Iran Cyber Operations Groups

xorl.wordpress.com/2021/05/06/iran-cyber-operations-groups/

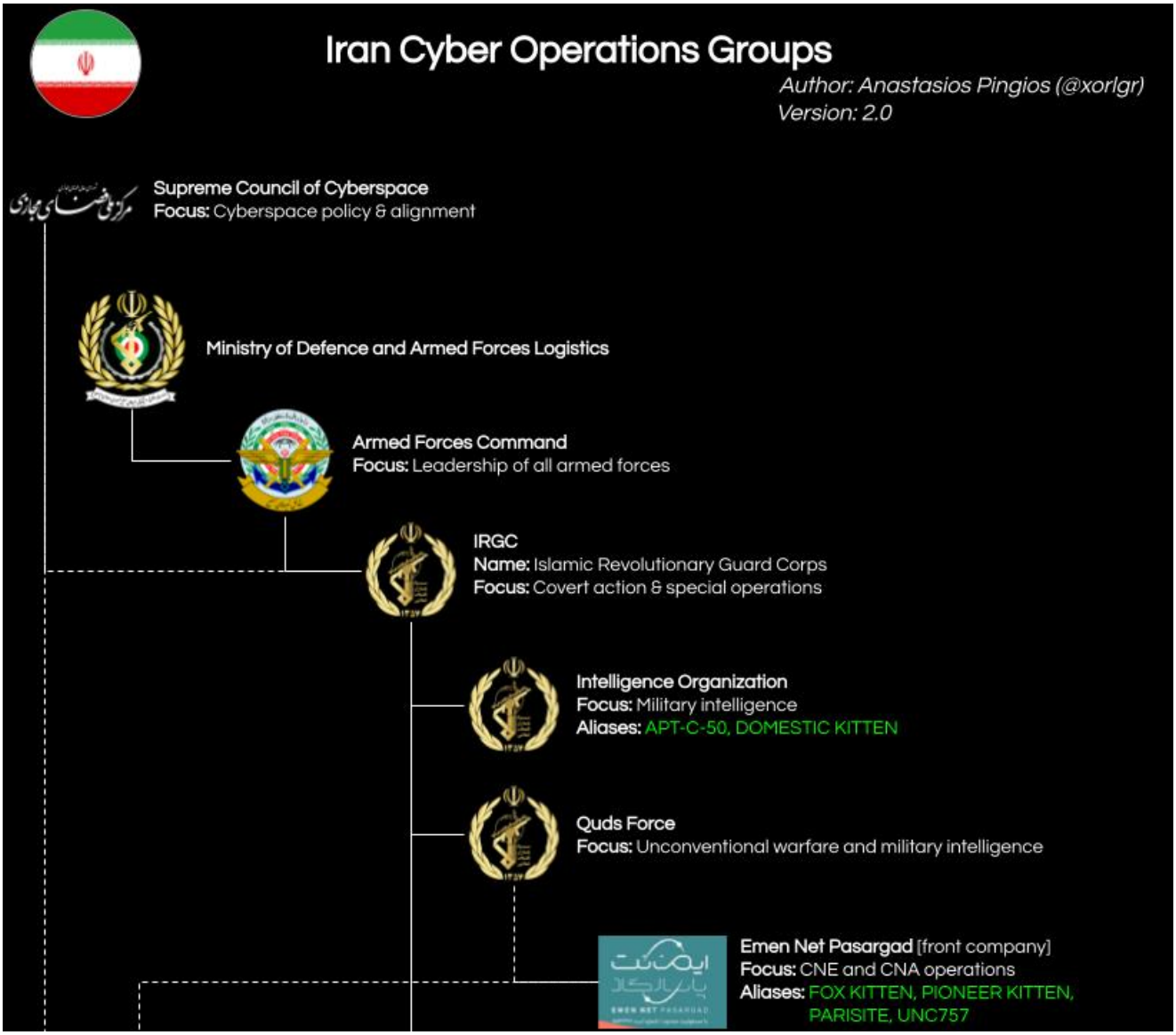
May 6, 2021

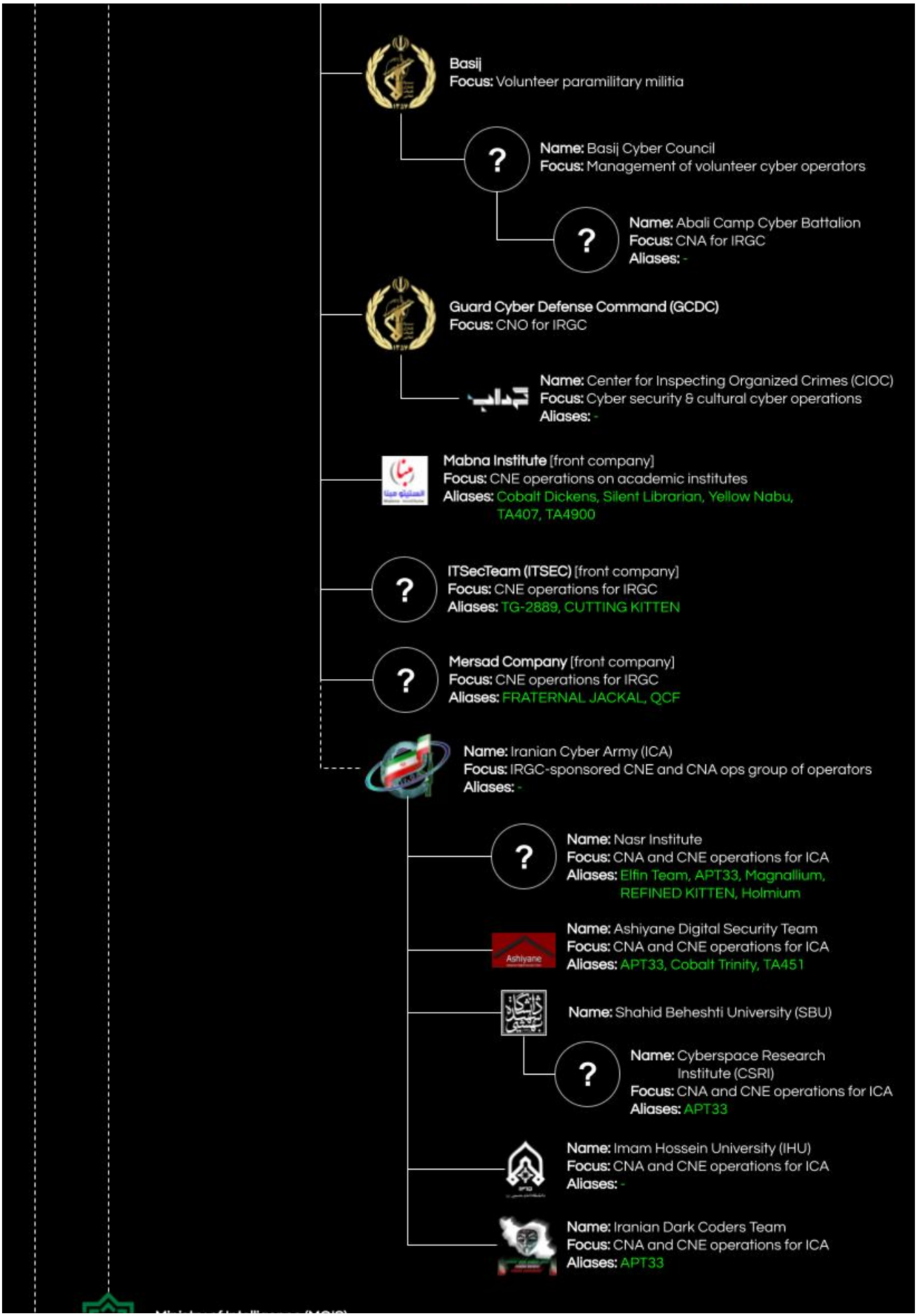
with 2 comments

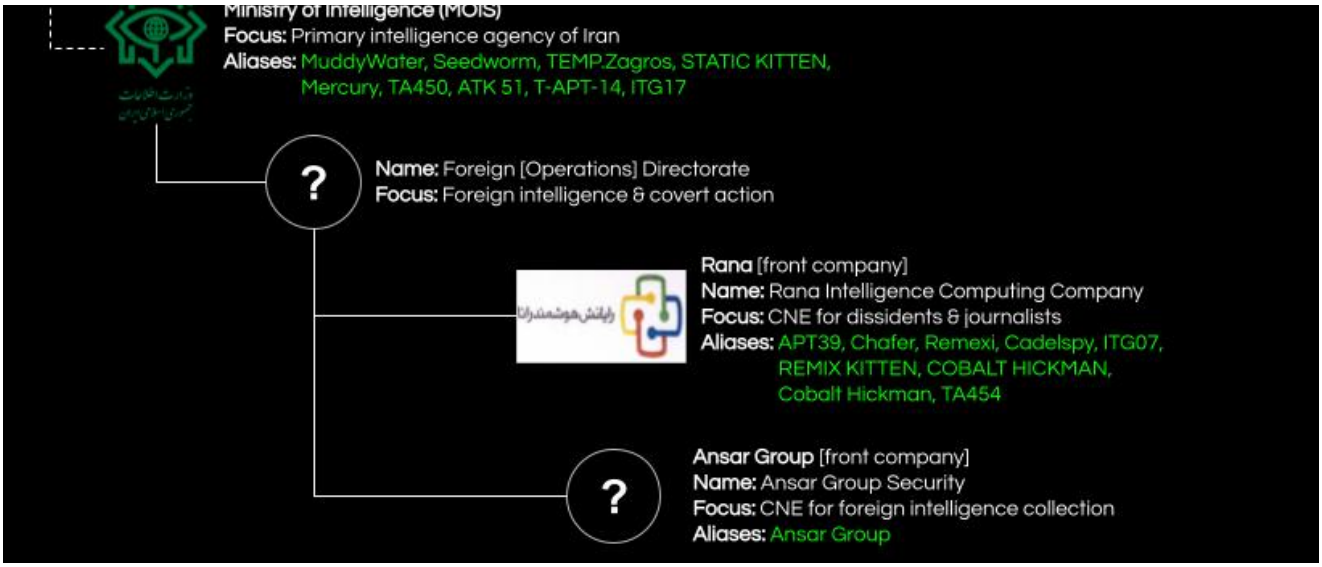
Unsurprisingly, after Russia, US, China, DPRK (North Korea), and EU… Here comes the mapping of the offensive cyber operations groups of Iran that have been attributed to a known government entity. Just like in the previous posts, sources and change log are available under the diagram.

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




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
Name: Iranian Cyber Army (ICA)
