the-shelf hacking tools and capable hackers offer intrusion or attack services for nominal fees, could also be utilized.

- In October, a Malaysia-based hacker was arrested on a provisional US arrest warrant alleging he hacked a US company's servers, stole personal information of 1,300 US military and federal personnel, and provided the data to ISIS, which subsequently released it on social media.

Terrorists Using Encryption Technology

The widespread proliferation of peer-to-peer (P2P) encryption technology has helped terrorists shield their communications from conventional surveillance techniques, creating digital safe havens for operational planning, command and control, logistics, and execution. Beyond the cryptographic challenges of surveilling this terrorist traffic, most technology companies lack access to terrorists' private encryption keys to unlock data in compliance with lawful search warrants.

This portion of the assessment was produced by the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC). Visit www.cyber.nj.gov to learn more.