Chinese Cyber Operations Groups

xorl.wordpress.com/2021/04/20/chinese-cyber-operations-groups/

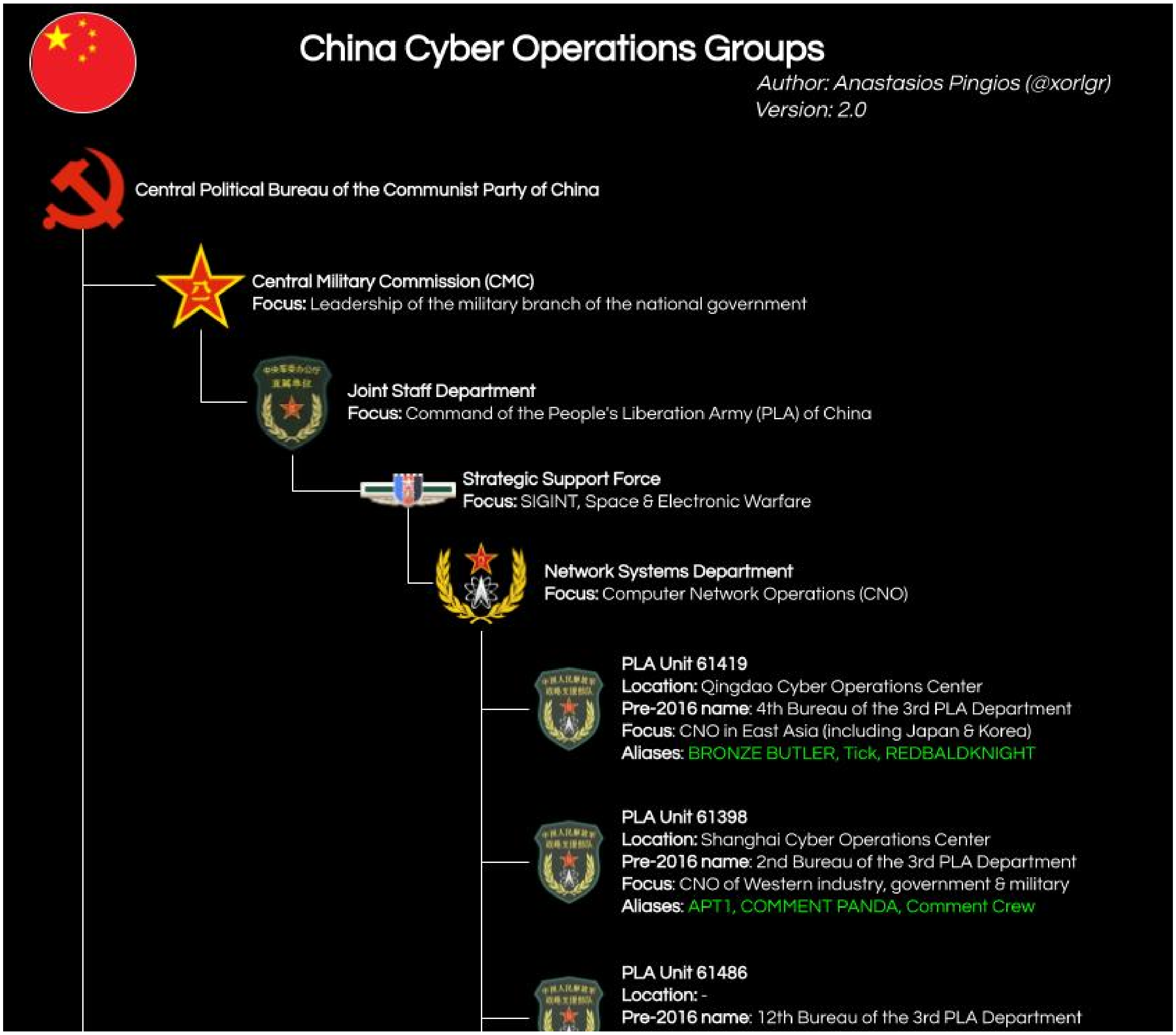
April 20, 2021

leave a comment »

And after the Russian and US ones, here is the one of the publicly known Chinese offensive cyber operations groups and their associations. Just like in the other cases, this will be a live document updated in this page as soon as new information becomes available.

