世界杰出华商500强俱乐部指定用茶
第四届中国国际徽商大会黄山市礼品茶
生产商：黄山市黄山区三门滩茶业有限公司
百年徽菜
胡氏
胡氏老徽菜
徽菜胡氏正宗

STRATEGIC REPORT TLP:CLEAR

A three-beat waltz:
The ecosystem behind Chinese state-sponsored cyber threats

Coline Chavane and TDR team, November 2024

sekoia

> China’s approach has enabled it to enhance the efficacy of its cyber operations against foreign targets while introducing operational asymmetries with other states.
>
> *Hacking Contests, Bug Bounties, and China’s Offensive Cyber Ecosystem*
> Eugenio Benincasa

目录

Table of Contents

介绍

Introduction

Recent reports about the **People's Republic of China (PRC) cyber capabilities** highlighted its important arsenal mobilising institutional and military actors, as well as private companies providing **hack-for-hire services** for governmental operations. These findings pointed out the complexity of attributing attack campaigns to specific clusters of malicious activity and tracing back Chinese state-sponsored units throughout the time.

This report aims at presenting the Chinese offensive cyber ecosystem, its key actors, their role and their relationships, based on Sekoia's analysis of the latest cyber campaigns attributed to China, open source reports, and interviews conducted with prominent researchers on the topic.

Thanks to **Ivan Kwiatkowski, Dakota Cary and Eugenio Benincasa** for their time and insights into this subject.

Key Takeaways

> The **People's Liberation Army** (PLA), the **Ministry of State Security** (MSS) and the **Ministry of Public Security** (MPS) are the three main **state actors** conducting state-sponsored offensive cyber operations for the interests of the Chinese Communist Party (CCP).

> From 2021 onward, Sekoia observed that operations attributed to China were **mostly linked to the Ministry of State Security (MSS)** rather than the People's Liberation Army (PLA). Still, since the 2015 PLA reform, malicious cyber activity attributed to MSS-sponsored entities **increased**, while activity attributed to the PLA **depleted**.

> **Provincial departments** of the MSS and the MPS enjoy a **large degree of autonomy** to conduct cyber operations and **rely on private companies** to outsource offensive capacities.

> In addition to state actors, **civilian actors also took part historically** in state-sponsored operations. This is the case of the **first communities of patriotic hackers**, which conducted hacktivist campaigns in reaction to geopolitical events, and were progressively integrated into state-sponsored operations.

> The role of patriotic hackers in Chinese cyber offensive capacities is highlighted by their participation in the **development of malicious payloads** used by China-nexus APTS, such as **PlugX and ShadowPad**. This proximity was encouraged by the policies of Xi Jinping, who made **Military-Civil Fusion (MCF) a national strategy** in 2015.

> The CCP policy regarding activities of patriotic hackers changed after 2002, leading patriotic hackers to **stop hacktivism and professionalise**. Today, many of these individuals work for private companies and maintain parallel activities like cybercrime.

> Recent leaks from the Chinese IT company I-SOON revealed important details about the **current hack-for-hire ecosystem** in China. State actors subcontract cyber offensive services at the provincial and the city levels.

> State actors **increasingly outsource** cyber offensive capabilities to private entities, a trend fueled by ministries like the **MSS collecting vulnerabilities** from researchers and companies. These vulnerabilities are then **weaponized** and used as exploits in state-sponsored operations.

> The companies providing cyber offensive capacities to state actors are historical tech giants, but also **smaller companies offering niche digital services**, like I-SOON.

> China-nexus APTs are likely to be a **mix of private and state actors cooperating** to conduct operations, rather than strictly being associated with single units.

Page left intentionally blank

壹

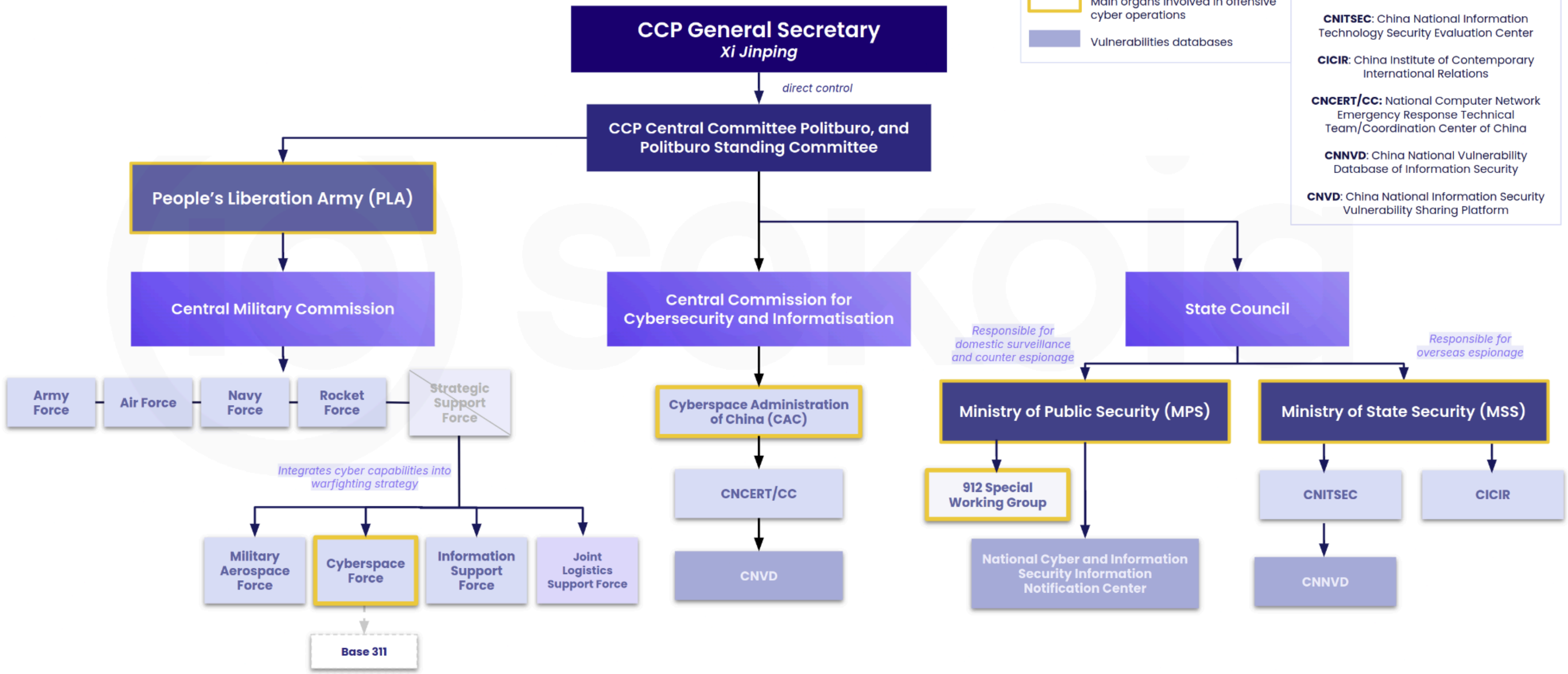
Part one

Chinese state actors involved in cyber activities

This section will explore the role of state actors in the Chinese offensive cyber ecosystem, which in this paper means the People's Liberation Army (PLA), the Ministry of State Security (MSS) and the Ministry of Public Safety (MPS).

