black hat®
ASIA 2024

APRIL 18-19, 2024
BRIEFINGS

China's Military Cyber Operations

Has the Strategic Support Force Come of Age?

Pukhraj Singh

Disclaimer

The views expressed in this presentation are strictly personal, and not of my employer’s

Before we proceed…

- When I say “*China*” or “*Chinese*”, it implies the state and organs of the *People’s Republic of China (PRC)*, established by the *Communist Party of China (CCP)*
    - It carries no judgement on the rich and fascinating Chinese history, culture and society

BLUF – Bottom line up front - I

- Grand summary: Recent PRC's cyber operations have all the hallmarks of a military mobilisation (Operational Preparation of the Environment)

- Grand objective: To secure the PRC's geo-economic interests in its near-abroad

- **The strategic shift**
  - Strategic information warfare as an enabler for air and sea control in the South China Sea (and Taiwan Strait)
  - Readjust the balance of power in the region by disrupting the US's logistics, naval power projection and Freedom of Navigation

- **The military cyber operations architecture**
  - Mobilisation of wartime constructs like the Information Operations Group (IOG) to rope in civilian authorities/threat actors

BLUF – Bottom line up front - II

- **The tactical and infrastructural overlaps in threat activity clusters**
  - The absorption of ‘authorised forces’ into the wartime IOG
- **The command-and-control**
  - Strategic information/cyber operations directly authorised by the Central Military Commission
- **The politico-military objectives**
  - Information/cyber operations as ‘first strike’, followed by electronic warfare and kinetic operations to disrupt the adversary’s system-of-systems
  - The degradation of will to resist and deterrent effects

Agenda

- Part I: Recent prepositioning operations: Volt Typhoon and RedEcho
- Part II: The People’s Liberation Army’s (PLA) Strategic Support Force (SSF)
- Part III: The CCP’s information warfare command-and-control (C2)
- Part IV: The PLA’s Military-Civil Fusion
- Part V: Summing it all: First strike and vital point (cyber) targets
- Part VI: The geopolitics of the Indo-Pacific

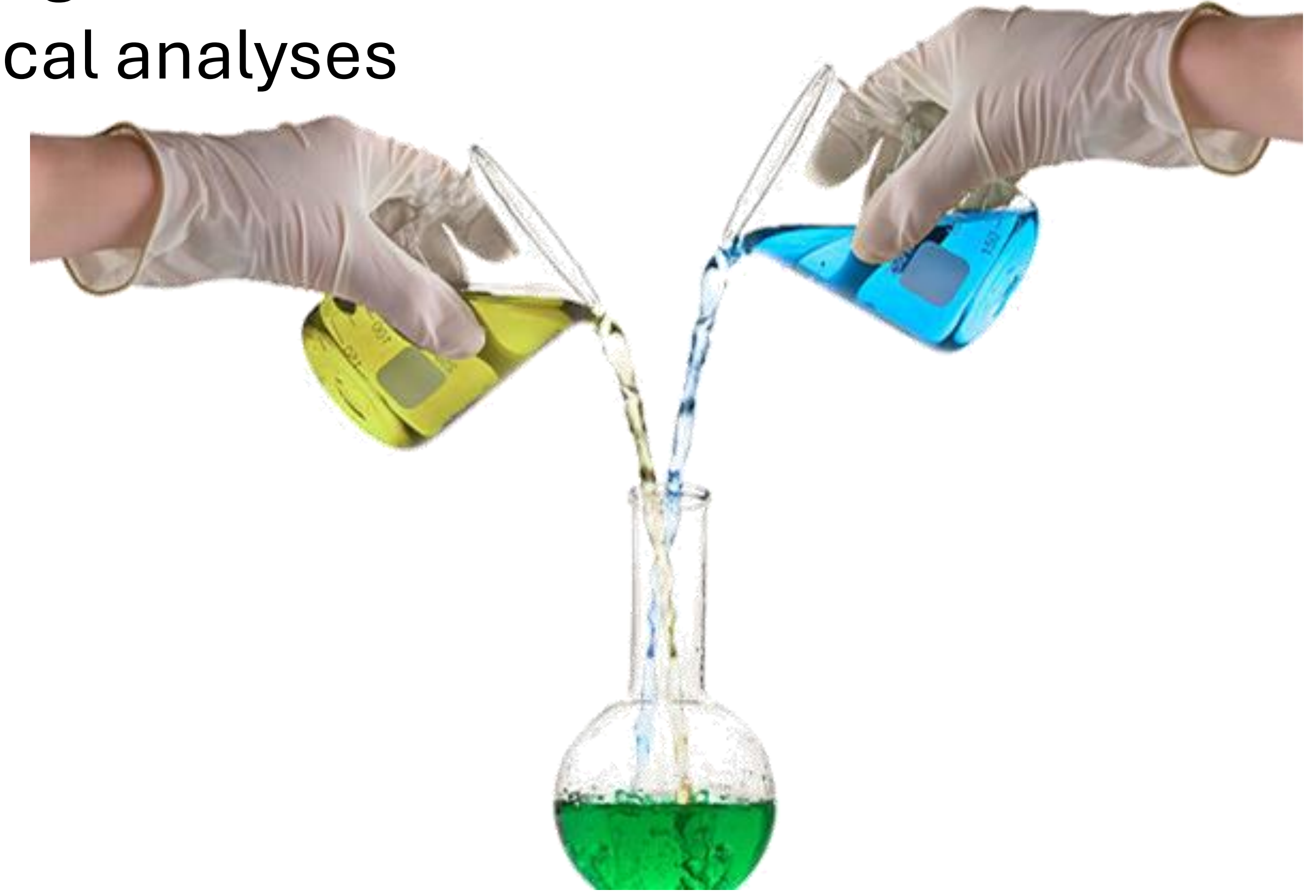
Introduction

- Blue teamer in the day, geopolitical analyst at night
- Background in malware analysis
- Computer science engineer with a master’s in cyber geostrategy from the Australian Defence Force Academy
- Published by the US Military Academy, US Army (pre-print), Australian Defence College, Australian Strategic Policy Institute and Indian Army

My approach

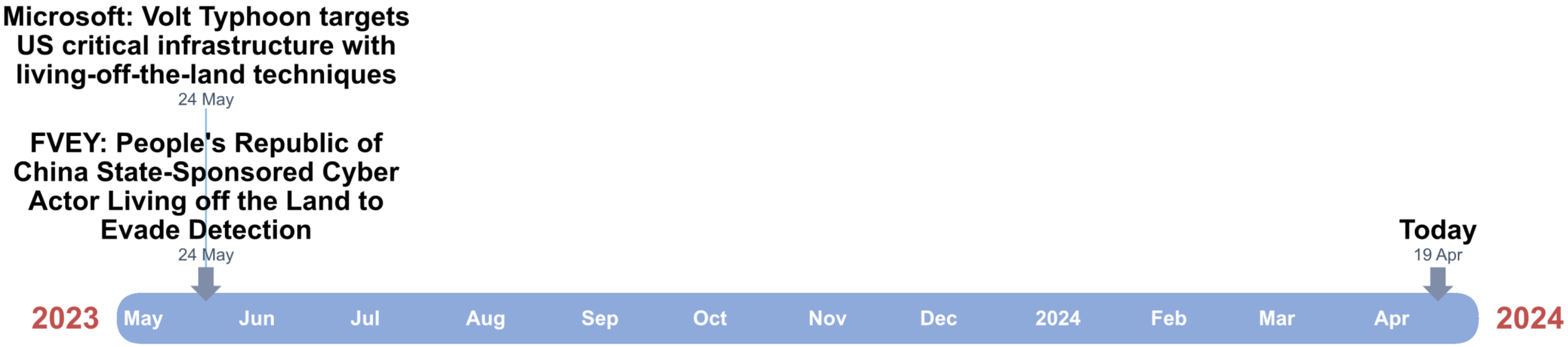
Geostrategic and geopolitical analyses

Malware analysis



Volt Typhoon

May'23: Five Eyes and Microsoft

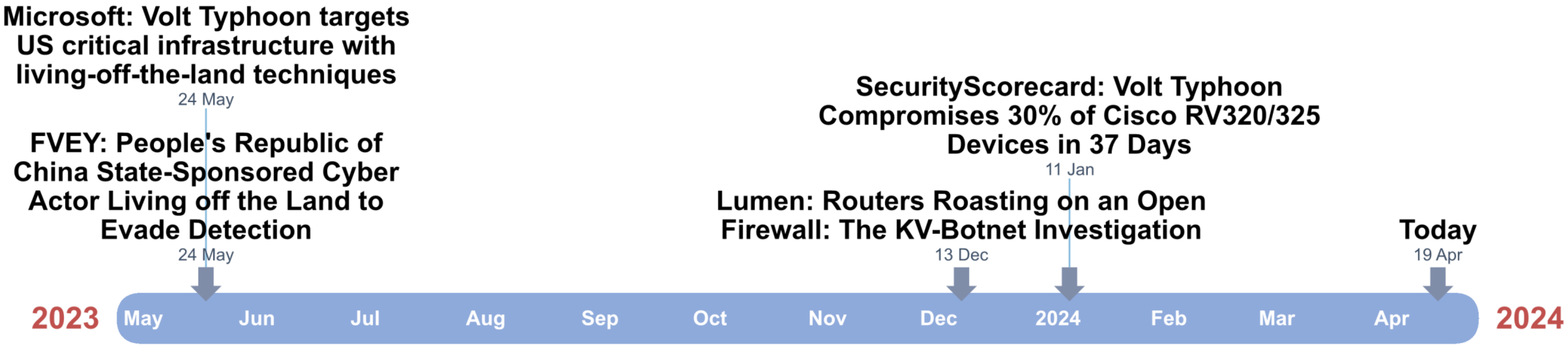


Microsoft: Volt Typhoon targets US critical infrastructure with living-off-the-land techniques
24 May

FVEY: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection
24 May

Today
19 Apr

Dec’23-Jan’24: Lumen and SecurityScorecard



Microsoft: Volt Typhoon targets US critical infrastructure with living-off-the-land techniques
24 May

FVEY: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection
24 May

Lumen: Routers Roasting on an Open Firewall: The KV-Botnet Investigation
13 Dec

SecurityScorecard: Volt Typhoon Compromises 30% of Cisco RV320/325 Devices in 37 Days
11 Jan

Today
19 Apr

Jan’24 – Now : More disclosures

Microsoft: Volt Typhoon targets US critical infrastructure with living-off-the-land techniques
24 May

FVEY: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection
24 May

Lumen: Routers Roasting on an Open Firewall: The KV-Botnet Investigation
13 Dec

SecurityScorecard: Volt Typhoon Compromises 30% of Cisco RV320/325 Devices in 37 Days
11 Jan

US DoJ: U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure
31 Jan

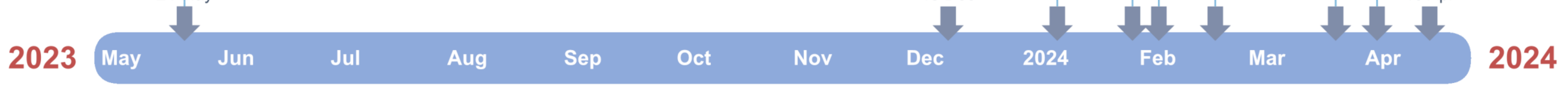
FVEY: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure
7 Feb

Dragos: VOLTZITE Threat Group’s Under the Radar Cyber Espionage on U.S. Critical Systems
22 Feb

Treasury & DoJ: Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure
25 Mar

Mandiant: Cutting Edge, Part 4: Ivanti Connect Secure VPN Post-Exploitation Lateral Movement Case Studies
5 Apr

