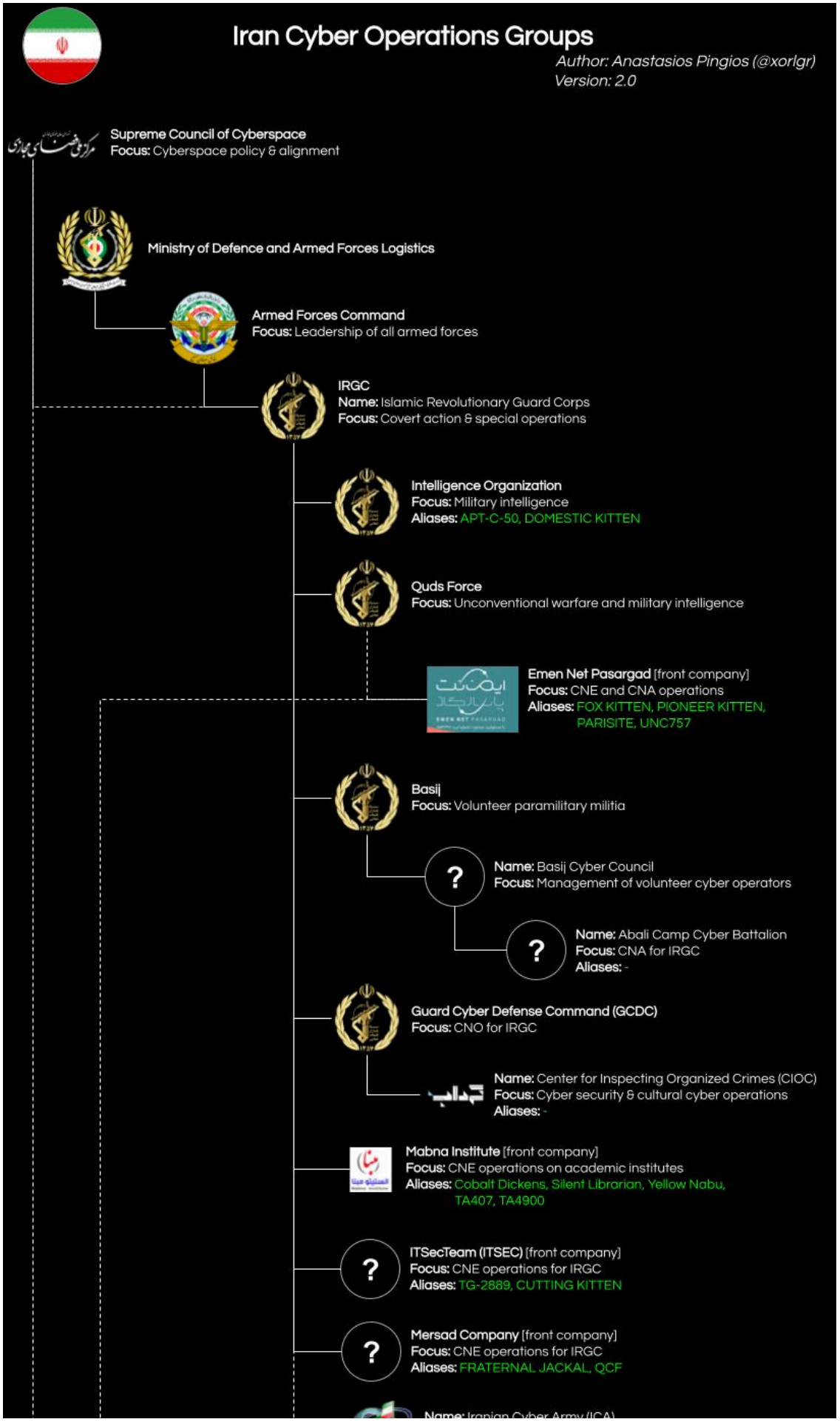
Iran Cyber Operations Groups

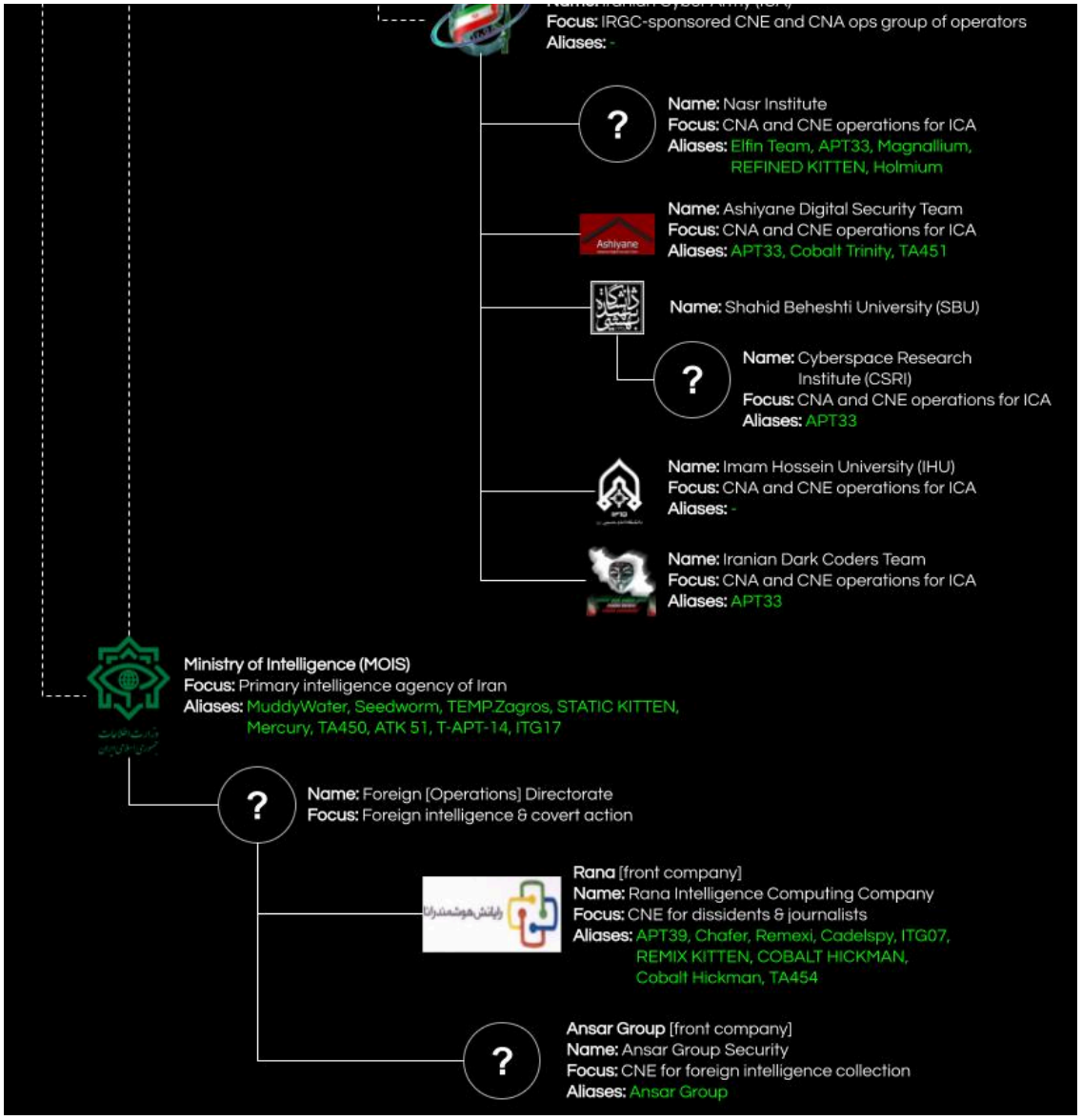
Published: 2021-05-06 · Archived: 2026-04-05 16:15:12 UTC

Unsurprisingly, after Russia, US, China, DPRK (North Korea), and EU… Here comes the mapping of the offensive cyber operations groups of Iran that have been attributed to a known government entity. Just like in the previous posts, sources and change log are available under the diagram.

If you notice anything missing, incorrect information, mistakes or anything like that please let me know to update it accordingly.