It will first dive into the development of China's military offensive cyber capabilities within the PLA and put it in perspective with broader Chinese geopolitical and domestic issues. It will then explain the role of the Ministry of State Security (MSS) and the Ministry of Public Safety (MPS), which also have cyber capabilities dedicated to offensive operations and have been particularly active in conducting cyber espionage campaigns during the last years.

sekoia | Chinese state actors involved in cyber activities


CCP General Secretary
Xi Jinping
direct control
CCP Central Committee Politburo, and Politburo Standing Committee
People's Liberation Army (PLA)
Central Military Commission
Army Force
Air Force
Navy Force
Rocket Force
Strategic Support Force
Integrates cyber capabilities into warfighting strategy
Military Aerospace Force
Cyberspace Force
Information Support Force
Joint Logistics Support Force
Base 311
Central Commission for Cybersecurity and Informatisation
Cyberspace Administration of China (CAC)
CNCERT/CC
CNVD
State Council
Responsible for domestic surveillance and counter espionage
Ministry of Public Security (MPS)
912 Special Working Group
National Cyber and Information Security Information Notification Center
Responsible for overseas espionage
Ministry of State Security (MSS)
CNITSEC
CICIR
CNNVD

LEGEND

- ▭ Main organs involved in offensive cyber operations
- ▨ Vulnerabilities databases

ACRONYMS

CCP: Chinese Communist Party

CNITSEC: China National Information Technology Security Evaluation Center

CICIR: China Institute of Contemporary International Relations

CNCERT/CC: National Computer Network Emergency Response Technical Team/Coordination Center of China

CNNVD: China National Vulnerability Database of Information Security

CNVD: China National Information Security Vulnerability Sharing Platform

Military actors - The People's Liberation Army

This section examines the development of **Chinese cyber capabilities within the People's Liberation Army (PLA)**, which is the sword arm of the Chinese Communist Party (CCP). This development has been especially shaped by China's global internet connection and the **Integrated Network Electronic Warfare (INEW) doctrine.**

This doctrine emphasises the **importance of information superiority in modern warfare** and has been central to China's military modernisation. Heavily influenced by China's understanding of US' technological and information dominance as a key element to rapid victory with minimal losses, this understanding has guided the development of Chinese military cyber capabilities, especially **under Xi Jinping's presidency.**

Development of military cyber capabilities

From 1990's to 2012

During this period, the Chinese cyber operations were relatively "loud", relying on malware with few defence evasion mechanisms, and focusing on ***targeting entities in the US and allied countries****. These operations were* ***mainly attributed to the PLA*** *and aimed at gathering intelligence to foster Chinese development and close the gap with Western countries.*

Context

The Internet arrived in China in 1994. Initially limited to government and academic institutions, it has extended to the population with the launch of the first Chinese Internet Service Provider ChinaNet in 1995. This expansion has been accompanied by a tight control over content and Internet traffic with the exterior: the **Great Firewall was introduced in 1998, becoming fully operational by 2003** to control internet traffic and censor politically sensitive content. But it has also led to the development of information and technological skills among Chinese citizens. In the 1990's, first **patriotic hacker communities** were founded, engaging in hacktivist DDoS campaigns to protest against perceived injustices regarding China.

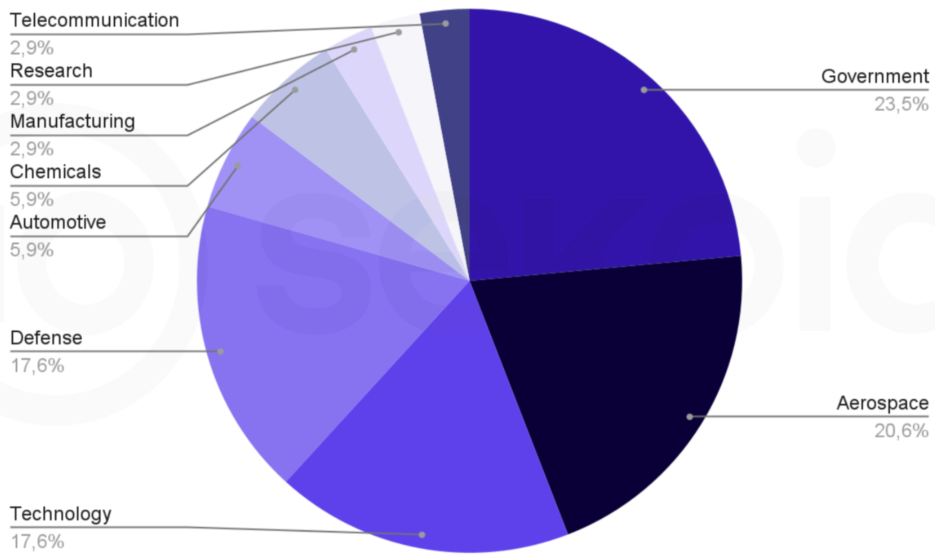
Development of Military Cyber Capabilities

By the early 2000s, the PLA developed cyber capabilities within the **General Staff Department (GSD)**, establishing the **3rd Department for Signal Intelligence (SIGINT)**, responsible for what can be considered as the equivalent of the US concept of Computer Network Defense (CND). In addition, the **PLA 4th Department** has been set up to conduct **electronic warfare** and what can be considered as Computer Network Attack (CNA).

Information warfare militia units were also created with private IT sector and academia experts to support strategic cyber operations. For instance, the Guangzhou Military Region implemented "Militia Information Technology Battalions" in local IT firms, composed of individuals with specific technical and linguistic skills to conduct offensive R&D and operations.

These military cyber capabilities aimed at **ensuring information dominance over a rival in the earliest phases of a conflict** and to support other conventional forces. From their early development in the 1990's to mid-2000, these capabilities especially focused on **targeting strategic sectors** to support intelligence collection against the US government and industry.

| US sectors targeted by Chinese cyber operations (2003-2012)



Source: Based on CSIS data, A Survey of Reported Chinese Espionage, 2000 to the Present March 2023

From 2012 to 2017

During this period, Chinese cyber operations entered a ***new era,*** *with campaigns targeting strategic sectors* ***more massive and in the long term****. It served to help China to catch up with the US from a strategic and economic point of view, using cyber to compensate for the asymmetry of forces. It also allowed China to defend its influence in the Asia Pacific region.*

In addition, the ***American strategy of public denunciation*** *of Chinese cyber espionage campaigns translated into a need for more sophisticated and discrete cyber operations. It has led historical Chinese APTs, such as APT1 attributed to the PLA, to* ***disappear from the radar of security researchers, while others have emerged.*** *It can be explained by both internal reorganisation of operational units and a higher degree of sophistication in attacks.*

Context

In 2012, Xi Jinping took office as the Chair of the Central Military Commission and became President in 2013. His foreign policy was marked by **its vision of US-China relations,** considering it as a **Thucydides trap**, with two great powers having to find balanced relationships and prevent confrontation for the sake of humanity. Xi Jinping was especially critical of the American pivot to Asia, with the reinforcement of US strategic alliances especially with Japan and the Philippines.

On the cyber front, Xi reoriented Chinese intelligence gathering priorities, focusing on **bolstering strategic objectives for China's development,** long term espionage campaigns, and competing with the US while making up with an asymmetry of forces. It constituted a turning point compared to previous less regulated state-sponsored operations stealing foreign commercial technologies to give or sell them to Chinese companies. The US responded with indictments publicly condemning Chinese hackers for conducting cyber operations against US entities from 2014. This surge was only **briefly slowed by the 2015 Cybersecurity Agreement between Beijing and Washington**, which aimed to reduce intellectual property theft through cyber means.

Development of Military Cyber Capabilities

China continued advancing its cyber military capabilities, making it a key element of its national strategy. In 2014, Xi Jinping emphasised that China must become **a "cyber powerhouse"** and conducted a **major PLA reform in 2015, establishing the Strategic Support Force** (SSF). The SSF united cyber, space, and electronic warfare under one command, shifting from a discipline-based to a domain-based approach. Cyber capabilities were centralised in the **Network Systems Department of the SSF,** putting an end to the initial separation between defensive and offensive capabilities that existed with the former 3rd and 4th departments.

The PLA also replaced previous military regions with **five theatre commands (TC)** under the Central Military Commission (CMC) to improve responsiveness, similar to US combatant commands. Indeed, each TC is responsible for threats and crises within its assigned region and controls brigades and units to conduct operations. Their chain of command extends to the national command structure in peacetime and is **restricted to the TC only in wartime**.

From 2017 to 2024

During this period, cyber campaigns attributed to the PLA decreased ***for unclear reasons,*** *whereas PRC-sponsored operations continue to target worldwide entities in strategic sectors. This observation denoted with the PLA reform started in 2015 and finalised in April 2024, which aims at increasing the effectiveness of PLA operations, especially regarding information warfare. It left open questions about the* ***distribution of responsibilities in terms of strategic cyber operations between the PLA and other institutions,*** *such as the Ministry of State Security (MSS) and the Ministry of Public Security (MPS), and about the evolution of military cyber capabilities throughout the time.*

Context

The 2016 Trump election to the White House led to tougher US policies on China, which **increased tensions between the two countries.** From 2018 to 2020, tensions were particularly high due to commercial competition translated into the rise of customs duties. The Covid-19 pandemic continued to illustrate this rivalry, with both countries accusing each other of being responsible for the crisis.