For the same reason, if you notice any mistakes, errors, or missing information please let me know and I will update it as soon as possible. Also, to improve the transparency below the diagram you can find a complete list of the sources used to construct it.

Last Update: 18 June 2021



China Cyber Operations Groups

Author: Anastasios Pingios (@xorlgr)
Version: 2.0

Central Political Bureau of the Communist Party of China

Central Military Commission (CMC)
Focus: Leadership of the military branch of the national government

Joint Staff Department
Focus: Command of the People's Liberation Army (PLA) of China

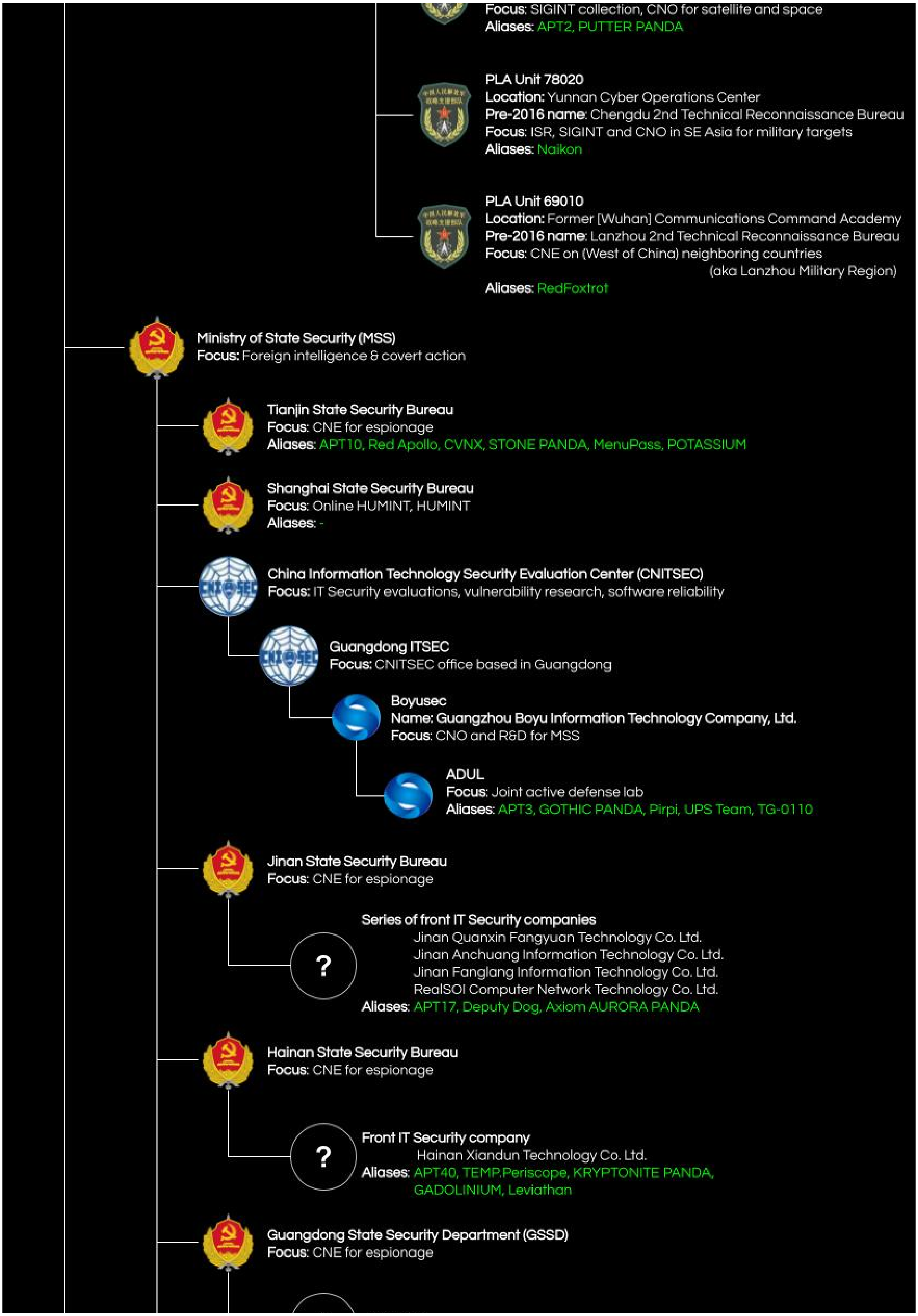
Strategic Support Force
Focus: SIGINT, Space & Electronic Warfare