Last update: 13 January 2022


Iran Cyber Operations Groups
Author: Anastasios Pingios (@xorlgr)
Version: 2.0
Supreme Council of Cyberspace
Focus: Cyberspace policy & alignment
Ministry of Defence and Armed Forces Logistics
Armed Forces Command
Focus: Leadership of all armed forces
IRGC
Name: Islamic Revolutionary Guard Corps
Focus: Covert action & special operations
Intelligence Organization
Focus: Military intelligence
Aliases: APT-C-50, DOMESTIC KITTEN
Quds Force
Focus: Unconventional warfare and military intelligence
Emen Net Pasargad [front company]
Focus: CNE and CNA operations
Aliases: FOX KITTEN, PIONEER KITTEN, PARISITE, UNC757
Basij
Focus: Volunteer paramilitary militia
?
Name: Basij Cyber Council
Focus: Management of volunteer cyber operators
?
Name: Abali Camp Cyber Battalion
Focus: CNA for IRGC
Aliases: -
Guard Cyber Defense Command (GCDC)
Focus: CNO for IRGC
Name: Center for Inspecting Organized Crimes (CIOC)
Focus: Cyber security & cultural cyber operations
Aliases: -
Mabna Institute [front company]
Focus: CNE operations on academic institutes
Aliases: Cobalt Dickens, Silent Librarian, Yellow Nabu, TA407, TA4900
?
ITSecTeam (ITSEC) [front company]
Focus: CNE operations for IRGC
Aliases: TG-2889, CUTTING KITTEN
?
Mersad Company [front company]
Focus: CNE operations for IRGC
Aliases: FRATERNAL JACKAL, QCF



Sources

- FBI: FBI Releases Cybersecurity Advisory on Previously Undisclosed Iranian Malware Used to Monitor Dissidents and Travel and Telecommunications Companies
- FBI: IRGC-AFFILIATED CYBER ACTORS
- Wikipedia: Ministry of Intelligence (Iran)
- Wikipedia: Supreme Council of Cyberspace (Iran)
- Wikipedia: Iranian Cyber Army
- Wikipedia: Intelligence Organization of the Islamic Revolutionary Guard Corps
- Federal Research Division Library of Congress: Iran's Ministry of Intelligence and Security: A Profile
- Malpedia: APT39
- Malpedia: Fox Kitten
- Flashpoint Intel: A Second Iranian State-Sponsored Ransomware Operation "Project Signal" Emerges
- US Cyber Command: Iranian intel cyber suite of malware uses open source tools
- US Department of Justice: Conspiracy to Commit Computer Hacking – ITSEC Team

- US Department of Justice: Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps
- US Department of Justice: Countering State-Sponsored Cybercrime
- US Department of Justice: Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities
- US Department of Treasury: Treasury Sanctions Iranian Organizations and Individuals Supporting Intelligence and Cyber Targeting of U.S. Persons
- US Congressional Research Service: Iranian Offensive Cyber Attack Capabilities
- US Congressional Research Service: Iran: Internal Politics and U.S. Policy and Options
- Recorded Future: Iran's Hacker Hierarchy Exposed
- Recorded Future: Despite Infighting and Volatility, Iran Maintains Aggressive Cyber Operations Structure
- Cyber Shafarat: Basij Cyber Battalions
- Global Security: IRGC's Guard Cyber Defense Command (GCDC)
- BBC: Structure of Iran's Cyber Warfare
- ThaiCERT: APT group: Mabna Institute, Cobalt Dickens, Silent Librarian
- ThaiCERT: APT group: APT 33, Elfin, Magnallium
- ThaiCERT: APT group: Cutting Kitten, TG-2889
- ThaiCERT: APT group: Chafer, APT 39
- ThaiCERT: Other threat group: Cyber fighters of Izz Ad-Din Al Qassam, Fraternal Jackal
- ThaiCERT: APT group: Domestic Kitten
- ThaiCERT: APT group: OilRig, APT 34, Helix Kitten, Chrysene
- Symantec: Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.
- Dragos: MAGNALLIUM
- FireEye: Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware
- Check Point Research: Domestic Kitten – An Inside Look at the Iranian Surveillance Operations
- King Faisal Center for Research and Islamic Studies: Iran's Cyberattacks Capabilities

ChangeLog

- Version 2.0 (13 Jan 2022): Updated MOIS based on US CYBERCOM statement.
- Version 1.5 (06 May 2021): Fixed a typo. Added missing "Focus" entries.
- Version 1.2 (06 May 2021): Minor fixes (typos, etc.)
- Version 1.0 (06 May 2021): First publication.