Since 2018, human rights abuses in Hong Kong and Xinjiang also have significantly strained relations between China and European countries. European nations have repeatedly condemned China's actions, leading to sanctions against Chinese officials, notably for the repression of Uyghurs and the imposition of the Hong Kong National Security Law.

At the same time, China expanded its influence worldwide through initiatives like the **Belt and Road Initiative adopted in 2017** and significant infrastructure projects such as the E763 highway in Serbia and the China Railway Express. The long-term **surveillance of the African Union’s headquarters illustrated how these Chinese infrastructure also served for cyber intelligence gathering at the benefit of Beijing**.

Alongside this, Beijing conducted significant cyber espionage campaigns **based on supply chain attacks.** It was illustrated by the **infection of a version of the popular CCleaner software** with a malicious backdoor in 2017, and by the **Operation ShadowHammer** detected in 2019 and infecting ASUS products. At the same time, China aimed at reinforcing domestic demands and the development of Chinese companies through the adoption of the **2022-2035 Strategic Plan for Expanding Domestic Demand.**

Development of Military Cyber Capabilities

During this period, cyber operations attributed to the PLA mainly focused on targeting entities in **Taiwan**. In April 2024, the PLA announced a **second major reform**, dissolving the SSF and creating three new forces: **the Aerospace Force, Information Support Force, and Cyberspace Force**. These new entities inherited the SSF’s capabilities and missions, while gaining greater autonomy by becoming independent forces.

Numerous Chinese cyberespionage operations targeted Europe, highlighting China's growing focus on European technologies and European Union (EU) policy, despite significant trade relations. Notably, **from 2021 onward, Sekoia observed that operations attributed to China were mostly linked to the Ministry of State Security (MSS) rather than the People's Liberation Army (PLA).** This observation should also be seen in the context of the decline in the number of campaigns formerly attributed to China since 2020.

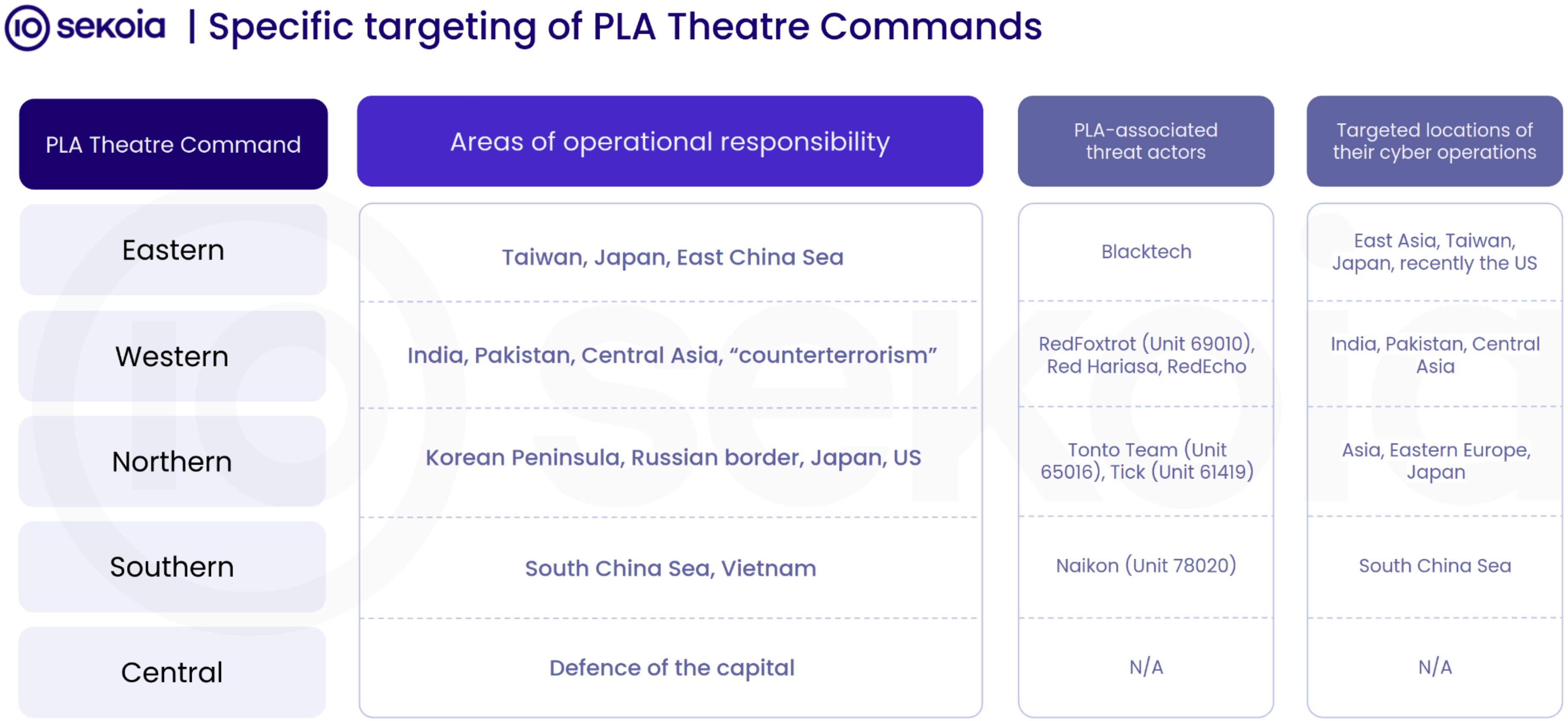
Geographical organisation: Theatre Commands

The 2015's PLA reform led to the creation of five theatre commands (TC), replacing the previous seven military regions. This military reform focuses on enhancing China's ability to conduct joint operations across different military branches. Regional theatre commands facilitate integrated operations by mobilising forces directly assigned to the region, supported by technical reconnaissance bureaus and bringing command centres closer to the field.

In his 2016 speech to the new commanders, Xi Jinping underscored TCs objectives, highlighting their importance in implementing **a joint command system**. Indeed, TCs hold significant - though not absolute - command authority over their regions. They are responsible for formulating strategies, tactics, and policies tailored to their specific areas and **are tasked with responding to threats and crises within their assigned region.** They command units of each military force and specialised brigades, as well as technical reconnaissance bureaus. These bureaus existed in previous military regions and were responsible for intelligence operations, including the use of cyber means.

This organisation also aims at preventing the creation of centres of power within the PLA. It reinforces the CCP's control over the military and corruption, with a centralised authority - the Central Military Commission (CMC) -, chaired by Xi Jinping. **Each theatre command focuses on specific areas**.

The **areas of responsibility assigned to each TC correspond with the victimology of APTs associated with military units located in a specific TC**. However, it has to be noted that the victimology of some historical APTs associated with PLA has not changed since after the 2015 PLA reform. This is the case for Tick, which is active since at least 2008, for BlackTech and Naikon, which are active since at least 2010, and for Tonto Team, which is active since at least 2013.



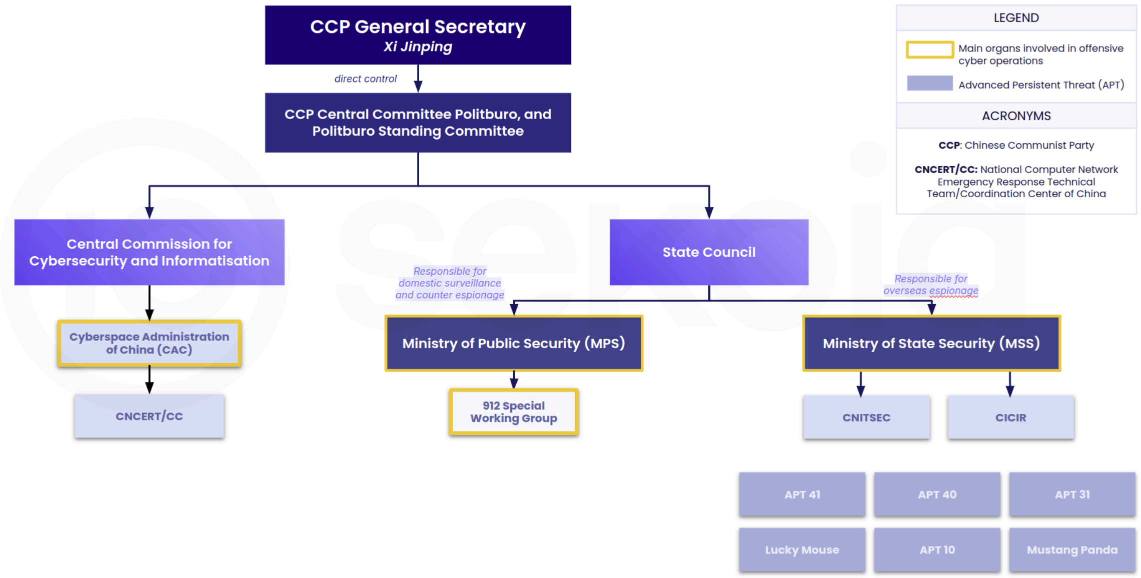
sekoia | Specific targeting of PLA Theatre Commands