Today
19 Apr

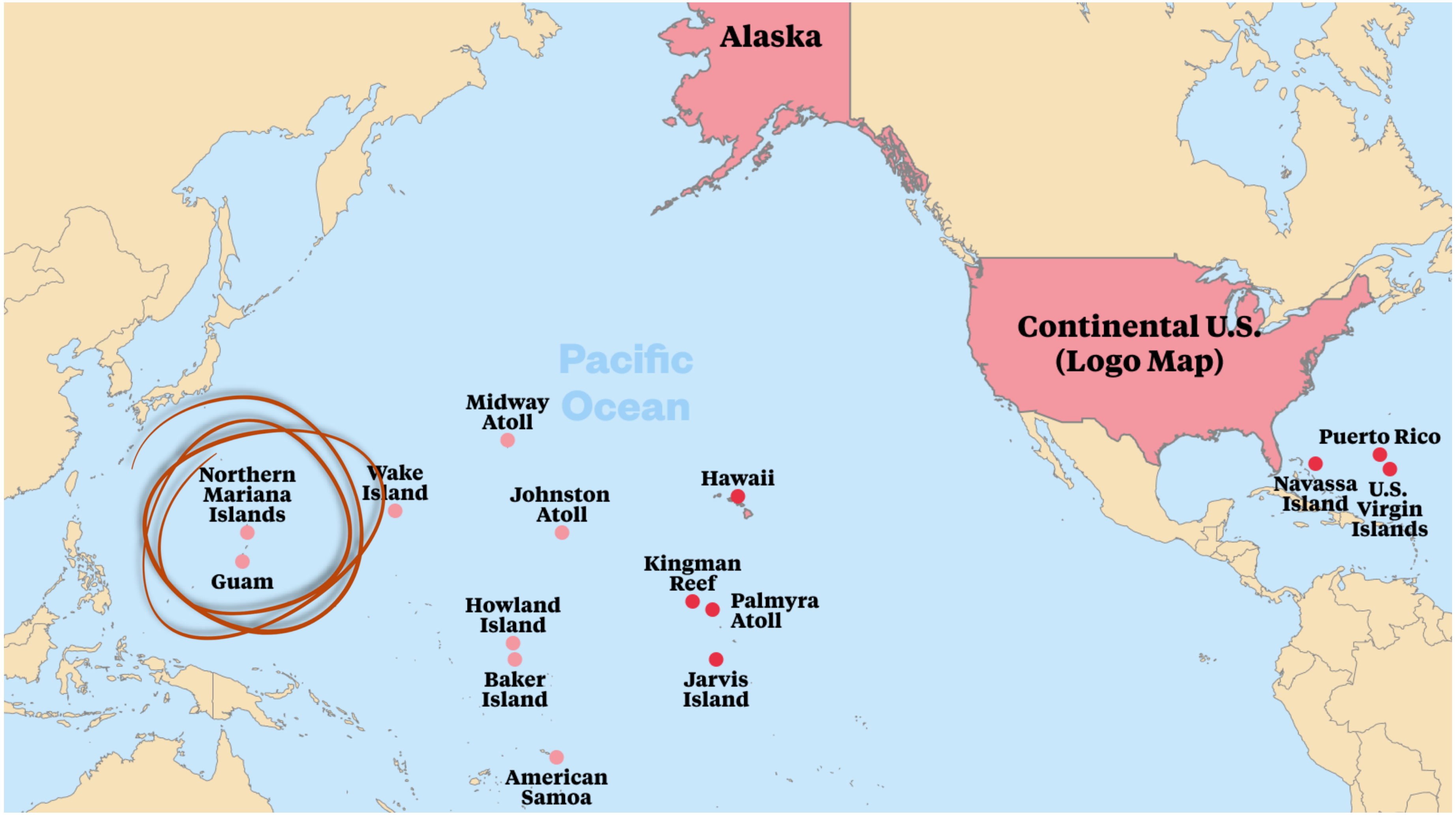


black hat ASIA 2024

Volt Typhoon - Notables

- Target geographies: Continental and non-continental US (Guam), Asia-Pacific and Africa
- Targets: Transportation, water and wastewater, electric utilities, power transmission and distribution, satellite networks, telecommunications, emergency management, defence industrial bases and geographical information systems
- Potential infrastructural and tactical overlaps with Kostovite (Dragos), APT31, Mirai botnet and UTA0178 (2024 Ivanti 0day)
- Unremarkable but effective TTPs: extensive pre-compromise recon, hands-on keyboard activity and living-of-the-land
- Active since at least five years

Guam: The US’s last military outpost in the Pacific

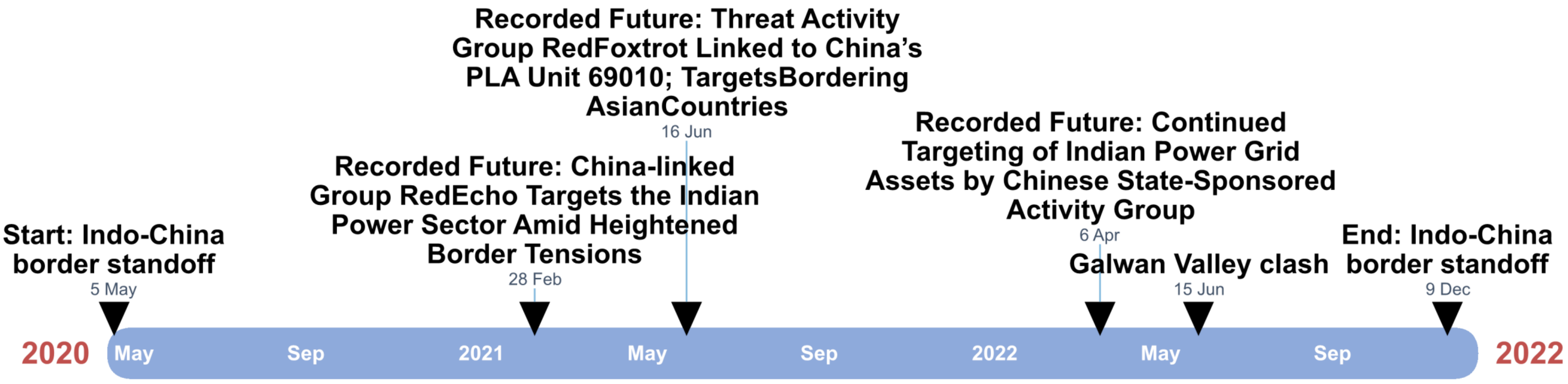


Source: thechinaproject.com

The South Asia military activity cluster:

RedEcho, RedFoxtrot, TAG-38 and TAG-26

2021-22: RedEcho and RedFoxtrot



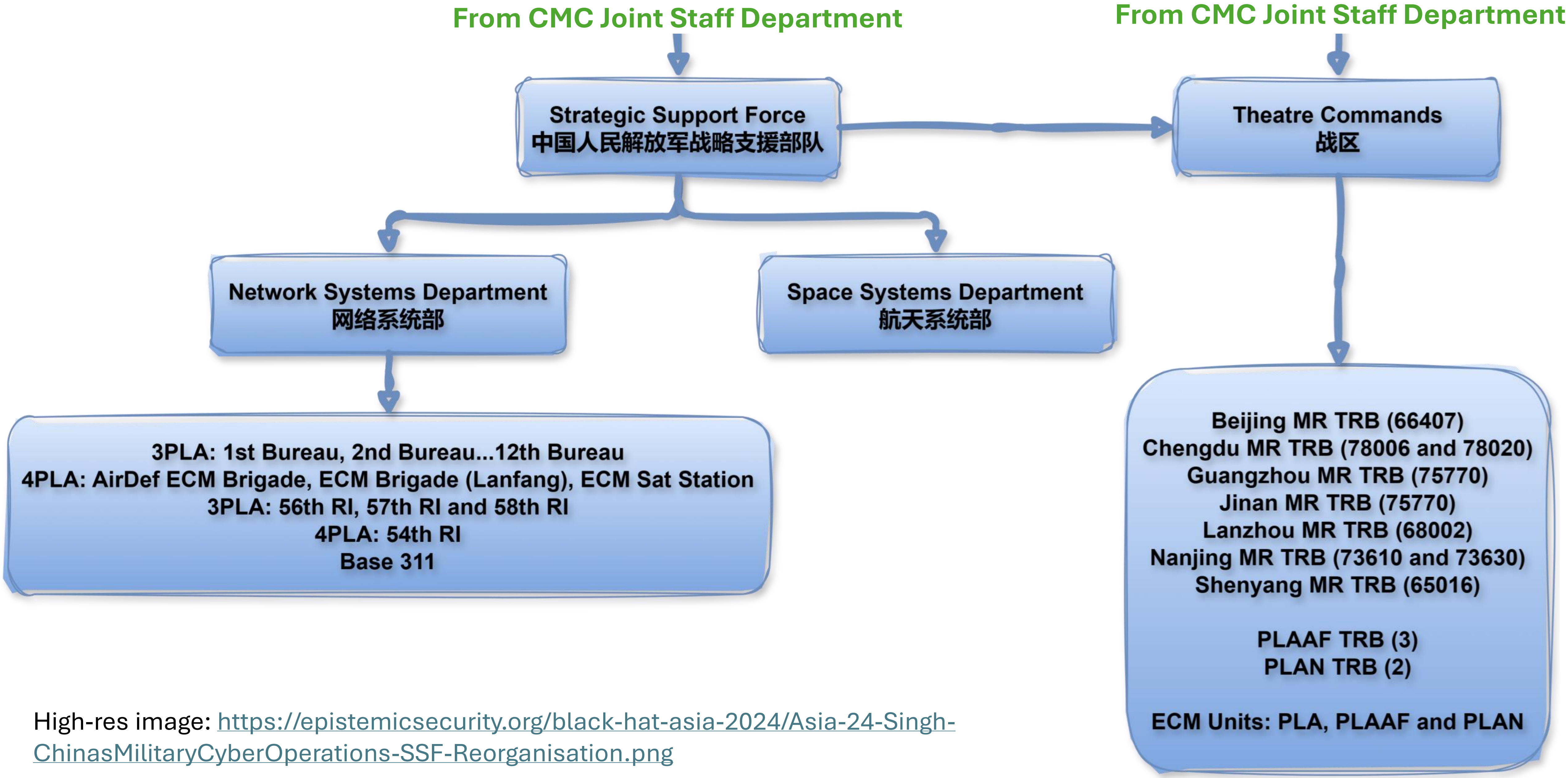
RedEcho and RedFoxtrot - Notables

- Infrastructural overlap with APT41 and Tonto Team; and tactical overlap with APT31

- Matches Volt Typhoon’s targeting criteria: Regional/State Load Despatch Centres, high-voltage transmission substation, thermal power plant, seaports, multinational logistics company, national emergency response system, and an MSP providing OT services to British utilities

- Some tactical similarities with Volt Typhoon: The use of compromised edge/IoT devices like IP cameras for C2; the use of Fast Reverse Proxy

The Strategic Support Force (PLASSF/SSF)



From CMC Joint Staff Department

Strategic Support Force
中国人民解放军战略支援部队

Network Systems Department
网络系统部

3PLA: 1st Bureau, 2nd Bureau...12th Bureau
4PLA: AirDef ECM Brigade, ECM Brigade (Lanfang), ECM Sat Station
3PLA: 56th RI, 57th RI and 58th RI
4PLA: 54th RI
Base 311

