This briefing was developed for **The Blue Book Project**, lead by the Commonwealth of Virginia, support by CNA, and funded through a FEMA regional catastrophic planning grant.

Blue Book Project Goal: Develop a coordinated operational process to support local, state, federal, and private sector priorities; support Virginia residents; and ensure continuity of government while managing consequences from a coordinated nation-state cyberattack on critical lifeline services.

The Blue Book Project

# Iran Threat Briefing

# Background

**Govt. of Iran believes it is currently engaged in a “soft war” with the U.S. and its allies.**

- Prevailing in cyberspace is critical to winning this conflict.

**Iranian cyber actors are aggressive and difficult to deter because the regime:**

- Views the boundaries between peace, competition, and war as blurred.
- Has been actively engaged in cyber conflict with its adversaries for decades.
- Perceives the actions of its adversaries in the information space as potentially posing an existential threat to the regime.

**Iran’s military and security services use cyber tools to collect intelligence, steal technology, distract their adversaries, and undermine their adversaries' societal cohesion and will to fight.**

- U.S. critical infrastructure is considered a legitimate target by the regime, even in peacetime.

# Threat actors

1. **Islamic Revolutionary Guard Corps (IRGC)**
   - Intelligence Dept.
   - Basij
   - Qods Force
2. **Ministry of Intelligence and Security (MOIS)**
3. **IT Sector**
4. **Militant Groups**
5. **Hacktivists**