PLA Theatre Command	Areas of operational responsibility	PLA-associated threat actors	Targeted locations of their cyber operations
Eastern	Taiwan, Japan, East China Sea	Blacktech	East Asia, Taiwan, Japan, recently the US
Western	India, Pakistan, Central Asia, “counterterrorism”	RedFoxtrot (Unit 69010), Red Hariasa, RedEcho	India, Pakistan, Central Asia
Northern	Korean Peninsula, Russian border, Japan, US	Tonto Team (Unit 65016), Tick (Unit 61419)	Asia, Eastern Europe, Japan
Southern	South China Sea, Vietnam	Naikon (Unit 78020)	South China Sea
Central	Defence of the capital	N/A	N/A

Ministerial actors - The Ministry of State Security and the Ministry of Public Security

The PLA is **not the only** Chinese state actor in charge of offensive strategic cyber operations. Indeed, ministries under the State Council also have dedicated competencies in this field. This section will focus on the role of **the Ministry of State Security (MSS) and the Ministry of Public Security (MPS)** in particular. It will examine their prerogatives in the conduct of cyber operations, and focus on the provincial level, where MSS and MPS departments enjoy a **high degree of autonomy** to launch operations.

sekoia | Chinese institutions with cyber responsibilities


CCP General Secretary
Xi Jinping
direct control
CCP Central Committee Politburo, and Politburo Standing Committee
Central Commission for Cybersecurity and Informatisation
State Council
Responsible for domestic surveillance and counter espionage
Responsible for overseas espionage
Cyberspace Administration of China (CAC)
Ministry of Public Security (MPS)
Ministry of State Security (MSS)
CNCERT/CC
912 Special Working Group
CNITSEC
CICIR
APT 41
APT 40
APT 31
Lucky Mouse
APT 10
Mustang Panda
LEGEND
Main organs involved in offensive cyber operations
Advanced Persistent Threat (APT)
ACRONYMS
CCP: Chinese Communist Party
CNCERT/CC: National Computer Network Emergency Response Technical Team/Coordination Center of China

Ministries prerogatives in terms of cyber operations

> *The MSS and the MPS have distinct responsibilities in terms of cyber operations and targeting. However, when it comes to domestic threats, such as the Five Poisons (Democracy advocates, Taiwan, Tibetans, Uyghurs and Falun Gong), the distinction between MSS and MPS respective roles in cyberspace remains unclear.*

Among CCP ministries having responsibilities in terms of cyber capabilities and cyber security, the **Ministry of State Security (MSS)** is the one which conducts most of the offensive operations against foreign entities. Indeed, it is in charge of intelligence gathering to support national interests, surveillance operations against domestic threats, as well as counter intelligence.

It can be considered as the equivalent of Russia's Federal Security Service (FSB) due to its large range of action inside and outside the borders. It is overseen by the CCP Politburo Standing Committee, which gathers the most influential members of the Politburo of the CCP. MSS operations are a great indicator of the strategic objectives of the CCP.

APT40, APT41, APT31, Mustang Panda, Lucky Mouse, and APT10 are active China-nexus intrusion sets directly associated with the MSS and conducting intelligence gathering and lucrative campaigns. APT41 can be considered as an umbrella group, encompassing various sub-clusters of malicious activities. APT40, APT41, APT31 particularly target Western countries, while Mustang Panda, Lucky Mouse and APT10 have a broader scope of targets, including North America, Europe, Middle East, Africa, and countries in the region of the South China Sea.

The **Ministry of Public Security (MPS)** also plays an important role in terms of cyber operations. It is China's national police force and is responsible for enforcing laws related to crime, public order and terrorism online, as well as controlling and monitoring Internet contents. It is organised and commanded locally, typically by provincial governments. Influence campaigns and surveillance operations have already been attributed to the MPS by researchers and state agencies. According to **A. Zhang, T. Hoja and J. Latimore in "Gaming Public Opinion"**, the MPS would have conducted influence operations in Southeast Asia and other countries with the participation of Qi An Xin, a leader in China's cybersecurity industry. In April 2023, the US Department of Justice also condemned 40 MPS officers for an operation against dissidents in the United States using fake social media accounts to harass them. During this operation, MPS officers operated with the **Cyberspace Administration of China (CAC).**

Poison Carp's activity can be associated with the MPS targeting, but most of the time MPS cyber operations are not related to a specific intrusion set. An US indictment indicated that the MPS officers responsible for conducting intelligence gathering against US entities leveraging cyber means would be part of the **"912 Special Project Working Group"**, which is a specific MPS unit responsible for "target[ing] Chinese dissidents located throughout the world".   It is interesting to note that contrary to the MSS, which is largely associated with several Advanced Persistent Threats (APTs), the MPS is linked to a very few number of intrusion sets. However, the 2024 I-SOON leaks revealed that the MPS bureaus are important clients of I-SOON hack-for-hire services at the provincial and the city level.

It might be explained by **several hypotheses:**

> It can indicate that MPS units **are less tracked** by cyber security providers as MPS bureaus focus mainly on Chinese dissidents and the Five Poisons.

> It may highlight a **lack of attribution of malicious clusters to the MPS**, as this Ministry is perhaps less known to cyber security providers as the source of offensive cyber operations, even outside of China.

Geographical organisation: Provinces

The MSS and the MPS have province-level administrative bureaus, which likely have an important degree of autonomy to conduct cyber operations. Indeed, provinces have proper cyber capabilities and targeting, and adopt different strategies to conduct cyber operations to fit with national objectives.

Based on Sekoia research and observations of Chinese state-sponsored campaigns, **distinct behavioural trends can be observed among provinces in terms of cyber operations**. For example, some provinces are more inclined to entrust part of their cyber operations to private companies, while others rely on front companies to carry out their operations. These trends can be explained partly by the following assumptions:

> According to I-SOON leaks, **vulnerabilities collected** by the MPS through the National Vulnerability Database (NVDB) and hacking contests **are not equally shared** among provinces, even though they could be used for offensive cyber operations. This can be explained by the difference in targeting, but also by discrepancies in terms of cyber capabilities of provinces to weaponize proof-of-concepts for cyber operations.

> Provinces seem to have **different degrees of cyber capabilities** internally and have different ways to **operate cyber operations**. Some provinces rely on contracts with private companies to outsource the conduct of their cyber operations. For instance, the MSS bureaus of the Sichuan Province have been identified several times as relying on private companies such as Chengdu 404 and I-SOON, for their offensive campaigns. This can be explained by the fact that Chengdu concentrates a large number of IT companies, bringing together a range of services that can then be exploited by state actors to carry out operations at lower cost. On the other hand, the MSS department of the Hubei Province, associated with APT31, was observed **relying on front companies to dissimulate its offensive cyber operations**. Fronts are not real companies, as they do not generate any business.

> MSS provincial bureaus seem to be in charge of **targeting specific locations and sectors abroad** and focus mainly on foreign entities and the five poisons, while MPS bureaus conduct surveillance operations against Chinese abroad or inside the country. The repartition of responsibilities between MPS and MSS bureaus regarding the surveillance of Chinese dissidents abroad remains unclear.

Provincial bureaus in the state security system

Provincial-level bodies have played an important role in the state security system overseen by the MSS since the creation of this ministry in **1983**. Prior to the MSS, state security and intelligence were carried out by the MPS and the Central Investigation Department.

Despite being part of a national security policy, **province-level governments incorporate provincial agencies**, which have their own missions and priorities. Identifying their particularities is therefore very insightful to understand their role in state-sponsored cyber operations. Indeed, cyber operations attributed to the MSS are linked to MSS-provincial bureaus rather than the central organ. The **fact that provinces carry out operations is coherent with the fact that, in terms of capacities, provincial state security agencies have a personnel which is approximately ten times larger than that of the MSS.**

The missions of the provinces are **guided by their geographical specialisation**, which seems to be influenced by their links with other countries, due to specific socio-economic or cultural dynamics, for example. In the 1980's, provincial state security bureaus integrated previous structures responsible for foreign intelligence such as Investigation departments, counterintelligence units of the MPS, United Front Work Department officials and SIGINT military units. It allowed the transmission of expertise.