Space Systems Department
航天系统部

From CMC Joint Staff Department

Theatre Commands
战区

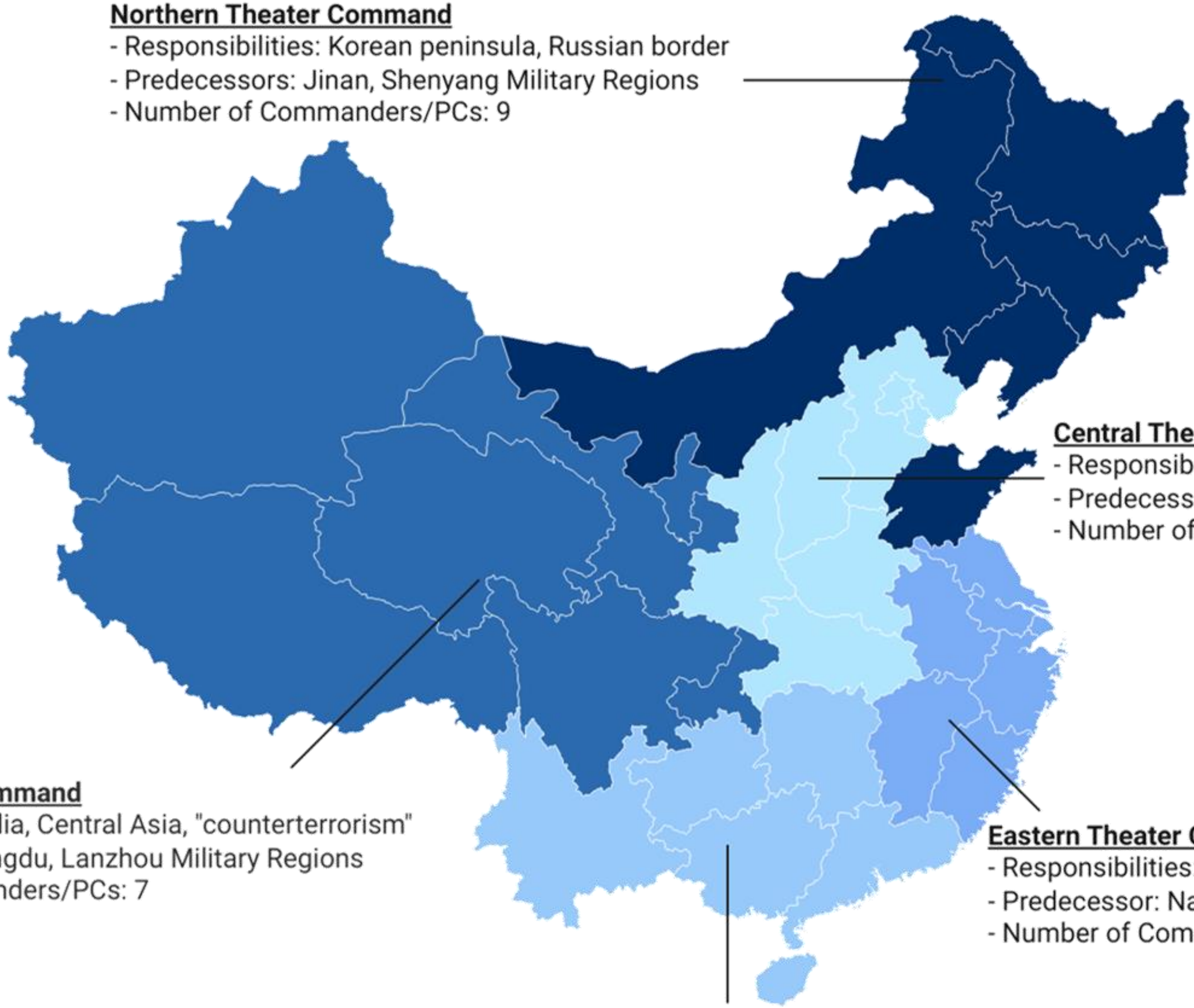
Beijing MR TRB (66407)
Chengdu MR TRB (78006 and 78020)
Guangzhou MR TRB (75770)
Jinan MR TRB (75770)
Lanzhou MR TRB (68002)
Nanjing MR TRB (73610 and 73630)
Shenyang MR TRB (65016)

PLAAF TRB (3)
PLAN TRB (2)

ECM Units: PLA, PLAAF and PLAN

High-res image: https://epistemicsecurity.org/black-hat-asia-2024/Asia-24-Singh-ChinasMilitaryCyberOperations-SSF-Reorganisation.png

The Theatre Commands



Northern Theater Command
- Responsibilities: Korean peninsula, Russian border
- Predecessors: Jinan, Shenyang Military Regions
- Number of Commanders/PCs: 9

Central Theater Command
- Responsibilities: Capital defense
- Predecessor: Beijing Military Region
- Number of Commanders/PCs: 1

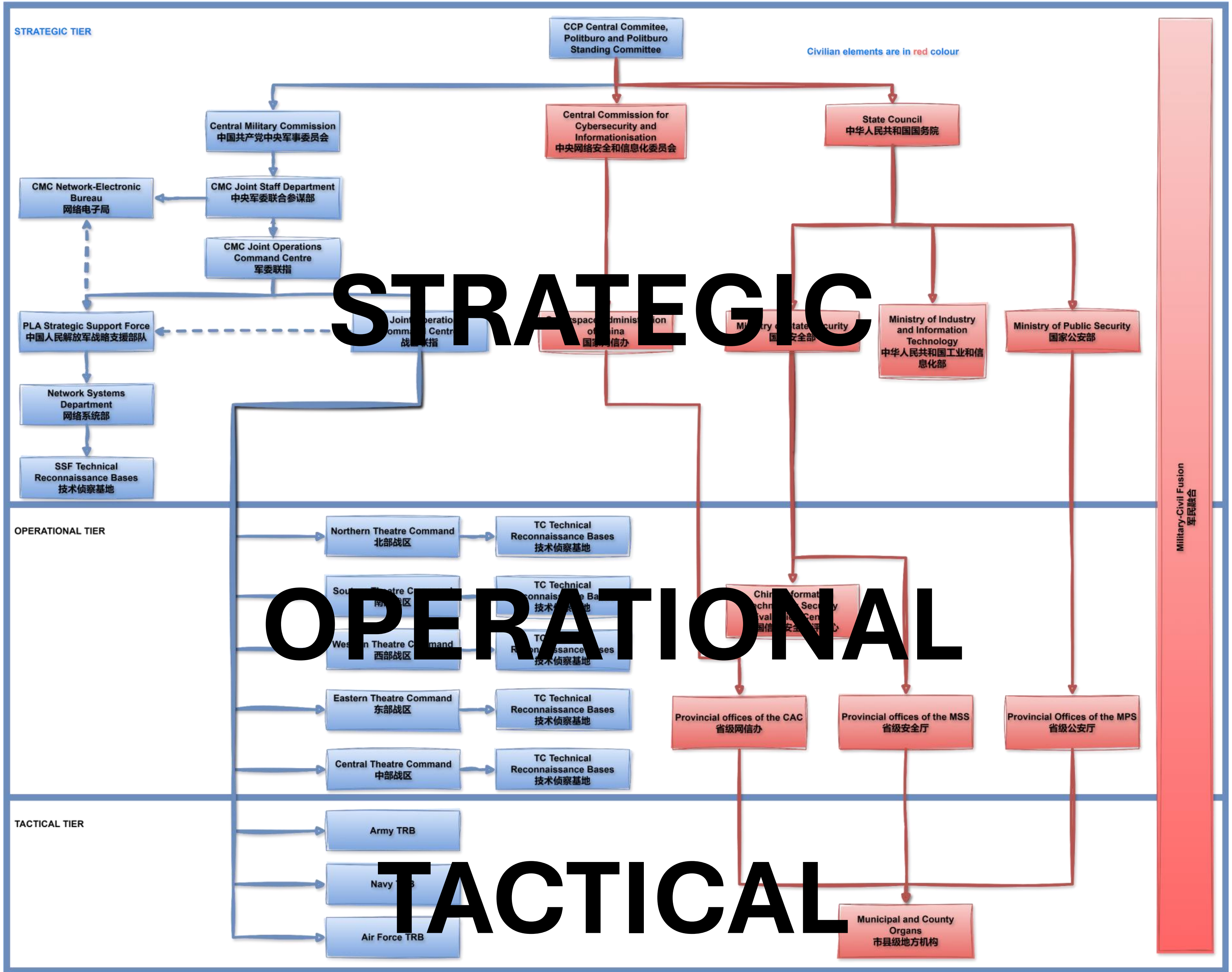
Western Theater Command
- Responsibilities: India, Central Asia, "counterterrorism"
- Predecessors: Chengdu, Lanzhou Military Regions
- Number of Commanders/PCs: 7

Eastern Theater Command
- Responsibilities: Taiwan, East China Sea
- Predecessor: Nanjing Military Region
- Number of Commanders/PCs: 3

Southern Theater Command
- Responsibilities: South China Sea, border defense
- Predecessor: Guangzhou Military Region
- Number of Commanders/PCs: 2