Network Systems Department
Focus: Computer Network Operations (CNO)

PLA Unit 61419
Location: Qingdao Cyber Operations Center
Pre-2016 name: 4th Bureau of the 3rd PLA Department
Focus: CNO in East Asia (including Japan & Korea)
Aliases: BRONZE BUTLER, Tick, REDBALDKNIGHT

PLA Unit 61398
Location: Shanghai Cyber Operations Center
Pre-2016 name: 2nd Bureau of the 3rd PLA Department
Focus: CNO of Western industry, government & military
Aliases: APT1, COMMENT PANDA, Comment Crew

PLA Unit 61486
Location: -
Pre-2016 name: 12th Bureau of the 3rd PLA Department



Focus: SIGINT collection, CNO for satellite and space
Aliases: APT2, PUTTER PANDA

PLA Unit 78020
Location: Yunnan Cyber Operations Center
Pre-2016 name: Chengdu 2nd Technical Reconnaissance Bureau
Focus: ISR, SIGINT and CNO in SE Asia for military targets
Aliases: Naikon

PLA Unit 69010
Location: Former [Wuhan] Communications Command Academy
Pre-2016 name: Lanzhou 2nd Technical Reconnaissance Bureau
Focus: CNE on (West of China) neighboring countries
(aka Lanzhou Military Region)
Aliases: RedFoxtrot

Ministry of State Security (MSS)
Focus: Foreign intelligence & covert action

Tianjin State Security Bureau
Focus: CNE for espionage
Aliases: APT10, Red Apollo, CVNX, STONE PANDA, MenuPass, POTASSIUM

Shanghai State Security Bureau
Focus: Online HUMINT, HUMINT
Aliases: -

China Information Technology Security Evaluation Center (CNITSEC)
Focus: IT Security evaluations, vulnerability research, software reliability

Guangdong ITSEC
Focus: CNITSEC office based in Guangdong

Boyusec
Name: Guangzhou Boyu Information Technology Company, Ltd.
Focus: CNO and R&D for MSS

ADUL
Focus: Joint active defense lab
Aliases: APT3, GOTHIC PANDA, Pirpi, UPS Team, TG-0110