Prior to MSS creation, MPS bureaus were responsible for foreign intelligence. Therefore, after 1983, MPS intelligence units remained in place in some provinces (Yunnan, Shanghai, Liaoning, Guangdong) and were not replaced by state security agencies. It can explain MPS cyber operations against foreign targets and overlaps with MSS activity.

The I-SOON leaks revealed **provinces are not the only level contracting with private companies** to conduct cyber operations. Indeed, **city-level entities were also numerous to pass contracts** with the company. It can indicate an important degree of autonomy regarding cyber operations for Chinese administrative entities, and also important internal competencies in this field, even at the city-level for police purposes.

Distribution of roles between the PLA and the MSS

The PLA is sharing prerogatives regarding cyber operations against foreign entities with the MSS. Still, since the 2015 PLA reform, ***malicious cyber activity attributed to MSS-sponsored entities increased, while activity attributed to the PLA depleted****. There is no clear evidence to explain this trend, but several hypotheses are possible.*

Several hypotheses can explain this observation:

> The first hypothesis is that the **MSS has taken more responsibility in terms of worldwide cyber espionage campaigns since the reforms of the PLA**. The reorganisation of military capabilities in 2015 and 2024 may have led PLA units to focus on specific targets linked to war operations.

> The second hypothesis is that **PLA-sponsored intrusion sets are less visible** to analyses based on open-source information.

> This can be explained by the possibility that PLA units focus on defence entities and high-level government profiles, which are less likely to disclose publicly when they are targeted.

> It can also be justified by the fact that PLA-sponsored attack campaigns have a higher level of sophistication and of discretion, which led to less detection and then, less reports on this type of threat.

> The third hypothesis is that **newly found malicious cyber campaigns attributed to China are difficult to attribute to a specific intrusion set or unit** due to the lack of distinctive technical evidence, to the overlap between different units operating on the same infected network and to the complexity of the offensive Chinese cyber ecosystem involving state entities and private companies.

According to Sekoia's observations, it seems the **PLA cyber operations are focusing on specific war objectives, whereas the MSS has become the main CCP organ to conduct strategic cyber operations and operates over a broader spectrum**. However, the information currently available does not allow Sekoia to assess the extent to which the MSS and the PLA coordinate in peacetime.

双

Part two

Communities of Patriotic hackers

In addition to traditional Chinese state actors involved in cyber offensive operations, civilian actors also play an important role. This role is highlighted by **the historical involvement of patriotic hackers in offensive campaigns** and the professionalisation of their activities within Chinese companies.

This section will focus on how patriotic hackers played a role in shaping the Chinese offensive cyber ecosystem from 1990's to the present. It will dive into the evolution of the activities of first Chinese communities of hackers from conducting hacktivist and lucrative campaigns, to taking part in state-sponsored operations and integrating the private sector.

From hacktivism…

This section will explore the activity of the first Chinese hacker communities and their use of cyber means to defend China against perceived rival countries. It illustrated the **important patriotism among Chinese hackers**, which helps to understand their progressive rapprochement with state-sponsored operations.

Patriotic hackers' taking part into 'cyber wars'

> *In the 1990's and at the beginning of the 2000's, Chinese citizens accessed the Internet with the launch of the first Chinese Internet Service Provider ChinaNet in 1995. This led to the creation of communities of hackers, motivated by a taste for challenge and patriotism, and who conducted hacktivist campaigns to defend their country against perceived rivals.*

Between 1997, with the creation of the **Green Army**, the first community of Chinese hackers, and 2002, patriotic hackers conducted hacktivist campaigns against foreign targets. Their campaigns were fueled by **nationalism** (Honker Union, hack4[.]com), the **taste for challenge and money** (NCPH). In 2001, they defaced American websites in reaction to the collusion between an American reconnaissance airplane (EP-3E) and a Chinese fighter jet in the South China Sea. Even if these attacks were more symbolic than disruptive, they highlighted the **spontaneous engagement of patriotic hackers to defend their country**, without necessarily the coordination of the government. During this period, the PRC government hailed Chinese hacker groups' activities.

Patriotic hackers constituted groups aiming at defending China's interests back to the early 2000's. The **Green Army**, and then the **Honcker Union** and the **Red Hacker Alliance** were among the first groups of Chinese hacktivists to emerge. These groups were relatively unstructured but constituted a pool of **motivated nationalist hackers** conducting disruptive campaigns for the sake of China. These hackers were patriotic, but they also had a **culture of sharing**, documenting most of their activities and the tools they developed on blogs or forums freely accessible on the Internet.

But since 2002, tolerance for hacktivists' actions waned, leading to the expansion of China's anti-hacking law during the 2009 National People's Congress, as well as the arrest of prominent hackers. Indeed, the Chinese government **began restricting pro-China hacktivists** due to concerns about potential retaliation from a targeted country and interference with state-sponsored operations. It led some hacker communities to evolve into formal information security companies (Black Eagle Base, XFocus), likely to be involved in state-sponsored operations (NSFocus).

Their involvement in state-sponsored operations was encouraged by the principles of the united front and of military-civil fusion.

Chinese strategic principles

The **principle of the United front** is a strategic policy used by the CCP to form alliances with various groups and individuals, both domestically and internationally, to bolster its power and influence. It seeks to unify support for the CCP's goals, even among those who may not fully share its ideology. Originating in the early 20th century, this tactic was initially used to partner with the Nationalists (Kuomintang) to resist Japanese imperialism during the Second Sino-Japanese war (1937-1945). Today, it remains central to Chinese governance and diplomacy, with the United Front Work Department (UFWD) overseeing these efforts, especially under Xi Jinping, who has expanded its focus to international influence, particularly within Chinese diaspora communities.

In addition, the **principle of Military-Civil Fusion (MCF)** refers to the seamless integration of civilian and military resources, aiming to strengthen China's military capabilities by leveraging advances in the private sector, such as technology, research, and infrastructure. Under Xi Jinping's presidency, civil-military fusion has become a central strategy, as it allows China to rapidly enhance its defence sector by tapping into private industry innovations. Xi has elevated MCF to a national strategy to close the technological gap with the US and ensure that private advancements directly support the PLA.

Key figures of hacker communities

Patriotic hackers shared their activity on blogs and forums, taking part in communities. Some of these groups gained recognition for their ***involvement in hacktivist campaigns*** *and for the* ***significant influence some of their members*** *had on China's offensive cyber capabilities.*

An example of a key figure of patriotic hackers is **Tan Dailin, also known as Wicked Rose**. He started as a member of the Green Army during university and created the Network Crack Program Hacker Group (NCPH). Dailin conducted DDoS campaigns of attacks against the US in 2001 in retaliation to the Hainan Island collusion between American and Chinese planes and **was later recruited by the PLA in 2005 in Chengdu**. In 2006, an operation against the US Department of Defense was attributed to APT1, which is linked to NCPH. In 2020, **Tan Dailin was associated with APT41**, a Chinese state-sponsored group linked to the MSS.

Tan Dailin's example highlights the **merger between civilian patriotic hackers and state sponsored units conducting cyber operations for China's strategic interests**. It also demonstrates the recruitment of civilian hackers very early, when they are still students in Chinese universities. This involvement of universities and the research community in educational establishments in state-sponsored operations has been proved by the past, with cyber campaigns attributed to Chinese universities, and is still relevant, as it was pointed out by the **Sophos investigation 'Pacific Rim'.**

Other prominent patriotic hackers emerged at the beginning of the 2000's, such as **Gong Wei** (Goodwell), who founded the Green Army, Cold Face and WZH from NCPH, or **Li0n**, who founded the Honker Union. The **Honker Union** was created in the 1990's in reaction to geopolitical events such as anti-Chinese riots in Indonesia in 1998, the bombing of the Chinese Embassy in Belgrade by NATO in 1999, and the collusion between an EP-3 US spy plane and a J8 Chinese jet fighter near to the Hainan Island in 2001. This community exchanged on a forum and continued to operate at least until 2010, when it reacted in retaliation to Iranian Cyber Army hijacking the DNS records of Baidu. Hackers of the Honker Union developed a hacking tool called **HTran**, which was used for hacktivist activities and by historical intrusion sets like APT1, APT12, and DragonOK.