Source: chinapower.csis.org

The CCP’s information warfare command-and-control



STRATEGIC TIER

CCP Central Commitee, Politburo and Politburo Standing Committee

Civilian elements are in red colour

Central Military Commission 中国共产党中央军事委员会

Central Commission for Cybersecurity and Informationisation 中央网络安全和信息化委员会

State Council 中华人民共和国国务院

CMC Network-Electronic Bureau 网络电子局

CMC Joint Staff Department 中央军委联合参谋部

CMC Joint Operations Command Centre 军委联指

PLA Strategic Support Force 中国人民解放军战略支援部队

Joint Operations Command Centre 战区联指

Cyberspace Administration of China 国家网信办

Ministry of State Security 国家安全部

Ministry of Industry and Information Technology 中华人民共和国工业和信息化部

Ministry of Public Security 国家公安部

Network Systems Department 网络系统部

SSF Technical Reconnaissance Bases 技术侦察基地

Military-Civil Fusion 军民融合

OPERATIONAL TIER

Northern Theatre Command 北部战区

TC Technical Reconnaissance Bases 技术侦察基地

Southern Theatre Command 南部战区

TC Technical Reconnaissance Bases 技术侦察基地

Western Theatre Command 西部战区

TC Technical Reconnaissance Bases 技术侦察基地

Eastern Theatre Command 东部战区

TC Technical Reconnaissance Bases 技术侦察基地

Central Theatre Command 中部战区

TC Technical Reconnaissance Bases 技术侦察基地

China Information Technology Security Evaluation Center 中国信息安全测评中心

Provincial offices of the CAC 省级网信办

Provincial offices of the MSS 省级安全厅

Provincial Offices of the MPS 省级公安厅

TACTICAL TIER

Army TRB

Navy TRB

Air Force TRB

Municipal and County Organs 市县级地方机构

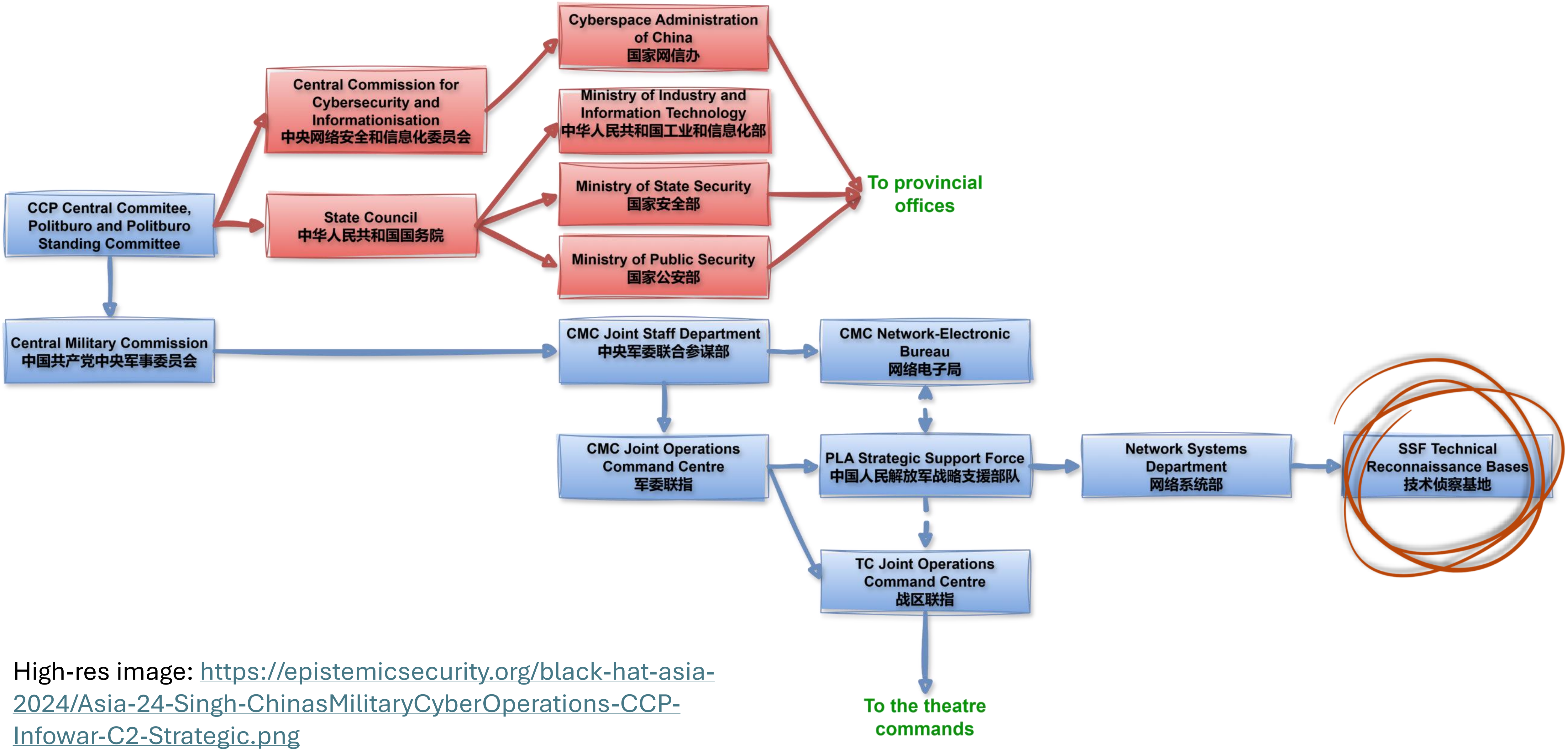
STRATEGIC

OPERATIONAL

TACTICAL

High-res image: https://epistemicsecurity.org/black-hat-asia-2024/Asia-24-Singh-ChinasMilitaryCyberOperations-CCP-Infowar-C2-Overall.png

The CCP’s infowar C2: The strategic tier

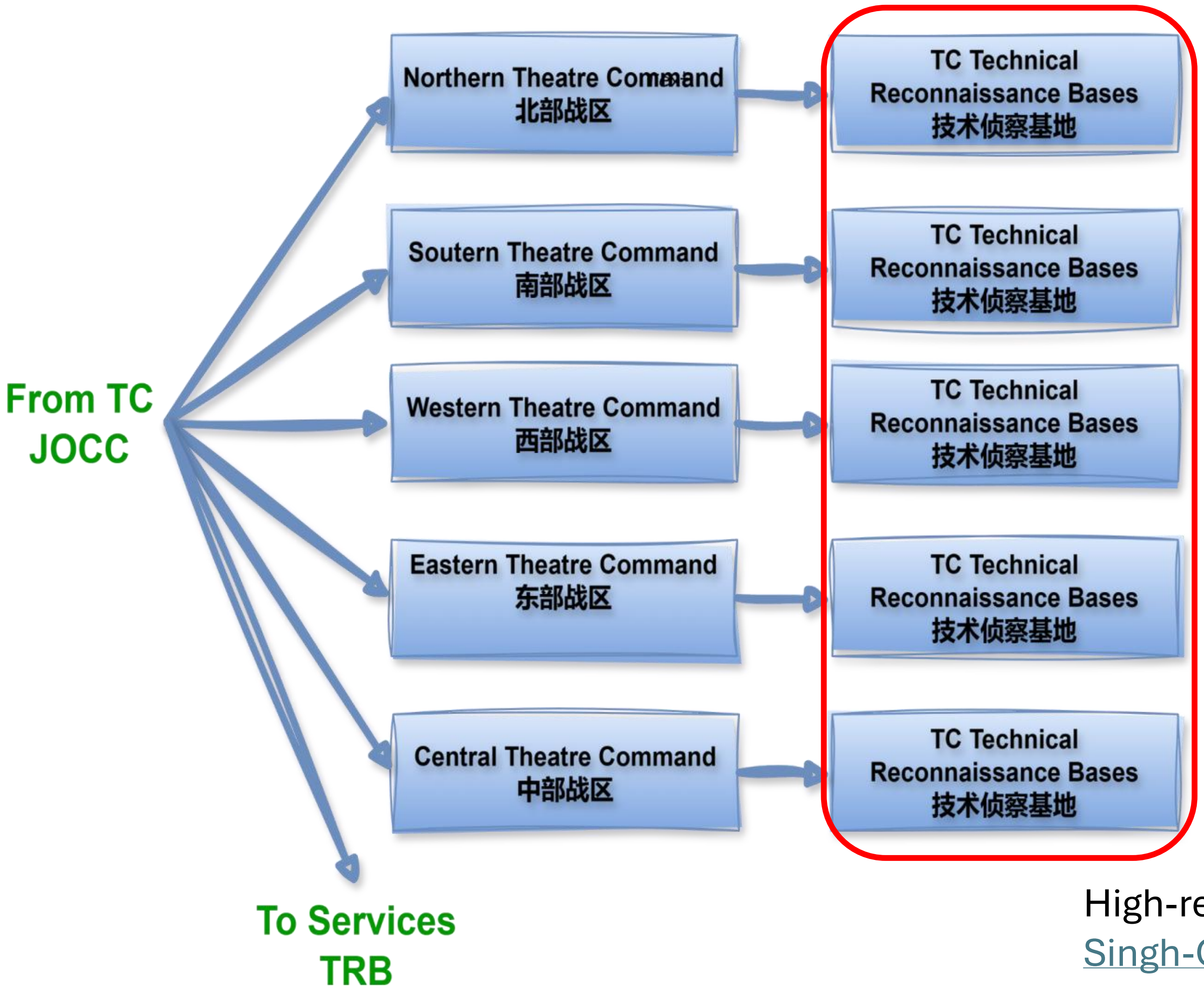

Cyberspace Administration of China
国家网信办
Central Commission for Cybersecurity and Informationisation
中央网络安全和信息化委员会
Ministry of Industry and Information Technology
中华人民共和国工业和信息化部
CCP Central Commitee, Politburo and Politburo Standing Committee
State Council
中华人民共和国国务院
Ministry of State Security
国家安全部
To provincial offices
Ministry of Public Security
国家公安部
Central Military Commission
中国共产党中央军事委员会
CMC Joint Staff Department
中央军委联合参谋部
CMC Network-Electronic Bureau
网络电子局
CMC Joint Operations Command Centre
军委联指
PLA Strategic Support Force
中国人民解放军战略支援部队
Network Systems Department
网络系统部
SSF Technical Reconnaissance Bases
技术侦察基地
TC Joint Operations Command Centre
战区联指
To the theatre commands

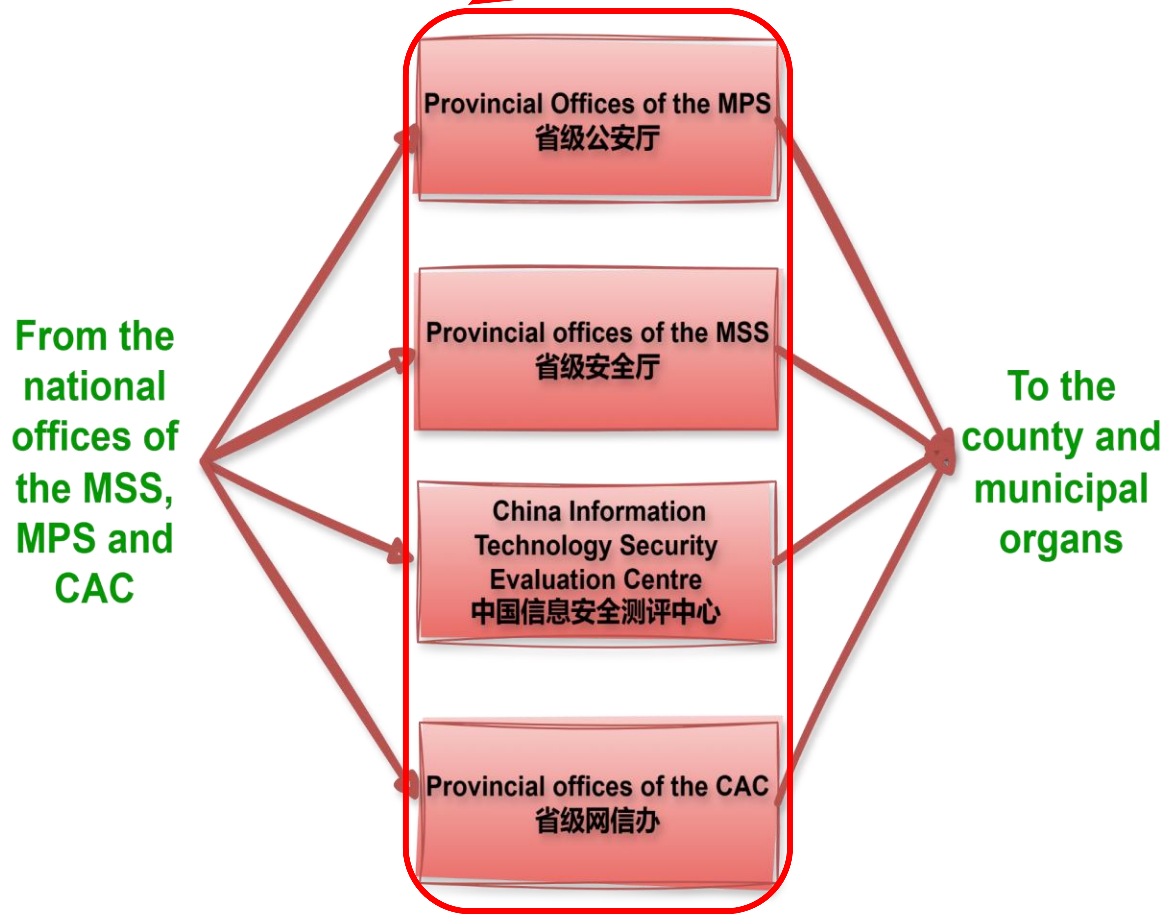
High-res image: https://epistemicsecurity.org/black-hat-asia-2024/Asia-24-Singh-ChinasMilitaryCyberOperations-CCP-Infowar-C2-Strategic.png

The CCP’s infowar C2: The operational tier

- Tonto Team (Northern TC)
- Tick (Northern TC)
- BlackTech (Eastern TC)
- Naikon (Southern TC)
- RedFoxtrot (Western TC)

- APT10 (Tianjin SSB)
- APT27 (Shanghai)
- APT31 (Hubei)
- APT40 (Hainan)
- Earth Lusca (Sichuan)
- APT41 (Sichuan)




From the national offices of the MSS, MPS and CAC
Provincial Offices of the MPS
省级公安厅
Provincial offices of the MSS
省级安全厅
China Information Technology Security Evaluation Centre
中国信息安全测评中心
Provincial offices of the CAC
省级网信办
To the county and municipal organs

