

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



CNA

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

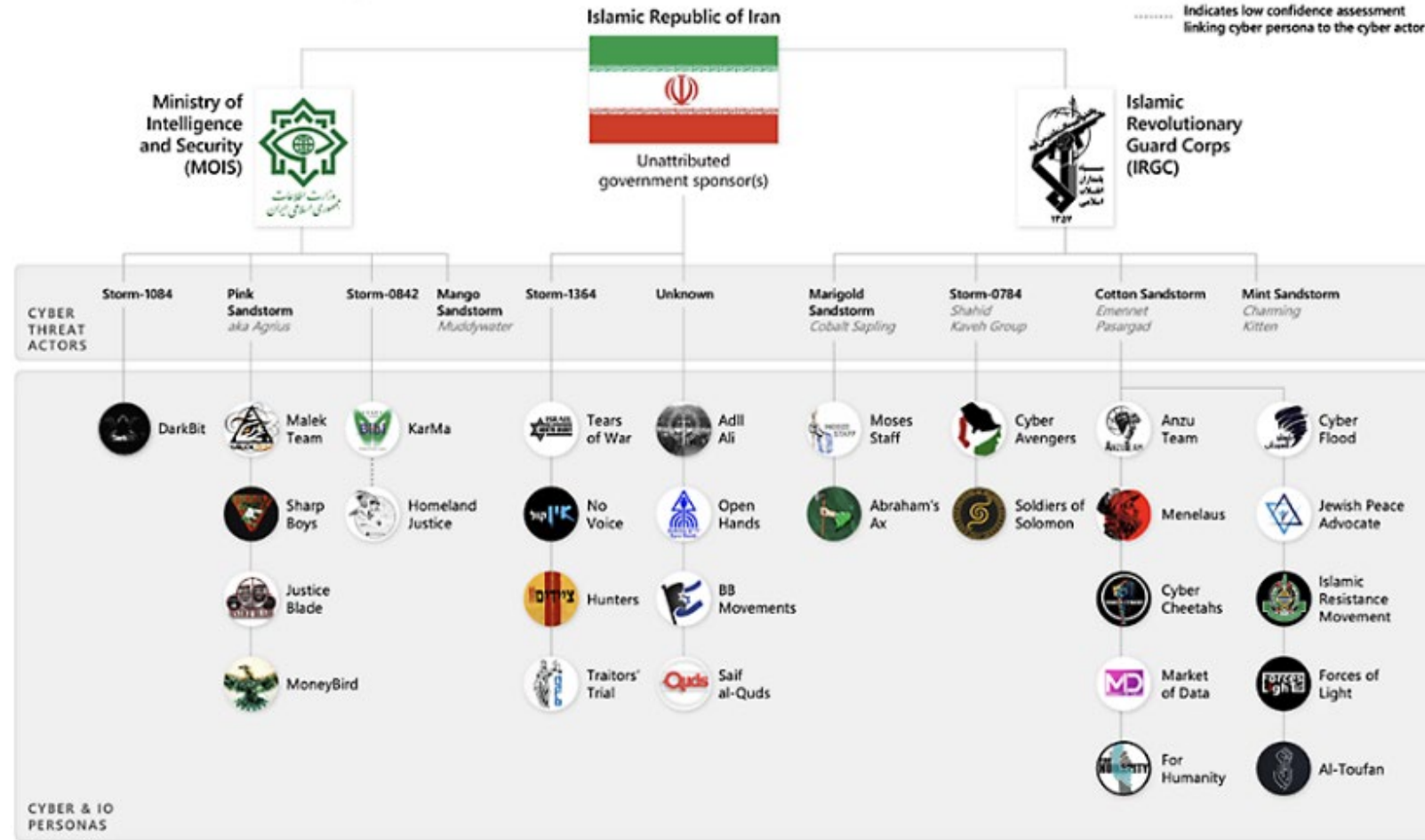
2. Ministry of Intelligence and Security (MOIS)

3. IT Sector

4. Militant Groups

5. Hacktivists

Figure 3
Iran at the crossroads of cyber and influence



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.



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 false 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>



The
Blue Book Project



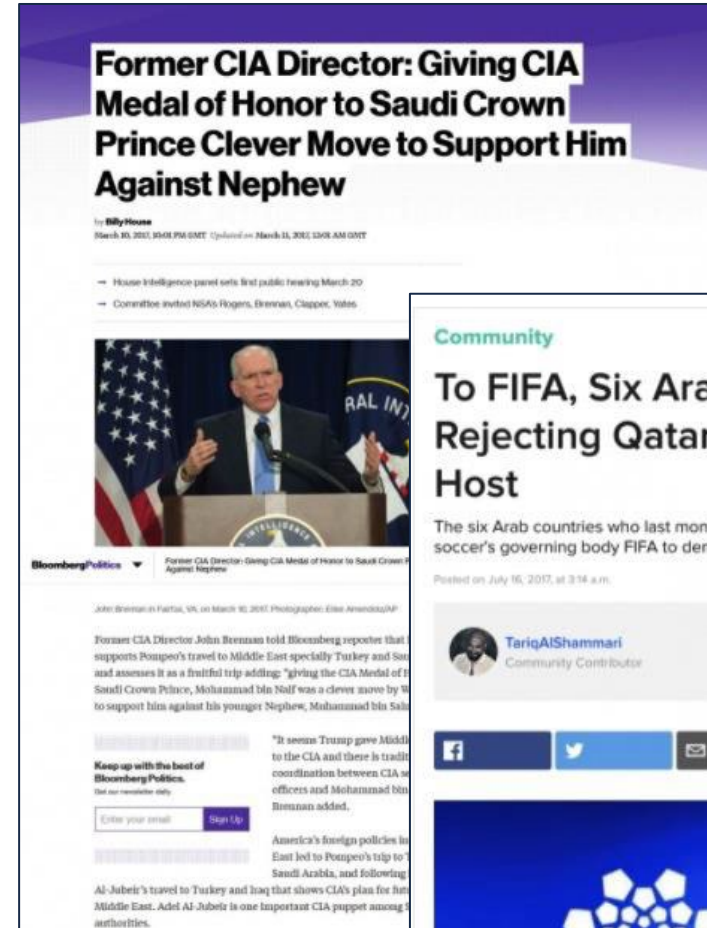
Iran's use of false and misleading information



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



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](#)