Another recent example is **Wu Haibo** (aka. shutdown), the CEO of I-SOON, a Chinese IT company that leaked more than 500 internal documents in 2024. Wu Haibo was part of the Green Army, and declared himself a patriotic "red hacker", offering its services to the CCP to defend China. In 2010, he created the first of the three branches of I-SOON in Shanghai. The 2024 I-SOON leaked revealed the company is outsourcing offensive cyber capabilities for the MSS, the MPS, and the PLA.

…To state-sponsored operations.

This section will focus on the post-2002 patriotic hackers' activity, when these communities **progressively became less active** and stopped conducting hacktivist campaigns against perceived enemies of China. They likely focused on cybercrime activities for personal financial gain, or took part in state-sponsored operations by developing malicious payloads or by conducting the campaign.

Integration of patriotic hackers into state capabilities

> *Patriotic hacker communities progressively became less active in conducting hacktivists campaigns due to restrictions imposed by the CCP. The Party adopted a strategy, which consists in enhancing the control over patriotic hackers' activities while taking advantage of their skills to conduct state-sponsored operations. Several of these hackers have joined MSS units or Chinese IT companies that subcontract offensive cyber services for the CCP.*

In the 2000's, militias to support military operations were created, involving personnel of Chinese IT companies. At the same time, hacker communities conducted disruptive operations against foreign targets in the US, Japan, the Philippines, South Korea, Taiwan and Indonesia in retaliation to perceived threats to China's interests. Looking at Tan Dailin story, some hackers of these Chinese hacktivist groups were close to PLA units as, for his case, he was both part of the Chendgu Militia and of the NCPH collective. This proximity can explain the **use of malicious tools developed by patriotic hackers in state sponsored operations.**

Patriotic hackers developing malicious payloads used in state sponsored operations

Patriotic hackers had connections with cyber offensive units related to the PLA or the State Council. It led to their **development of malicious payloads used in state-sponsored cyber operations**. Great examples are **PlugX** and its successor, **ShadowPad**.

PlugX is a Remote Access Trojan firstly discovered in 2008, during a campaign targeting government entities and an organisation in Japan. Active since at least 2012, this malware has been largely used under different variants by intrusion sets associated with front companies linked to the MSS. PlugX was developed by **Zhao Jibin (WHG)**, a close affiliate of Tan Dailin, who was central in the development of the NCPH rootkit GinWui, used by the group to compromise US entities in 2006's targeted campaigns.

ShadowPad is a modular malware platform developed by Tan Dailin and used by MSS fronts and PLA units to conduct strategic cyber operations. It was used for espionage by at least four intrusion sets associated with China. It emerged in 2015, and was quickly adopted by state-sponsored intrusion sets, which stop developing their own backdoors, significantly reducing the cost of their cyber operations. ShadowPad was sold to a limited set of customers and highlighted the role and the benefits of involving private contractors in state-sponsored operations.

Parallel activities: cybercrime

> *In parallel to their involvement in state-sponsored operations, Chinese hackers also conduct lucrative campaigns for their own benefit. The CCP likely turned a blind eye on this activity despite national laws prohibiting cybercrime.*

Chinese hackers were also involved in **cybercriminal activities** and **developed several open source malicious payloads** that are still in use today, notably for illegal cryptocurrency mining. These lucrative campaigns are used for personal gain and, to a lesser extent, to fund the activities of hacker communities.

Due to the involvement of patriotic hackers in state-sponsored operations and their technical skills, the **MSS likely turned a blind eye to their cybercrime campaigns**. For instance, APT41 (aka. Winnti, BARIUM, Earth Baku) was observed conducting both cyber espionage and lucrative operations, sometimes re-using tools and malware of strategic operations for financial gain. Recently, ChamelGang APT, active since at least 2021, was observed conducting both cyber espionage operations and lucrative campaigns. In particular, it used the CatB ransomware for financial gain.

sekoia | Chinese APT conducting cybercrime activities

Threat actor	Targeted entities	Cybercrime activity	Motivations
APT41 *sub cluster* BARIUM *sub cluster* Chendgu 404	Gaming Industry in East and Southeast Asia	Ransomware	Lucrative and Disruption for political purposes
APT19	US companies	Ransomware	Lucrative
ChamelGang	Healthcare and Government in India and Brazil	CatB ransomware	Financial gain, disruption, misattribution, removal of evidence
Bronze Starlight	Gambling, manufacturing, financial services, engineering, legal, business services, travel and tourism	NightSky Ransomware	Financial gain, covering Espionage

Lucrative operations likely serve as a complement of revenue for Chinese hackers, who do not earn a significant income in the majority of cases. They mainly target **sectors of activities prohibited in China**, such as gambling and cryptocurrency industry, **gaming industry**, or **the five poisons** in order to protect their illegal activity against state retaliation.

Part three

The current hack-for-hire ecosystem

The Chinese hack-for-hire ecosystem observed today is partly inherited from the activities of patriotic hackers, who were **involved in state-sponsored programs to conduct cyber operations, developed offensive tools, and work in IT companies outsourcing services for state-sponsored operations.** It reinforces the proximity between state and private actors, which is at the root of this ecosystem.

This section will explore the outsourcing of offensive cyber services to private companies by state actors and the development of Chinese IT companies, which constitute a pool of resources for state-sponsored operations.

Ministries outsourcing offensive operations

This section aims at analysing the **outsourcing of offensive cyber capabilities** to Chinese private companies by state actors. The analysis is mainly based on the recent leaks from the company I-SOON and on the attribution of Chinese companies involved in state sponsored operations. It dives into the process of vulnerability reporting organised and controlled by the CCP, which serves to weaponize vulnerabilities found by civilian contributors for cyber operations.

Lessons from the I-SOON leaks

The I-SOON leaks ***highlighted the outsourcing of state-sponsored operations*** *conducted by the MSS and the MPS.* ***Lists of clients*** *of the company were leaked, as well as* ***internal conversations*** *about deals, the distribution of vulnerabilities found during hacking contests and the relationship between Chinese IT companies.*

In February 2024, leaked documents from the **Sichuan branch of the Chinese company I-SOON** were found on a Github repository. Sichuan I-SOON, also called I-SOON, is an IT security services company conducting R&D and penetration testing activities. It is located in Chengdu, a known cybersecurity hub in China. Since then, I-SOON is characterised as **providing hacker-for-hire services for Chinese authorities.**

The leaks came from the Sichuan branch of Shanghai I-SOON Information Technology founded in 2010. Alongside Sichuan i-SOON, the parent company oversees three other subsidiaries and maintains offices in Nanjing (Jiangsu Province), Taizhou (Zhejiang Province), and Ningbo (Zhejiang Province).

Wu Haibo (aka shutd0wn), the CEO of I-SOON and affiliated companies, has a background as a "patriotic hacker" in the Green Army. The company's stated culture reflected his past, claiming a direction to evolve into a robust national defence reserve with a profound sense of political responsibility and allegiance to the Party and the People.

The I-SOON leaks revealed important details about China's **hack-for-hire system.** Lists of clients were leaked, helping to understand partly how state actors outsource services for their operations. The **way to rely on a private company for cyber operations seems to differ** depending on the government contractor. Indeed, distinct patterns can be observed when comparing PLA, MPS and MSS's way of outsourcing cyber campaigns.

The I-SOON leaks of February 2024 contained a list of contracts passed with many Chinese public entities, revealing part of the clients of its hack-for-hire services. Among them 66 contracts out of 120 were dedicated to provincial and city-level MPS entities, 22 to MSS entities, while **only one contract was signed with the PLA.** The 31 left were passed with research institutes, universities, state-owned enterprises, and other government entities.

Therefore, PLA units seem to rely less on private contractors to conduct cyber operations. In contrast, the **MSS and MPS are more likely relying on private companies** for cyber operations - the MPS passing a larger amount of contracts for hack-for-hire services from Chinese companies compared to the MSS. **An hypothesis is that MSS entities rely also on front companies**, which directly pass contracts with subcontractors.

Another interesting information from the I-SOON leaks is the **degree of cooperation and proximity** between Chinese tech companies. In a leaked list of I-SOON contracts, 50% of the customers were other tech companies similar to I-SOON. **It illustrates how I-SOON also acts as a supplier,** addressing not exclusively end users. It also demonstrates how Chinese companies can share their tools and services for a price, despite being competitors on the same market. In leaked internal communication of I-SOON, there were discussions about buying Linux Trojan malware to another Chinese company and how much an exploit for a QQ vulnerability would cost.