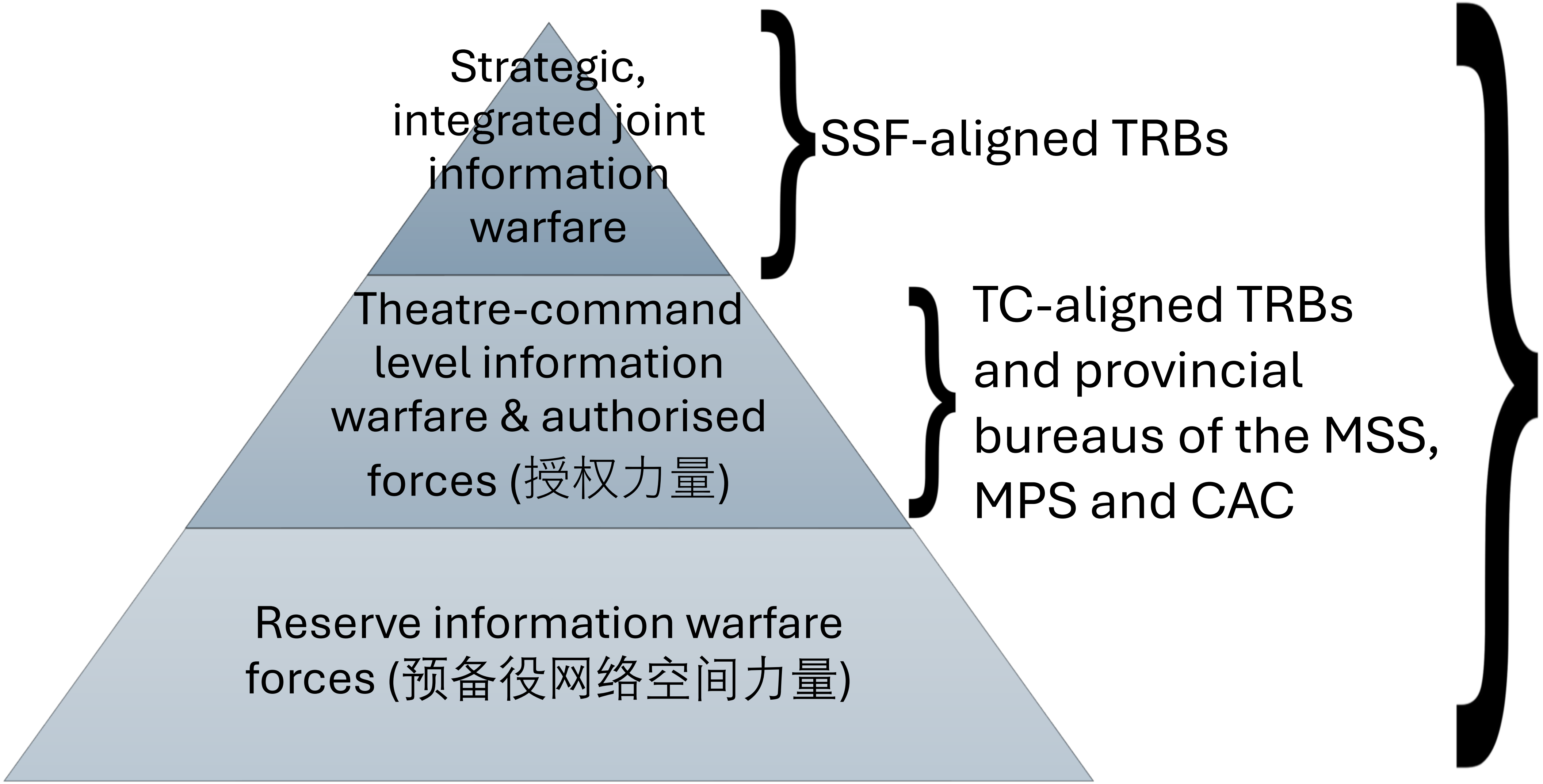
High-res image: https://epistemicsecurity.org/black-hat-asia-2024/Asia-24-Singh-ChinasMilitaryCyberOperations-CCP-Infowar-C2-Operational.png

Military-Civil Fusion (军民融合)

"PLA cyber operators outnumber those of U.S. Cyber Command's Cyber Mission Force by a factor of nearly ten to one"

-- Jacquelyn Schneider in her testimony to the US-China Economic and Security Review Commission

Military-Civil Fusion - Organisation



Strategic, integrated joint information warfare
Theatre-command level information warfare & authorised forces (授权力量)
Reserve information warfare forces (预备役网络空间力量)
SSF-aligned TRBs
TC-aligned TRBs and provincial bureaus of the MSS, MPS and CAC
Wartime information operations groups (信息作战群)

Military Struggle (军事斗争) in cyberspace

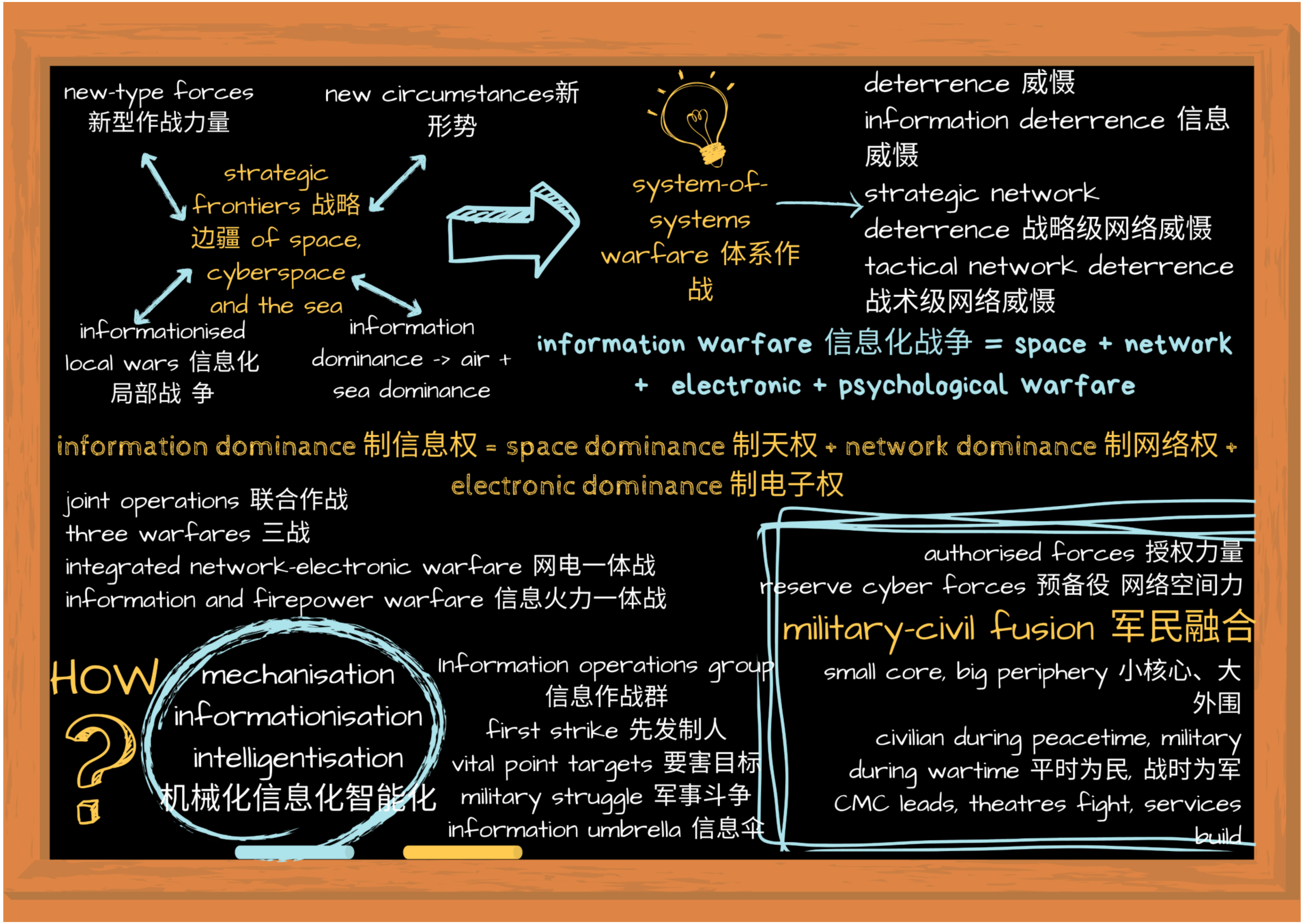
Military-Civil Fusion – Guiding principles

- “Small core, big periphery” (小核心、大外围)
- “Civilian during peacetime, military during wartime” (平时 为民, 战时为军)
- “CMC leads, theatres fight, and services build”

The digital quartermasters - Examples

- Not only tool-based overlaps, but also infrastructural or operational overlaps
  - ShadowPad: Moonlighting contractors and the pecking order
  - APT31: Anonymised C2 and opportunistic targeting
  - Exploit supply chains: 2021 ProxyLogon mass-exploitation and many edge device vulnerabilities

The PLA’s doctrinal constructs for infowar



new-type forces
新型作战力量

new circumstances新
形势

strategic
frontiers 战略
边疆 of space,
cyberspace
and the sea

informationised
local wars 信息化
局部战 争

information
dominance -> air +
sea dominance

system-of-
systems
warfare 体系作
战

deterrence 威慑
information deterrence 信息
威慑
strategic network
deterrence 战略级网络威慑
tactical network deterrence
战术级网络威慑

information warfare 信息化战争 = space + network
+ electronic + psychological warfare

information dominance 制信息权 = space dominance 制天权 + network dominance 制网络权 +
electronic dominance 制电子权

joint operations 联合作战
three warfares 三战
integrated network-electronic warfare 网电一体战
information and firepower warfare 信息火力一体战

HOW
?

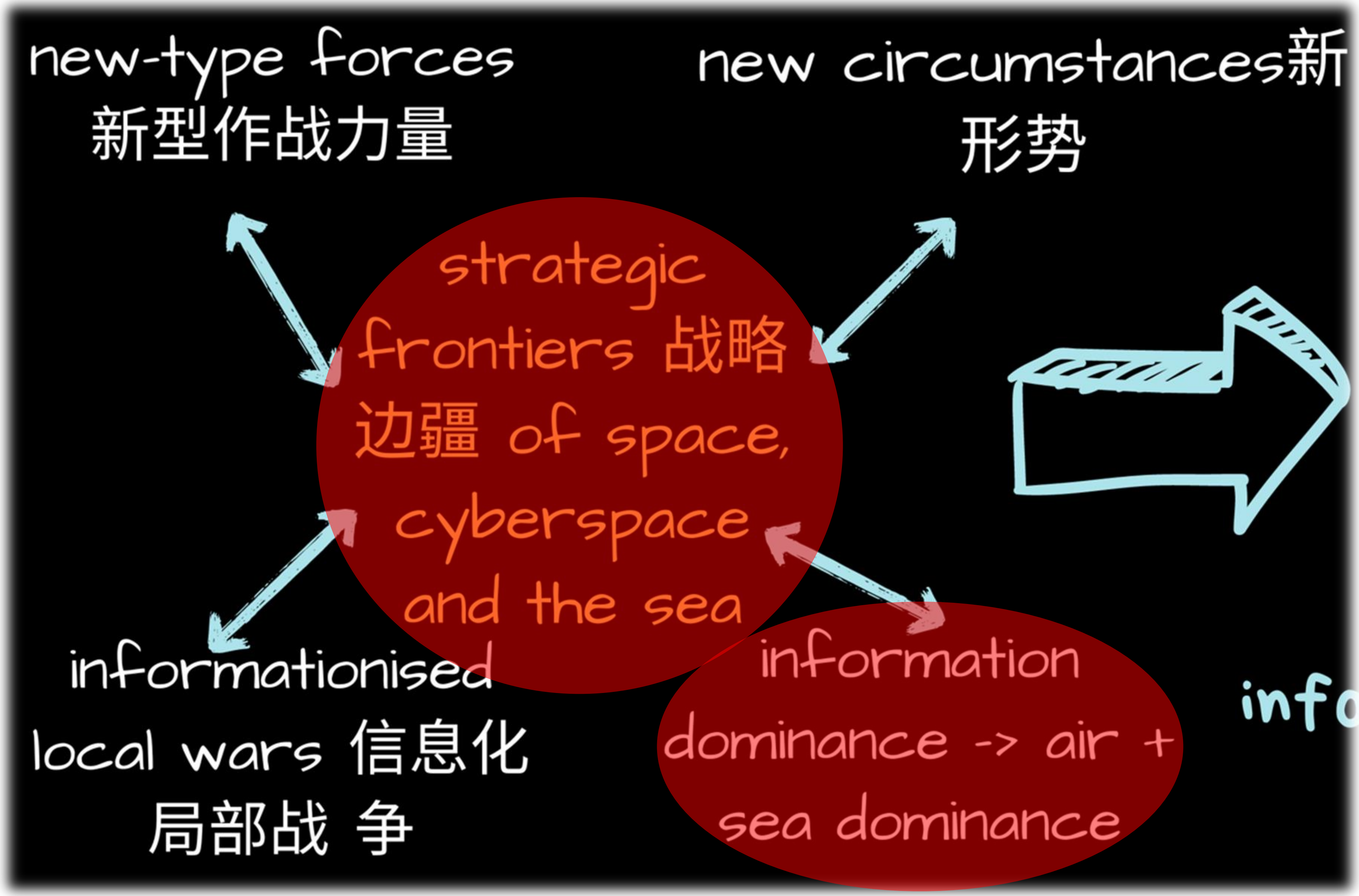
mechanisation
informationisation
intelligentisation
机械化信息化智能化