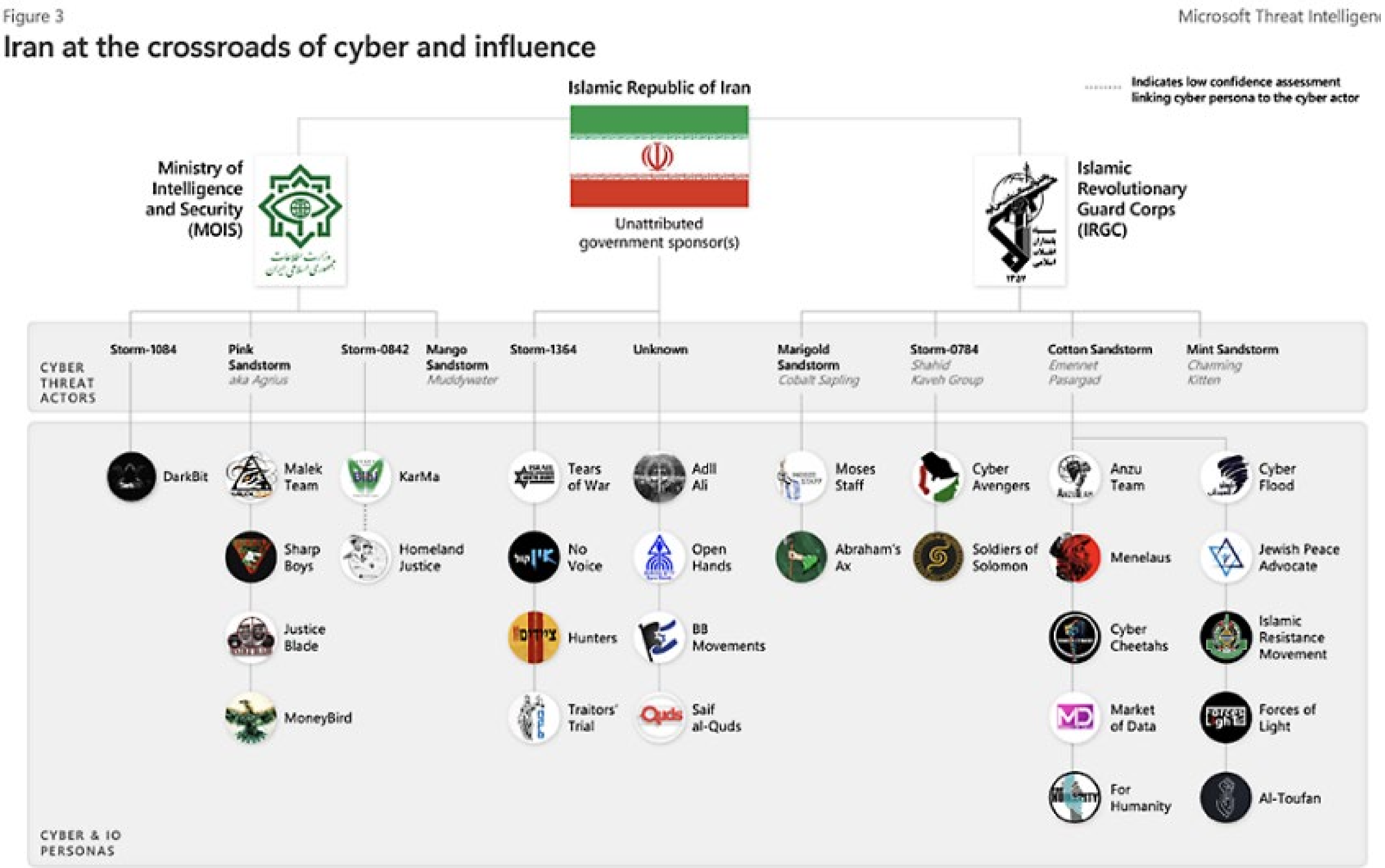


Figure 3

Iran at the crossroads of cyber and influence

Microsoft Threat Intelligen

Source: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas#:~:text=Iran's%20cyber%20and%20influence%20operations%20have%20progressed%20through%20multiple%20phases,precision%20or%20scope%20of%20impact.

# Capabilities and TTPs

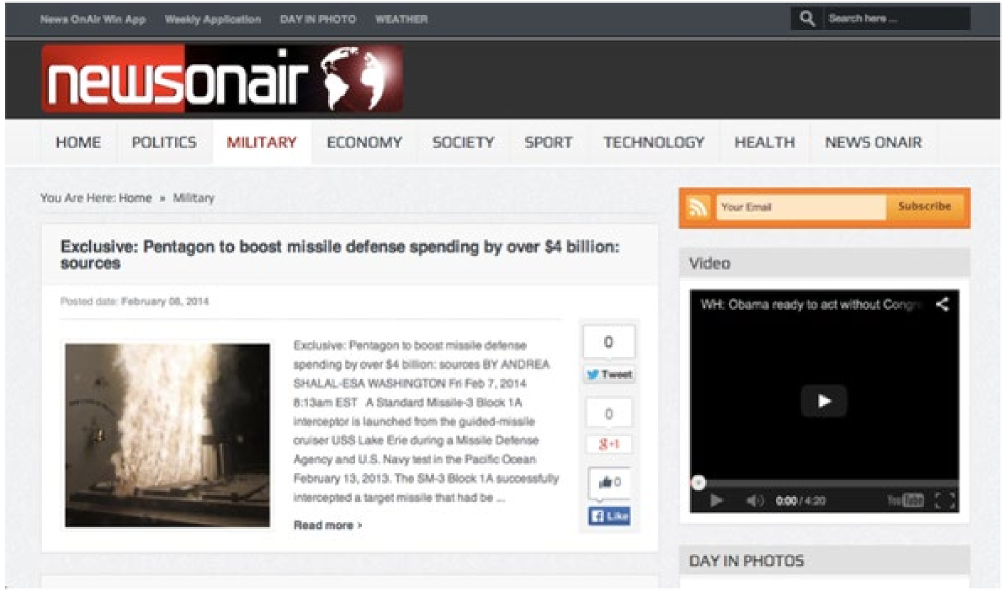
**Iran is a “tier-2” cyber power with modest, but growing capabilities.**

**Relative late-comer to cyber operations.**

**Following mass unrest in 2009, the regime made a serious investment in capabilities.**

**Tactics, techniques, and procedures (TTPs) have evolved:**

- From web defacements and redirects
- To using sophisticated social engineering techniques to harvest credentials, reconnoiter and compromise networks and cloud environments with malware, and install backdoors.