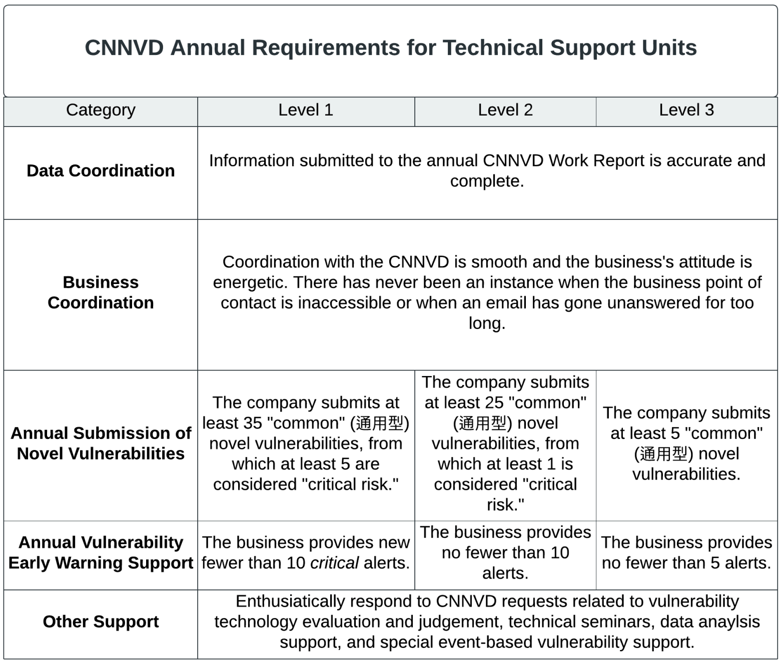
Weaponization of vulnerabilities

> *The I-SOON leaks also highlight the **distribution of vulnerabilities discovered during Chinese hacking contests, such as the Tianfu Cup, among private contractors.** They demonstrate that the **process of vulnerability reporting** in China is a key element for the weaponisation of vulnerabilities to conduct state-sponsored cyber operations.*

In the I-SOON leaks, internal conversations showed that **vulnerabilities from Chinese hacking contests, such as the Tianfu Cup and the Matrix Cup, are distributed among private contractors by ministries**. Indeed, Ministries have played an important role since 2021 in collecting vulnerabilities from researchers and companies and sharing them among the ecosystem to turn them into exploits.

The MSS 13th bureau, also called the China Information Technology Security Evaluation Center (CNITSEC), is responsible for operating the China National Vulnerability Database (CNNVD), which serves to collect non-publicly disclosed vulnerabilities from Chinese companies and researchers. The vulnerabilities reported and collected within the CNNVD are then used for MSS cyber operations and can be distributed among MSS partners, including front and private companies.

To contribute to vulnerability collection by the MSS, enterprises have to apply to become **“technical support units” (TSU) of this ministry**. Three levels exist, with different requirements, especially in terms of vulnerabilities to report each year and their criticality**. In 2024, 292 companies** were listed as technical support units of the MSS. They were 151 in 2023, and only 15 in 2016.



CNNVD Annual Requirements for Technical Support Units

Category	Level 1	Level 2	Level 3
Data Coordination	Information submitted to the annual CNNVD Work Report is accurate and complete.		
Business Coordination	Coordination with the CNNVD is smooth and the business's attitude is energetic. There has never been an instance when the business point of contact is inaccessible or when an email has gone unanswered for too long.		
Annual Submission of Novel Vulnerabilities	The company submits at least 35 "common" (通用型) novel vulnerabilities, from which at least 5 are considered "critical risk."	The company submits at least 25 "common" (通用型) novel vulnerabilities, from which at least 1 is considered "critical risk."	The company submits at least 5 "common" (通用型) novel vulnerabilities.
Annual Vulnerability Early Warning Support	The business provides new fewer than 10 *critical* alerts.	The business provides no fewer than 10 alerts.	The business provides no fewer than 5 alerts.
Other Support	Enthusiatically respond to CNNVD requests related to vulnerability technology evaluation and judgement, technical seminars, data anaylsis support, and special event-based vulnerability support.		

Source: Sleight of hand: How China weaponizes software vulnerabilities - Atlantic Council

Based on the Annual Requirements for TSUs and the number of TSUs in 2024, this means that **at least 3530 "common" novel vulnerabilities, and 219 vulnerabilities considered as "critical risk" would have been submitted to the CNNVD this year.** The incentives for companies to participate in vulnerability reporting are unclear, as identifying security flaws incurs costs for them. Several companies with the MSS status of "Level-1" TSU are known for conducting state-sponsored operations, such as **NSFocus, TopSec and Integrity Technology.**

The security flaws can be directly collected by the MSS, but can also come from the NVDB, operated by the Ministry of Industry and Information Technology (MIIT), and the China National information Security Vulnerability Sharing Platform (CNVD), operated by the CNCERT/CC.

The **MPS also manages its own vulnerabilities database** called the National Cyber and Information Security Information Notification Centre, which benefits from vulnerabilities collected through the NVDB of the MIIT.

Chinese regulation for vulnerability management

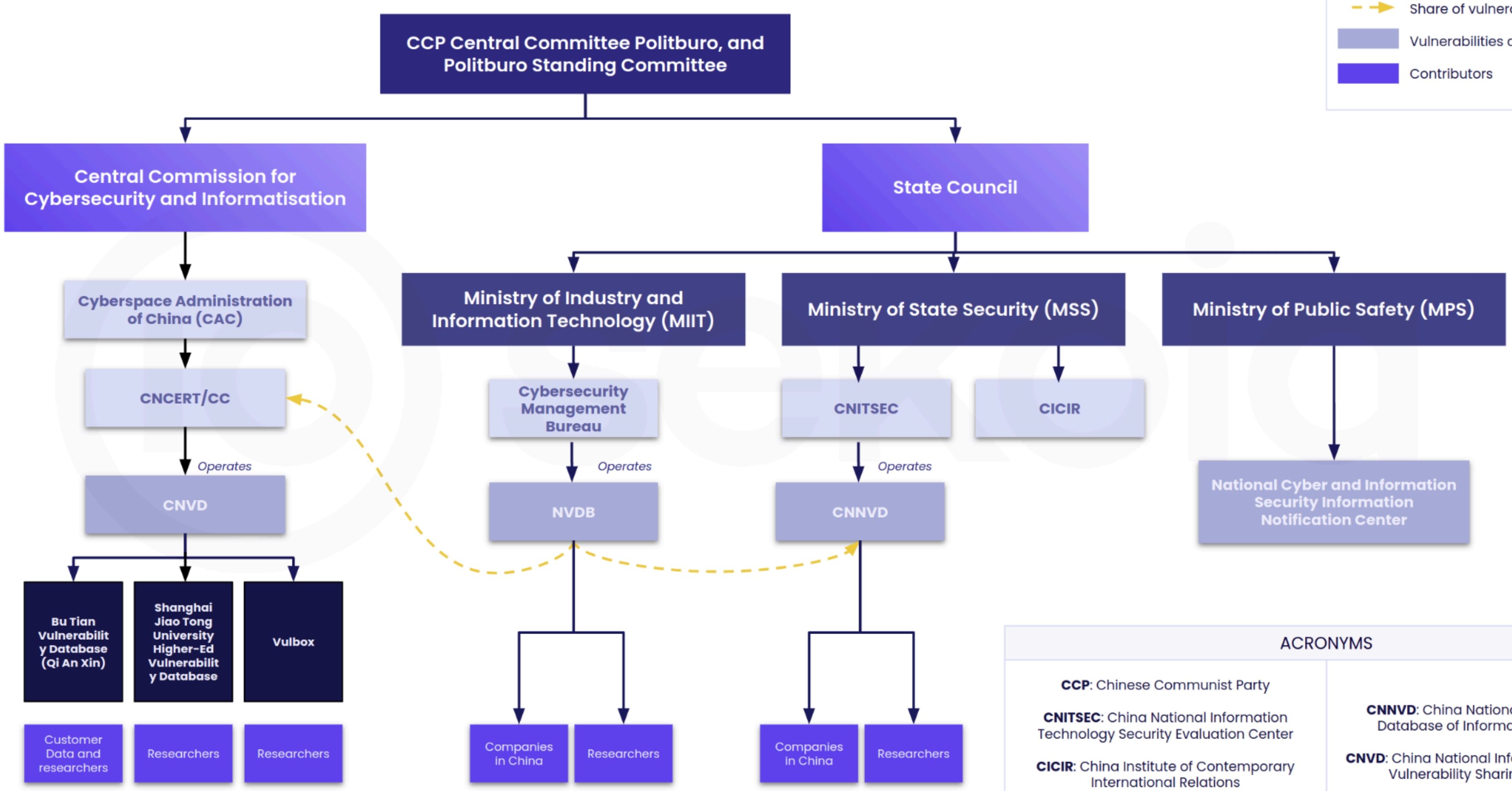
In 2021, the **"Regulations on the Management of Network Product Security Vulnerabilities" (RMSV) law** was passed, requiring any security flaw to be reported within 48 hours to the MIIT database, the **Cybersecurity Threat and Vulnerability Information Sharing Platform (NVDB)**. These regulations move away **from responsible disclosure processes and leave the publication of collected vulnerabilities to the discretion of the CCP**. Vulnerabilities and proof-of-concepts collected through the NVDB are then shared with CNCERT/CC and the Ministry of Public Security (MPS), and civilian partners.