Information operations group
信息作战群
first strike 先发制人
vital point targets 要害目标
military struggle 军事斗争
information umbrella 信息伞

authorised forces 授权力量
reserve cyber forces 预备役 网络空间力
military-civil fusion 军民融合
small core, big periphery 小核心、大
外围
civilian during peacetime, military
during wartime 平时为民, 战时为军
CMC leads, theatres fight, services
build

High-res image:
https://epistemicsecurity.org/black-hat-asia-2024/Asia-24-Singh-ChinasMilitaryCyberOperations-PLA-IW-Doctrine-Chalkboard.png

Info dominance -> air + sea dominance



new-type forces 新型作战力量

new circumstances新形势

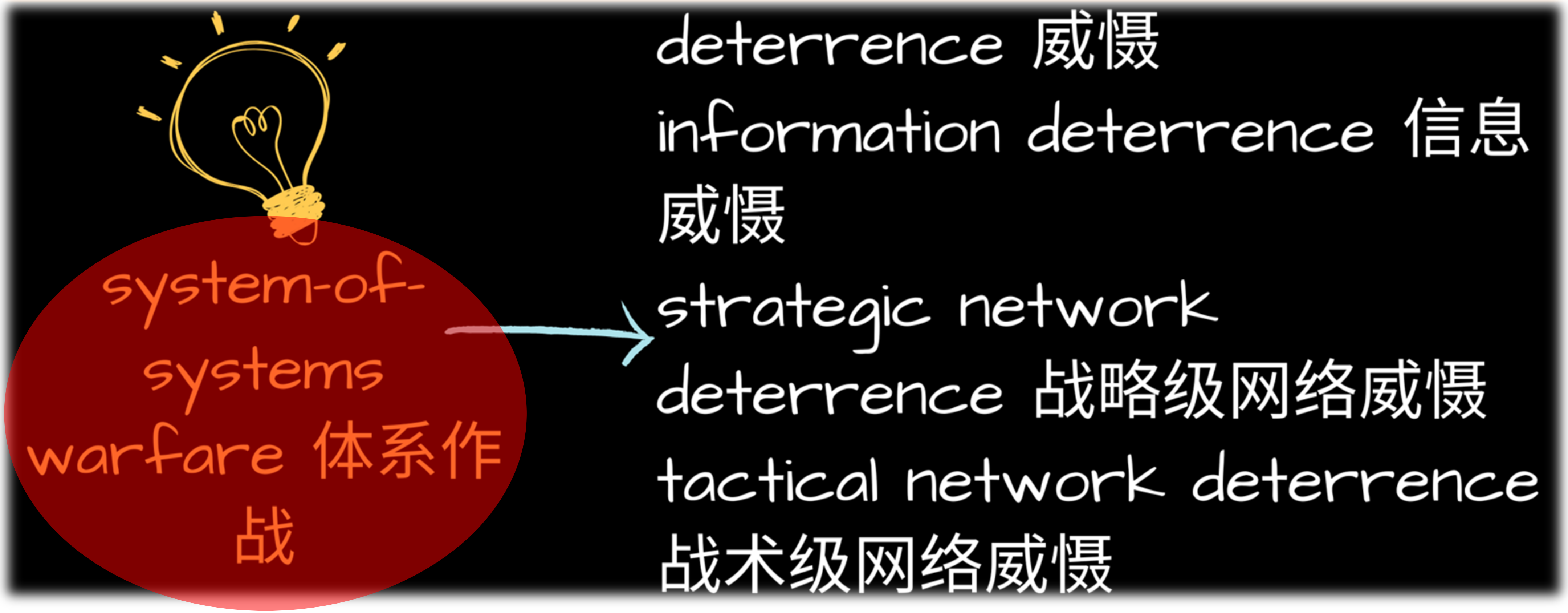
strategic frontiers 战略边疆 of space, cyberspace and the sea

informationised local wars 信息化局部战 争

information dominance -> air + sea dominance

info

System-of-systems warfare and political warfare



system-of-systems warfare 体系作战

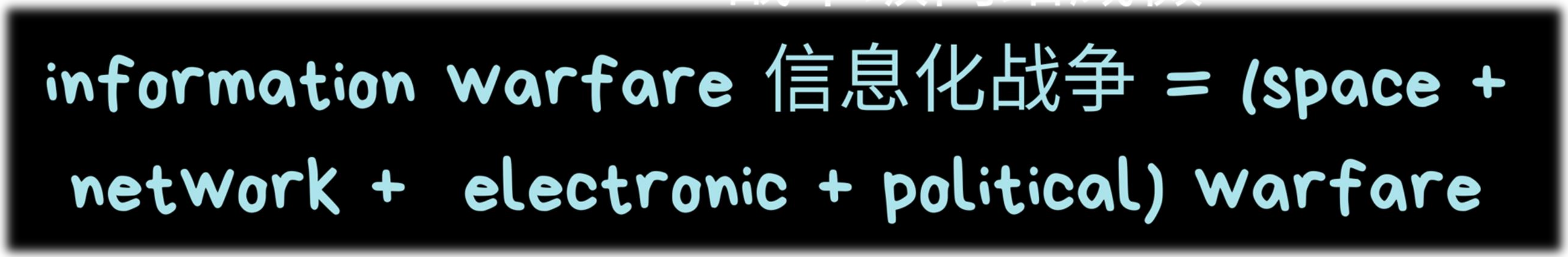
deterrence 威慑

information deterrence 信息威慑

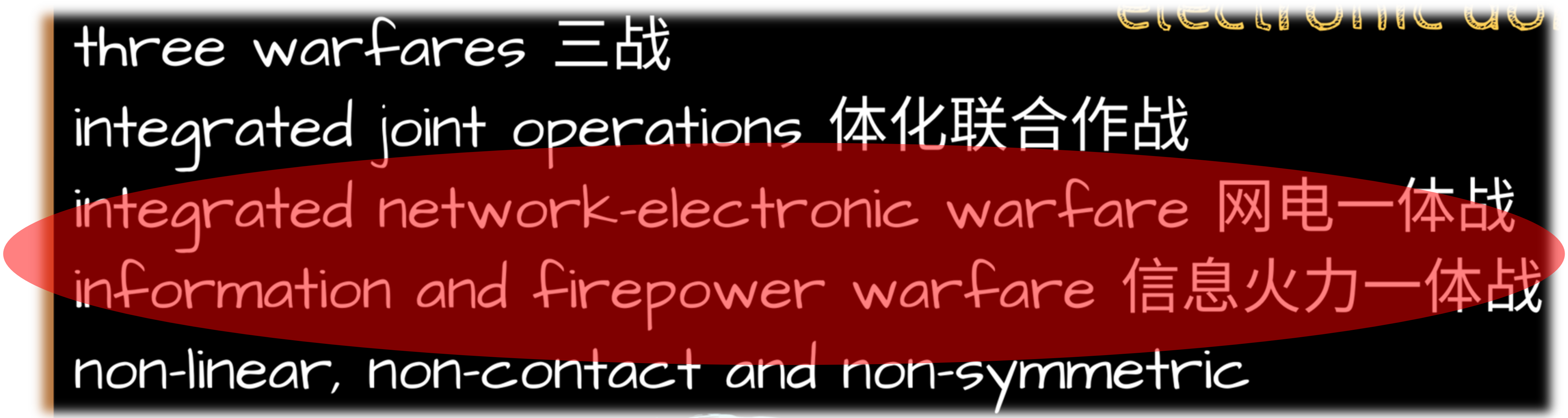
strategic network deterrence 战略级网络威慑

tactical network deterrence 战术级网络威慑

Warfighting principles



information warfare 信息化战争 = (space + network + electronic + political) warfare



electronic do

three warfares 三战

integrated joint operations 体化联合作战

integrated network-electronic warfare 网电一体战

information and firepower warfare 信息火力一体战

non-linear, non-contact and non-symmetric

Strategic infowar, first strike and political warfare

The strategic presets and key strike targets

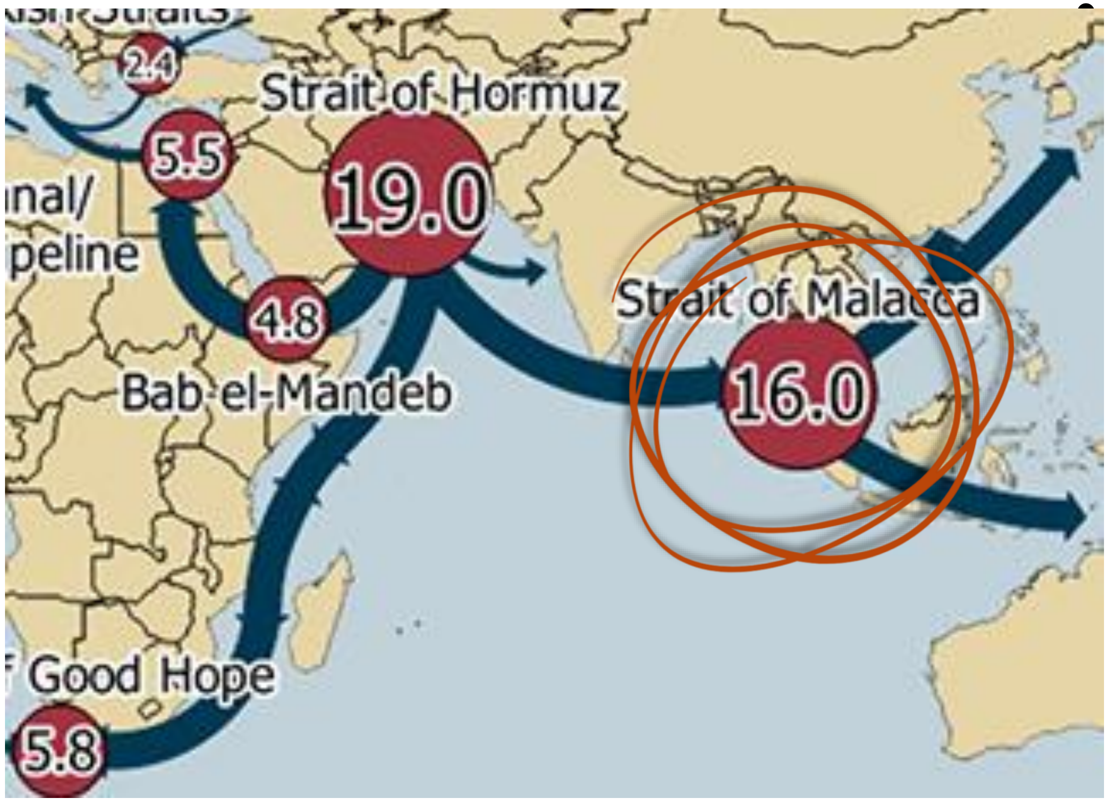
- Strategic preset and first strike (先发制人)
  - “Require careful selection of targets…so that the first salvo of hard-kill and soft-kill measures can completely cripple an enemy’s ‘operational system of systems’” (Kania and Costello, 2018)

- PLA’s Science of Military Strategy Key (2020) - Key strike targets (重点打击目标)/ vital point targets (要害目标) for INEW:
  - National and military decision-making elements, strategic early warning systems, military information networks, and financial, energy and transportation networks

- Strategic cyber warfare is a “severe escalation of interstate conflict” (国家冲突严重升级) (Chen, 2022)

The great power competition in the Indo-Pacific and the PRC's grand strategy

Multipolar Asia’s ‘Great Game’