You Are Here: Home » Military

**Exclusive: Pentagon to boost missile defense spending by over $4 billion: sources**

Posted date: February 08, 2014

Exclusive: Pentagon to boost missile defense spending by over $4 billion: sources BY ANDREA SHALAL-ESA WASHINGTON Fri Feb 7, 2014 8:13am EST A Standard Missile-3 Block 1A interceptor is launched from the guided-missile cruiser USS Lake Erie during a Missile Defense Agency and U.S. Navy test in the Pacific Ocean February 13, 2013. The SM-3 Block 1A successfully intercepted a target missile that had be ...

Read more ›

WH: Obama ready to act without Congr

APT-42’s Operation Newscaster (2,000+ individuals affected)

Source: https://archive.nytimes.com/bits.blogs.nytimes.com/2014/05/29/cyberespionage-attacks-tied-to-hackers-in-iran/

# Targeting U.S. infrastructure (examples)

**Iranian-affiliated cyber actors have targeted a broad range of US infrastructure targets for financial gain (e.g., ransomware operations) and to lay the groundwork for potential future destructive, mass-casualty cyberattacks.**

**Communications:**

- Internet service providers (ISPs) (Cox Media Group, etc.)
- Navy-USMC NMCI: network reconnaissance, data exfil
- Federal, state, and local government websites: DDoS attacks on public websites

**Water and wastewater systems:**

- Municipal water treatment plant, Aliquippa, PA: Unitronics PLC rendered inoperable
- NY Bowman Dam: SCADA systems controlling sluice gates compromised

Bowman Dam sluice gate

Source: https://archive.nytimes.com/bits.blogs.nytimes.com/2014/05/29/cyberespionage-attacks-tied-to-hackers-in-iran/

# Targeting U.S. infrastructure (examples)

## Healthcare

- Ardent Health Services: ER ambulances rerouted (Thanksgiving, 2023)
- Boston Children's Hospital: attempted hack of environmental control networks (2022)

## Financial sector

- DDoS attacks on Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T and HSBC

## Cyber-enabled information operations

- Use of fake social media accounts to spread pro-Iran govt., anti-U.S. propaganda
- Spreading misinformation/disinformation to influence U.S. elections
- Doxing of U.S. officials

## Intelligence gathering to target Iranian expats

Boston Children's Hospital

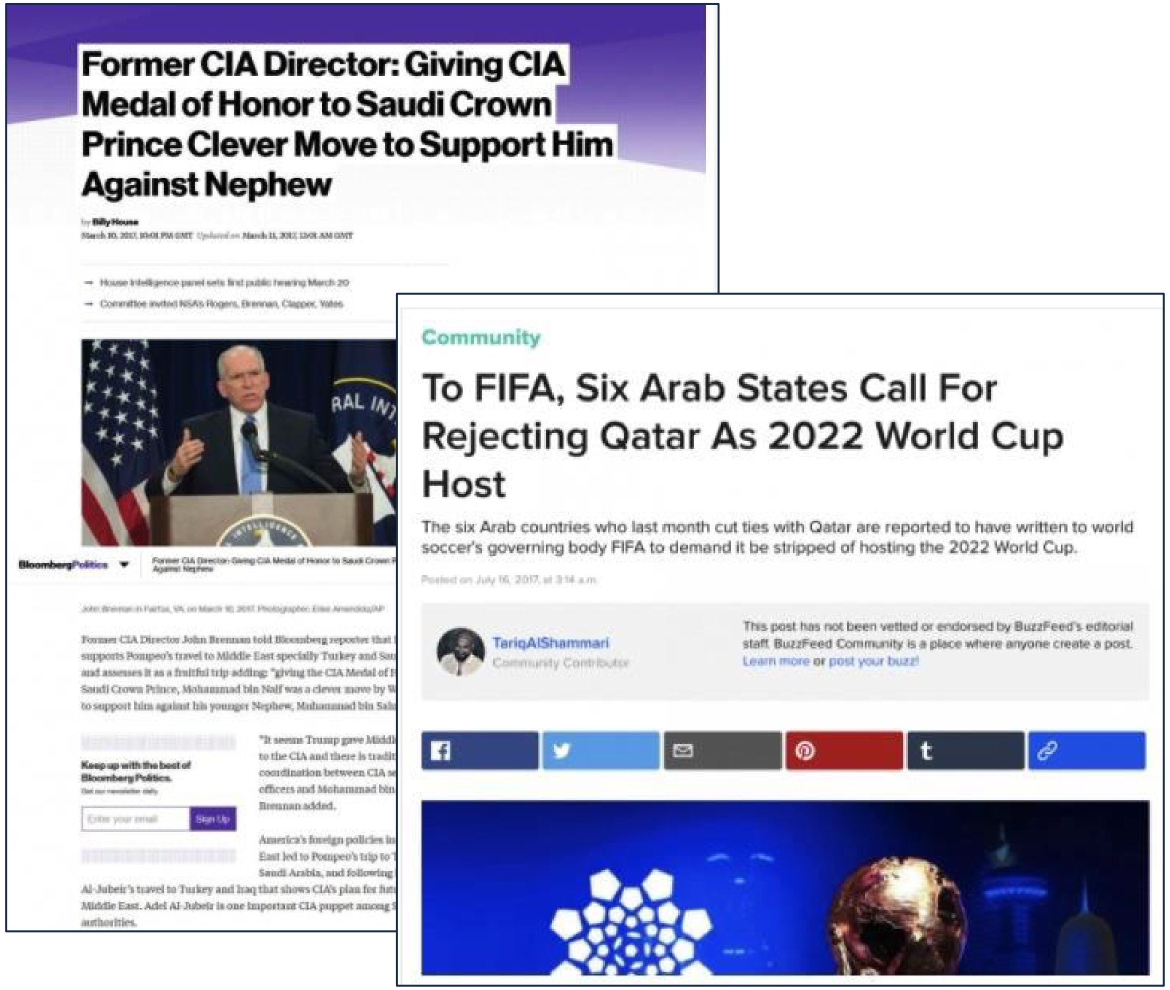
Source: https://www.zivanza.org/medical-institution/boston-childrens-hospital