Focus: IRGC-sponsored CNE and CNA ops group of operators
Aliases: -
?
Name: Nasr Institute
Focus: CNA and CNE operations for ICA
Aliases: Elfin Team, APT33, Magnallium, REFINED KITTEN, Holmium
Ashiyane
Name: Ashiyane Digital Security Team
Focus: CNA and CNE operations for ICA
Aliases: APT33, Cobalt Trinity, TA451
Name: Shahid Beheshti University (SBU)
?
Name: Cyberspace Research Institute (CSRI)
Focus: CNA and CNE operations for ICA
Aliases: APT33
Name: Imam Hossein University (IHU)
Focus: CNA and CNE operations for ICA
Aliases: -
Name: Iranian Dark Coders Team
Focus: CNA and CNE operations for ICA
Aliases: APT33



Sources

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.

Written by xorl

May 6, 2021 at 13:00

Posted in threat intelligence

2 Responses

Subscribe to comments with RSS.

1. how did you miss israel. its a major player. please do for it.

   jonathan

   May 16, 2021 at 12:34

2. I only know of IDF Unit 8200 doing offensive cyber operations in Israel and being linked with known APT groups.

   I have it in my backlog.

   xorl

   May 17, 2021 at 15:17

Leave a Reply

Fill in your details below or click an icon to log in:

You are commenting using your WordPress.com account. (Log Out / Change)

You are commenting using your Twitter account. (Log Out / Change)


You are commenting using your Facebook account. (Log Out / Change)

Cancel
Connecting to %s