Source: eia.gov

- “The Malacca Dilemma”
  - 3rd of all maritime traffic
  - ½ world’s container traffic
  - 2/3rd of South Korea’s energy needs
  - 60% of Japan’s energy supplies
  - 80 per cent of China’s crude oil

CCP’s “geopolitical claustrophobia”
- 7 of 10 world’s largest armies
- 5 nuclear-armed nations

Realism and the Balance of Power theory of International Relations

China’s east coast: 90% population, 75% economy

Bottom line - I

- Recent Chinese cyber operations have all the hallmarks of a military mobilisation (Operational Preparation of the Environment)

- **The strategic shift**
  - Strategic information warfare as an enabler for air and sea dominance in the South China Sea and Taiwan Strait
  - Readjust the balance of power by disrupting the US's logistics, naval projection and Freedom of Navigation in the region

- **The military cyber operations architecture**
  - Mobilisation of wartime constructs like the Information Operations Group (IOG) to rope in civilian authorities

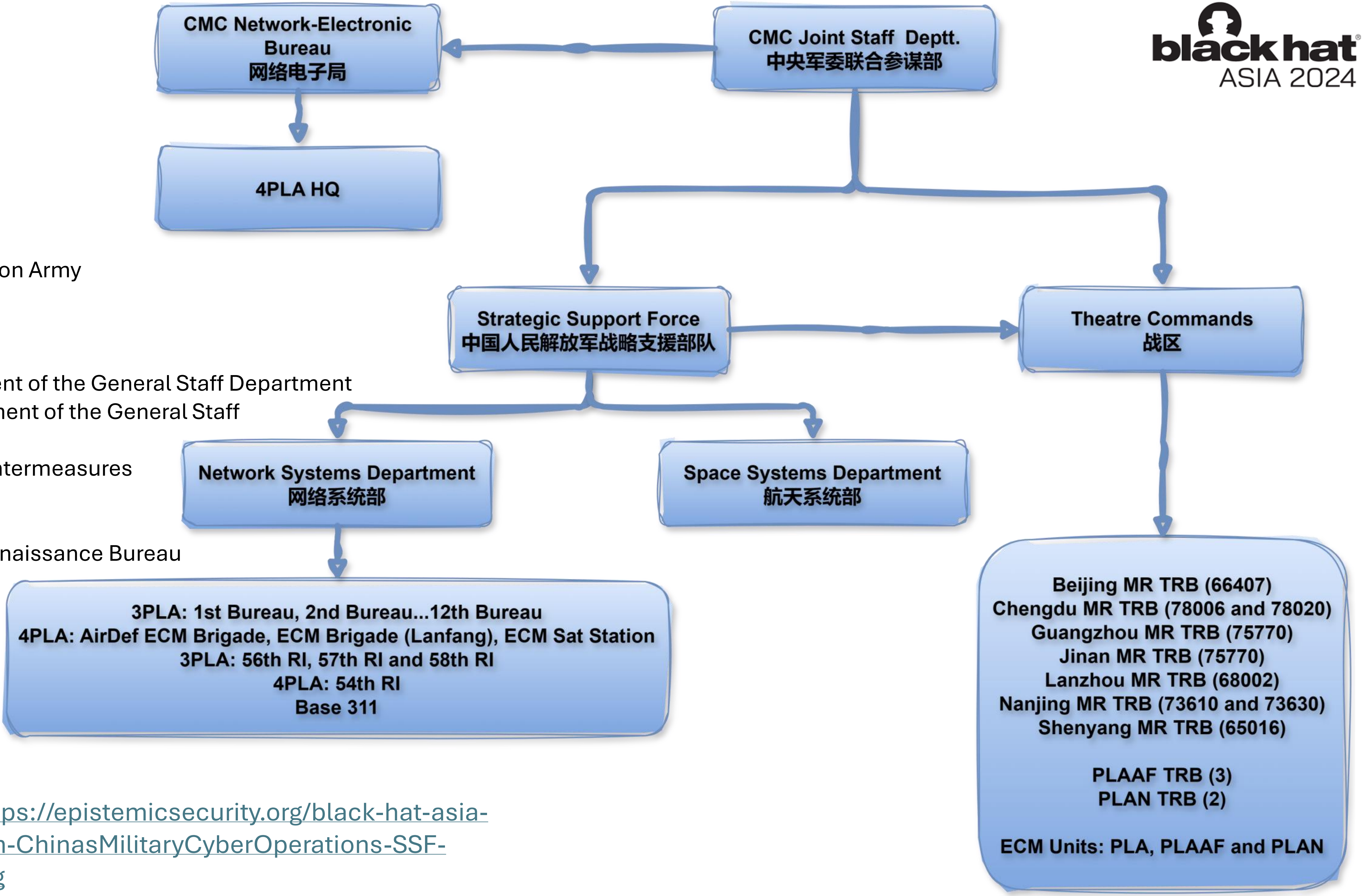
BLUF – Bottom line - II

- **The operational and tactical overlaps in threat activity clusters**
  - The absorption of ‘authorised forces’ into the wartime IOG

- **The command-and-control**
  - Strategic information operations directly authorised by the Central Military Commission

- **The political objectives**
  - Information operations, followed by electronic warfare and kinetic operations to disrupt the adversary’s system-of-systems
  - The degradation of will to resist and fight

Annexures



CMC Network-Electronic Bureau
网络电子局

CMC Joint Staff Deptt.
中央军委联合参谋部

4PLA HQ

Strategic Support Force
中国人民解放军战略支援部队

Theatre Commands
战区

Network Systems Department
网络系统部

Space Systems Department
航天系统部

3PLA: 1st Bureau, 2nd Bureau...12th Bureau
4PLA: AirDef ECM Brigade, ECM Brigade (Lanfang), ECM Sat Station
3PLA: 56th RI, 57th RI and 58th RI
4PLA: 54th RI
Base 311

Beijing MR TRB (66407)
Chengdu MR TRB (78006 and 78020)
Guangzhou MR TRB (75770)
Jinan MR TRB (75770)
Lanzhou MR TRB (68002)
Nanjing MR TRB (73610 and 73630)
Shenyang MR TRB (65016)

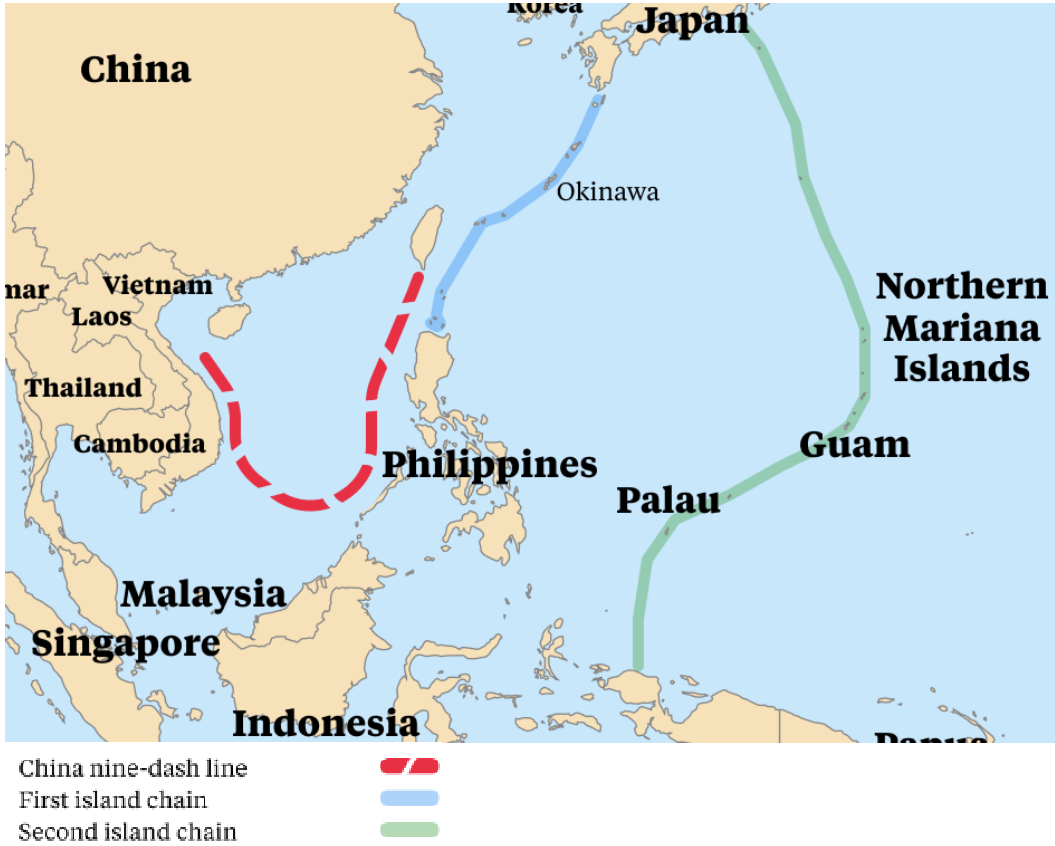
PLAAF TRB (3)
PLAN TRB (2)

ECM Units: PLA, PLAAF and PLAN

Key:
PLA: People's Liberation Army
PLAN: PLA Navy
PLAAF: PLA Air Force
AirDef: Air Defense
3PLA: Third Department of the General Staff Department
4PLA: Fourth Department of the General Staff Department
ECM: Electronic Countermeasures
RI: Research Institute
MR: Military Region
TRB: Technical Reconnaissance Bureau

High-res image: https://epistemicsecurity.org/black-hat-asia-2024/Asia-24-Singh-ChinasMilitaryCyberOperations-SSF-Reorganisation.png

Multipolar Asia’s ‘Great Game’



Source: thechinaproject.com

- AirSea Battle(US) vs. Anti-Access Area Denial (CN)
- Sea Control (CN) vs. Freedom of Maneuver (US)
- Hub-and-spokes and extended nuclear deterrence (US)

The PLA infowar strategy: Escalatory blindspots

- Strategic cyber warfare is a “severe escalation of interstate conflict” (国家冲突严重升级) (Chen, 2022)

yet…

- “Chinese strategic writings do not scrutinize the escalation risks associated with using cyber intrusions for operational preparation of the environment” (USCC, 2022)

Why did Volt Typhoon possibly target Africa?

‘Multilateral deterrence’

Chinese leadership may not necessarily engage only in deterrent activities against, say, the United States or Japan, even in the midst of a crisis with those states. Heightened operations or **limited offensive information operations, in the deterrent context, may be undertaken against third parties**, both in order to demonstrate capability and resolve against the main target (Cheng, 2021)

Sources

Volt Typhoon

- ‘2023 Adversary Infrastructure Report | Recorded Future’. Accessed 16 March 2024. https://www.recordedfuture.com/2023-adversary-infrastructure-report.
- ‘China’s Cyber Intrusions Have Hit Ports and Utilities, Officials Say - The Washington Post’. Accessed 16 March 2024. https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict/.
- ‘Chinese Cyberespionage Group BRONZE SILHOUETTE Targets U.S. Government and Defense Organizations’. Accessed 16 March 2024. https://www.secureworks.com/blog/chinese-cyberespionage-group-bronze-silhouette-targets-us-government-and-defense-organizations.
- ‘Cyber Propaganda & Influence Ops: Rising Asia-Pacific Threats | Security Insider’. Accessed 16 March 2024. https://www.microsoft.com/en-us/security/business/security-insider/reports/nation-state-reports/digital-threats-from-east-asia-increase-in-breadth-and-effectiveness/.
- ‘Dragos 2023 OT Cybersecurity Year in Review’. Accessed 16 March 2024. https://www.dragos.com/ot-cybersecurity-year-in-review/.
- Menn, Joseph. ‘U.S. Says Chinese Hackers Breached Gear in Guam, Key to Pacific Defense’. *Washington Post*, 24 May 2023. https://www.washingtonpost.com/technology/2023/05/24/china-hack-guam-taiwan/.
- ‘Office of Public Affairs | U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure | United States Department of Justice’. Accessed 16 March 2024. https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical.
- ‘People’s Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection | CISA’, 24 May 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a.
- ‘PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA’. Accessed 29 February 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.
- ‘Routers Roasting on an Open Firewall: The KV-Botnet Investigation - Lumen’. Accessed 16 March 2024. https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/.
- ‘Office of Public Affairs | Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians | United States Department of Justice’, 25 March 2024. https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived.
- U.S. Department of the Treasury. ‘Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure’, 19 March 2024. https://home.treasury.gov/news/press-releases/jy2205.