# Examples of MDM Operations

## Endless Mayfly

Targets Iranian adversaries Saudi Arabia, Israel and the US

- 5+ years
- 70+ lookalike domains; fake personas; amplification of content
- Sowed confusion and degraded trust in content



**Former CIA Director: Giving CIA Medal of Honor to Saudi Crown Prince Clever Move to Support Him Against Nephew**

by Billy House
March 10, 2017, 10:01 PM GMT Updated on March 11, 2017, 12:01 AM GMT

→ House Intelligence panel sets first public hearing March 20
→ Committee invited NSA's Rogers, Brennan, Clapper, Yates

BloombergPolitics ▾ | Former CIA Director: Giving CIA Medal of Honor to Saudi Crown P Against Nephew

John Brennan in Fairfax, VA on March 10, 2017. Photographer: Elise Amendola/AP

Former CIA Director John Brennan told Bloomberg reporter that supports Pompeo's travel to Middle East specially Turkey and Sau and assesses it as a fruitful trip adding: "giving the CIA Medal of H Saudi Crown Prince, Mohammad bin Naif was a clever move by W to support him against his younger Nephew, Muhammad bin Salm

"It seems Trump gave Middl to the CIA and there is tradit coordination between CIA se officers and Mohammad bin Brennan added.

Keep up with the best of Bloomberg Politics.
Get our newsletter daily.
Enter your email | Sign Up

America's foreign policies in East led to Pompeo's trip to T Saudi Arabia, and following Al-Jubeir's travel to Turkey and Iraq that shows CIA's plan for fut Middle East. Adel Al-Jubeir is one important CIA puppet among S authorities.

Community

**To FIFA, Six Arab States Call For Rejecting Qatar As 2022 World Cup Host**

The six Arab countries who last month cut ties with Qatar are reported to have written to world soccer's governing body FIFA to demand it be stripped of hosting the 2022 World Cup.

Posted on July 16, 2017, at 3:14 a.m.

TariqAlShammari
Community Contributor

This post has not been vetted or endorsed by BuzzFeed's editorial staff. BuzzFeed Community is a place where anyone create a post. Learn more or post your buzz!

# Let’s Connect

CNA

**Feel free to email us with questions**

**bluebookproject@vdem.virginia.gov**

**Check out the Blue Book TV Reading Corner for more information and resources**

**Reading Corner - The Blue Book Project | VDEM**

The Blue Book Project