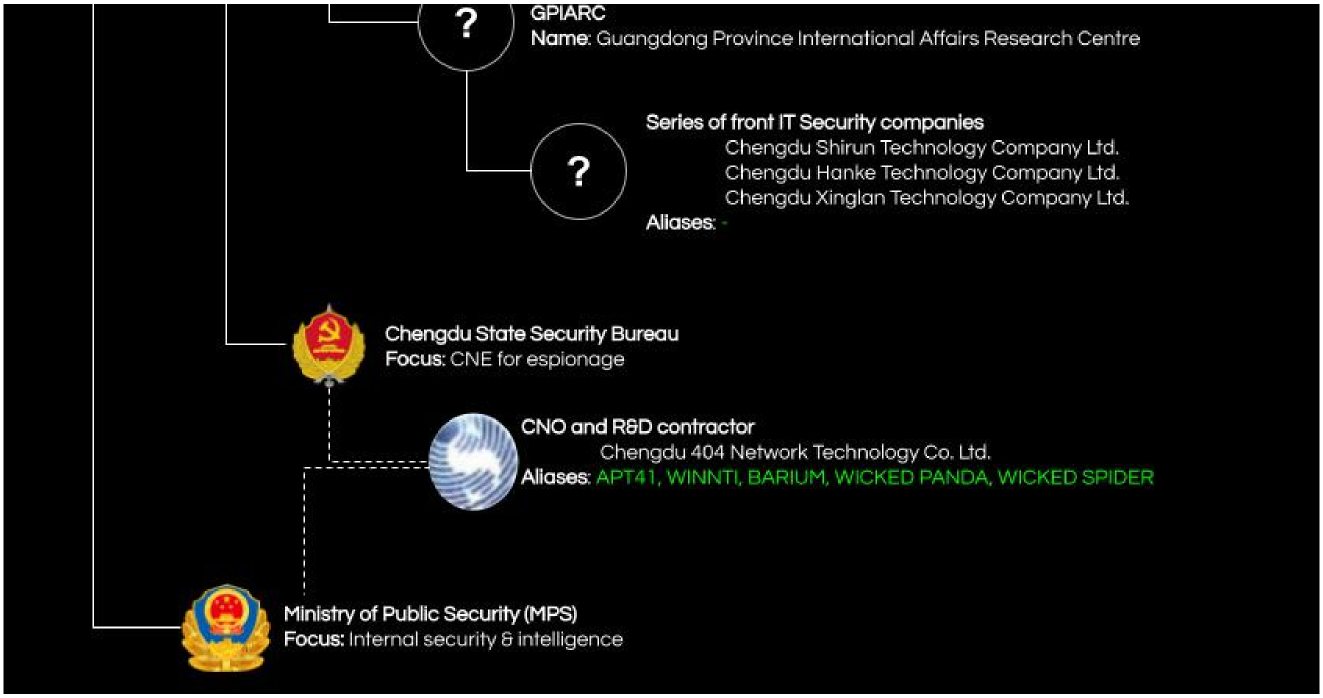
Jinan State Security Bureau
Focus: CNE for espionage

Series of front IT Security companies
Jinan Quanxin Fangyuan Technology Co. Ltd.
Jinan Anchuang Information Technology Co. Ltd.
Jinan Fanglang Information Technology Co. Ltd.
RealSOI Computer Network Technology Co. Ltd.
Aliases: APT17, Deputy Dog, Axiom AURORA PANDA

Hainan State Security Bureau
Focus: CNE for espionage

Front IT Security company
Hainan Xiandun Technology Co. Ltd.
Aliases: APT40, TEMP.Periscope, KRYPTONITE PANDA, GADOLINIUM, Leviathan

Guangdong State Security Department (GSSD)
Focus: CNE for espionage


?
GPIARC
Name: Guangdong Province International Affairs Research Centre
?
Series of front IT Security companies
Chengdu Shirun Technology Company Ltd.
Chengdu Hanke Technology Company Ltd.
Chengdu Xinglan Technology Company Ltd.
Aliases: -
Chengdu State Security Bureau
Focus: CNE for espionage
CNO and R&D contractor
Chengdu 404 Network Technology Co. Ltd.
Aliases: APT41, WINNTI, BARIUM, WICKED PANDA, WICKED SPIDER
Ministry of Public Security (MPS)
Focus: Internal security & intelligence

Sources

ChangeLog

- Version 2.0 (18 June 2021): Added PLA 69010 (thanks to @monacasec for the heads up)
- Version 1.6 (13 May 2021): Removed China Chopper as it's not an actor (credits: @r0ny_123)
- Version 1.5 (13 May 2021): Added GSSD and relevant entities.
- Version 1.0 (20 April 2021): First publication.

Written by xorl

April 20, 2021 at 22:05

Posted in threat intelligence

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