- Sanger, David E. ‘Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?’ *The New York Times*, 24 May 2023, sec. U.S. https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html.

- ‘Threat Intelligence Research: Volt Typhoon Compromises 30% of Cisco RV320/325 Devices in 37 Days | SecurityScorecard’. Accessed 16 March 2024. https://securityscorecard.com/blog/threat-intelligence-research-volt-typhoon/.

- ‘U.S. Hunts Chinese Malware That Could Disrupt American Military Operations - The New York Times’. Accessed 16 March 2024. https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html.

- ‘Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques | Microsoft Security Blog’. Accessed 29 February 2024. https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

- ‘VOLTZITE Espionage Operations Targeting U.S. Critical Systems | Dragos’, 13 February 2024. https://hub.dragos.com/report/voltzite-espionage-operations-targeting-u.s.-critical-systems.

- ‘VOLTZITE Threat Group’s Under the Radar Cyber Espionage on U.S. Critical Systems | Dragos’, 22 February 2024. https://www.dragos.com/blog/voltzite-threat-group-under-the-radar-cyber-espionage-on-us-critical-systems/.

RedEcho and RedFoxtrot

- ‘4 Chinese APT Groups Identified Targeting Mail Server of Afghan Telecommunications Firm Roshan’. Accessed 16 March 2024. https://www.recordedfuture.com/blog/chinese-apt-groups-target-afghan-telecommunications-firm.

- ‘Dragos 2021 Industrial Cybersecurity Year In Review Summary | Dragos’. Accessed 29 February 2024. https://www.dragos.com/blog/dragos-2021-industrial-cybersecurity-year-in-review-summary/.

- Inc, Recorded Future. ‘Exposing RedFoxtrot: Uncovering Targeted Espionage by Chinese Military-Linked Group’. Accessed 16 March 2024. https://go.recordedfuture.com/exposing-redfoxtrot-webinar.

- ———. ‘Insikt Report: Suspected Chinese Threat Activity Group RedFoxtrot’. Accessed 16 March 2024. https://go.recordedfuture.com/redfoxtrot-insikt-report.

- Insikt Group. ‘China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions’. *Recorded Future* (blog), 28 February 2021. https://www.recordedfuture.com/redecho-targeting-indian-power-sector.

- ———. ‘Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group’. *Recorded Future* (blog), 6 April 2022. https://www.recordedfuture.com/redecho-targeting-indian-power-sector.

- ———. ‘Threat Activity Group RedFoxtrot Linked to China’s PLA Unit 69010; Targets Bordering Asian Countries’. *Recorded Future* (blog), 16 June 2021. https://www.recordedfuture.com/redfoxtrot-china-pla-targets-bordering-asian-countries.

- ‘Space Pirates: Analyzing the Tools and Connections of a New Hacker Group’. Accessed 16 March 2024. https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections/.

- ‘Vulnerable SDK Components Lead to Supply Chain Risks in IoT and OT Environments | Microsoft Security Blog’. Accessed 16 March 2024. https://www.microsoft.com/en-us/security/blog/2022/11/22/vulnerable-sdk-components-lead-to-supply-chain-risks-in-iot-and-ot-environments/.

Other PLA TRB cyber operations

- ‘Bisonal: 10 Years of Play’. Accessed 29 February 2024. https://blog.talosintelligence.com/bisonal-10-years-of-play/#more.

- ‘CactusPete APT Group’s Updated Bisonal Backdoor | Securelist’. Accessed 16 March 2024. https://securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962/.

- ‘China’s PLA Unit 61419 Purchasing Foreign Antivirus Products, Likely for Exploitation’. Accessed 16 March 2024. https://www.recordedfuture.com/blog/china-pla-unit-purchasing-antivirus-exploitation.

- *Chinese Cyber Espionage Evolves to Support Higher Level Missions*. Cyber Defense Summit 2019, 2019. https://www.youtube.com/watch?v=mSk6I6egRD4.

- Cimpanu, Catalin. ‘Japanese Police Say Tick APT Is Linked to Chinese Military’. *The Record by Recorded Future*, 20 April 2021. https://therecord.media/japanese-police-say-tick-apt-is-linked-to-chinese-military/.

- Group-IB. ‘Nice Try Tonto Team’. Accessed 16 March 2024. https://www.group-ib.com/blog/tonto-team/.

- gygy0101. ‘Tonto Team Using Anti-Malware Related Files for DLL Side-Loading’. ASEC BLOG, 25 April 2023. https://asec.ahnlab.com/en/51746/.

- Hegel, Tom. ‘Targets of Interest | Russian Organizations Increasingly Under Attack By Chinese APTs’. SentinelOne, 7 July 2022. https://www.sentinelone.com/labs/targets-of-interest-russian-organizations-increasingly-under-attack-by-chinese-apts/.

- ‘Naikon - Traces from a Military Cyber-Espionage Operation’. Accessed 29 February 2024. https://www.bitdefender.com.au/business/resource-library/naikon---traces-from-a-military-cyber-espionage-operation.html.

- ‘Naikon APT Hid Five-Year Espionage Attack Under Radar | Threatpost’. Accessed 29 February 2024. https://threatpost.com/naikon-apt-five-year-espionage-attack/155492/.

- ‘Operation ENDTRADE: Multi-Stage Backdoors That TICK’. Accessed 29 February 2024. https://www.trendmicro.com/en_us/research/19/k/operation-endtrade-finding-multi-stage-backdoors-that-tick.html.

- ThreatConnect. ‘Project CameraShy Closing The Aperture On China’s Unit 78020 | Resources’. Accessed 29 February 2024. https://threatconnect.com/resource/project-camerashy-closing-the-aperture-on-chinas-unit-78020/.

- ‘GB APT31 Intrusion Set Campaign: Description, Countermeasures and Code – CERT-FR’. Accessed 16 March 2024. https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-013/.

- Aimé, Felix. ‘Walking on APT31 Infrastructure Footprints’. Sekoia.io Blog, 10 November 2021. https://blog.sekoia.io/walking-on-apt31-infrastructure-footprints/.

ShadowPad

- Constantin, Lucian. ‘ShadowPad Has Become the RAT of Choice for Several State-Sponsored Chinese APTs’. *CSO*, 16 February 2022. https://www.csoonline.com/article/3649777/shadowpad-has-become-the-rat-of-choice-for-several-state-sponsored-chinese-apts.html.

- FireEye. ‘Double Dragon: APT41, a Dual Espionage and Cyber Crime Operation’, 2019. https://content.fireeye.com/apt-41/rpt-apt41/.

- ‘Higaisa or Winnti? APT41 Backdoors, Old and New’. Accessed 16 March 2024. https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/.

- Hsieh, Yi-Jhen, and Joey Chen. ‘ShadowPad: A Masterpiece of Privately Sold Malware in Chinese Espionage’. SentinelOne, August 2021. https://assets.sentinelone.com/c/Shadowpad?x=P42eqA#page=1.

- Intrusion Truth. ‘Chinese APTs: Interlinked Networks and Side Hustles’, 24 July 2022. https://intrusiontruth.wordpress.com/2022/07/24/chinese-apts-interlinked-networks-and-side-hustles/.

- ‘ShadowPad: New Activity from the Winnti Group’. Accessed 16 March 2024. https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/shadowpad-new-activity-from-the-winnti-group/.

The Chinese grand strategy, PLA, SSF and information warfare doctrine

- ‘463. Intelligentization and the PLA’s Strategic Support Force | Mad Scientist Laboratory’. Accessed 16 March 2024. https://madsciblog.tradoc.army.mil/463-intelligentization-and-the-plas-strategic-support-force/.

- ‘America’s Convenient Territories: How Washington Is Preparing to Duel Beijing in the Pacific – The China Project’. Accessed 16 March 2024. https://thechinaproject.com/2023/08/25/americas-convenient-territories-how-washington-is-preparing-to-duel-beijing-in-the-pacific/.

- Cao, Cosmo. ‘The PLA Strategic Support Force: Future-Proofing China’s Military’. The Strategist, 9 November 2023. https://www.aspistrategist.org.au/the-pla-strategic-support-force-future-proofing-chinas-military/.

- ‘Charting China’s Climb as a Leading | Recorded Future Global Cyber Power’. Accessed 29 February 2024. https://www.recordedfuture.com/charting-chinas-climb-leading-global-cyber-power.

- Chen, John, Joe McReynolds, and Kieran Green. ‘The PLA Strategic Support Force: A “Joint” Force for Information Operations’. In *The PLA beyond Borders : Chinese Military Operations in Regional and Global Context*. People’s Liberation Army beyond Borders. Washington, D.C.: Washington, D.C. : National Defense University Press, 2021.

- Cheng, Dean. *Cyber Dragon: Inside China’s Information Warfare and Cyber Operations : Inside China’s Information Warfare and Cyber Operations*. Westport STATES: ABC-CLIO, LLC, 2016. http://ebookcentral.proquest.com/lib/unsw/detail.action?docID=4723164.

- ‘China’s Digital Colonialism: Espionage and Repression Along Digital Silk Road’. Accessed 29 February 2024. https://www.recordedfuture.com/blog/china-digital-colonialism-espionage-silk-road.

- ‘Chinese State-Sponsored Cyber Espionage Activity Supports Expansion of Regional Power and Influence in Southeast Asia’. Accessed 16 March 2024. https://www.recordedfuture.com/blog/chinese-state-sponsored-cyber-espionage-expansion-power-influence-southeast-asia.

- ‘From Coercion to Invasion: The Theory and Execution of China’s Cyber Activity in Cross-Strait Relations | Recorded Future’. Accessed 29 February 2024. https://www.recordedfuture.com/blog/from-coercion-to-invasion-the-theory-and-execution-of-china-cyber-activity.

- Inc, Recorded Future. ‘Off the Record: The Digital Silk Road: How Beijing Embeds Itself in Foreign Infrastructure | Recorded Future’. Accessed 16 March 2024. https://go.recordedfuture.com/the-digital-silk-road.

- Inkster, Nigel. *China’s Cyber Power*. Routeledge, 2018.

- Institute, Project 2049. ‘The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure’, 11 November 2011. https://project2049.net/2011/11/11/the-chinese-peoples-liberation-army-signals-intelligence-and-cyber-reconnaissance-infrastructure/.

- Kania, Elsa B., and John K. Costello. ‘The Strategic Support Force and the Future of Chinese Information Operations’. *Cyber Defense Review*, no. Spring 2018 (2018): 105–21.

- Lockyer, Adam. *Australia’s Defence Strategy : Evaluating Alternatives for a Contested Asia*. Kindle Edition. Melbourne, AUSTRALIA: Melbourne University Publishing, 2017.

- ‘Section 2: China’s Cyber Capabilities: Warfare, Espionage and Implications for the United States’. In *2022 Report to Congress of the U.S.-China Economic and Security Review Commission*. Superintendent of Documents, U.S. Government Publishing Office, 2022. https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf.

- U.S. China Economic and Security Review Commission. ‘Hearing: China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States’, 17 February 2022. https://www.uscc.gov/hearings/chinas-cyber-capabilities-warfare-espionage-and-implications-united-states.

- Hart, Brian. ‘How Did the 20th Party Congress Impact China’s Military?’ ChinaPower Project (blog), 12 October 2022. https://chinapower.csis.org/20th-party-congress-china-military-pla-cmc/.
- Stokes, Mark. ‘The PLA General Staff Department Third Department Second Bureau’, 2015. https://project2049.net/wp-content/uploads/2018/04/P2049_Stokes_PLA_General_Staff_Department_Unit_61398_072715.pdf.

Thanks!