The RMSV solidifies a **trend observed since 2018**, when the Notice on regulating the promotion of cybersecurity competitions was adopted, restricting Chinese researchers from participating in international hacking competitions. The purpose of this law was **to ensure vulnerabilities are exclusive for use by intelligence agencies and military forces** supporting CCP's interests. Indeed, zero-day vulnerabilities enable attackers to exploit flaws in software to breach adversary systems and achieve strategic objectives. As long as they are unreported, these vulnerabilities are unknown to the vendor, leaving no patch available to protect the software from malicious exploitation. Yet, because software companies quickly release patches to fix newly found security flaws, the value of stored vulnerabilities diminishes rapidly unless they are continuously replenished with newly discovered ones. This can explain some requirements to maintain the status of Level-1 TSU.

Vulnerability disclosure ecosystem

LEGEND

- ➜ Share of vulnerabilities
- ▨ Vulnerabilities databases
- ■ Contributors


CCP Central Committee Politburo, and Politburo Standing Committee
Central Commission for Cybersecurity and Informatisation
State Council
Cyberspace Administration of China (CAC)
Ministry of Industry and Information Technology (MIIT)
Ministry of State Security (MSS)
Ministry of Public Safety (MPS)
CNCERT/CC
Cybersecurity Management Bureau
CNITSEC
CICIR
Operates
CNVD
Operates
NVDB
Operates
CNNVD
National Cyber and Information Security Information Notification Center
Bu Tian Vulnerability Database (Qi An Xin)
Shanghai Jiao Tong University Higher-Ed Vulnerability Database
Vulbox
Customer Data and researchers
Researchers
Researchers
Companies in China
Researchers
Companies in China
Researchers

ACRONYMS

CCP: Chinese Communist Party

CNITSEC: China National Information Technology Security Evaluation Center

CICIR: China Institute of Contemporary International Relations

CNCERT/CC: National Computer Network Emergency Response Technical Team/Coordination Center of China

CNNVD: China National Vulnerability Database of Information Security

CNVD: China National Information Security Vulnerability Sharing Platform

NVDB: Cybersecurity Threat and Vulnerability Information Sharing Platform

Source: Sleight of hand: How China weaponizes software vulnerabilities - Atlantic Council

Development of the Chinese IT industry

The outsourcing of cyber capabilities in the private sectors by state actors is **boosted by the process of vulnerability reporting controlled by the CCP**. This process helps for the **weaponization** of vulnerabilities by sharing them among the community to turn them into exploits. Contributors to this process, such as researchers and companies, are key elements for its effectiveness.

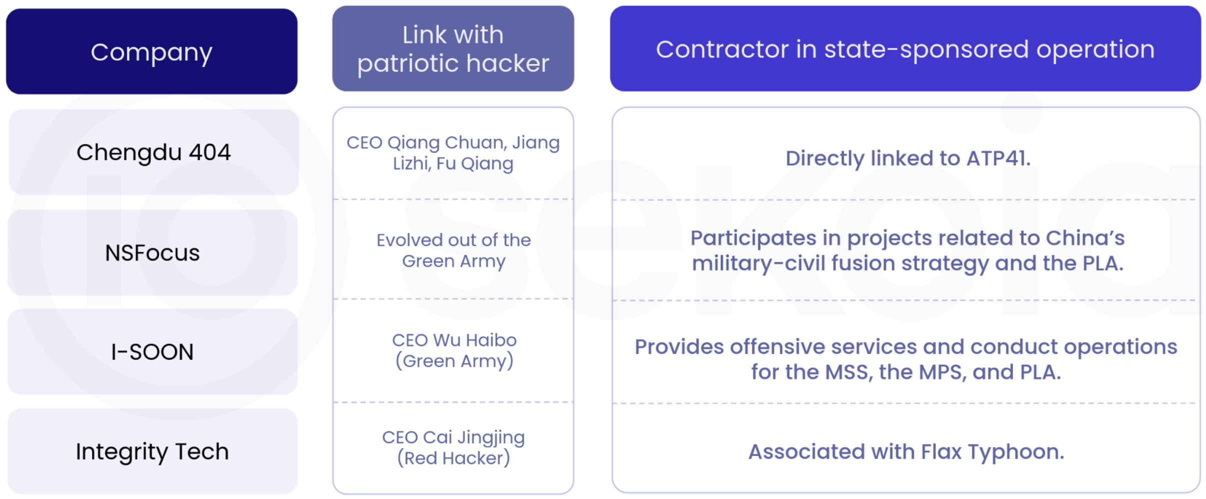
Therefore, this section will focus on the development of Chinese IT companies since 2002, accompanied by the professionalisation of patriotic hackers, and by members of Chinese hacker teams. It will also explain how the employees of these companies are recruited from universities to provide the necessary workforce.

Creation of companies

Starting in 2002, the Chinese government ***began restricting pro-China hacktivists*** *due to concerns about potential retaliation from a targeted country and interference with state-sponsored operations. This led patriotic hacker communities to either dissolve, rebrand to focus on government-approved targets, or* ***evolve into private companies****. The trend intensified since 2015 when successive "Clean-up the Internet" campaigns were launched by the CCP, which included arrests of Chinese hackers for illegal activities. These private companies subsequently became* ***a resource pool for state-sponsored cyber operations.***

It led to the creation of major Chinese IT companies **between 1990's and at the beginning of the 2000's**, such as **NSFocus, Alibaba, Tencent, Qihoo 360**, which were founded by early Chinese hackers and engaged in Military-Civil Fusion. These companies are suspected to cooperate with state entities **by discovering critical vulnerabilities, which are weaponised and used in state-sponsored operations**. For instance, Qihoo 360 researchers discovered a critical zero-day vulnerability in 2018, which was exploited one month later by APT40, known for being associated with the MSS. Several high technology Chinese companies also receive **funds from the PLA for specific programs dedicated to R&D and computer network operations expertise**, such as Huawei, ZTE Corp, NSFocus, and Venus Technologies.

| Patriotic hackers creating IT companies



Company	Link with patriotic hacker	Contractor in state-sponsored operation
Chengdu 404	CEO Qiang Chuan, Jiang Lizhi, Fu Qiang	Directly linked to ATP41.
NSFocus	Evolved out of the Green Army	Participates in projects related to China's military-civil fusion strategy and the PLA.
I-SOON	CEO Wu Haibo (Green Army)	Provides offensive services and conduct operations for the MSS, the MPS, and PLA.
Integrity Tech	CEO Cai Jingjing (Red Hacker)	Associated with Flax Typhoon.

Starting from 2013, IT companies development has been especially guided by Xi Jinping's desire to strengthen China's self-sufficiency in advanced technologies, as illustrated by the Made in China 2025 Plan, and its desire to increase China's economic weight in the global economy. This objective was supported in part by the **BATX (Baidu, Alibaba, Tencent, Xiaomi)** and by five-year plans encouraging **Chine**se big data industry and development based on quality and innovation, rather than exports and foreign investment.

It has also led to the growing participation and performance of Chinese hacking teams in international hacking competitions (DEFCON, Pwn2Own). These teams were usually attached to universities (Tsinghua, Jiangsu, Zhejiang) and major technology companies (Huawei, Tencent, Qihoo360). **Retired members of these teams joined tech giants or created their own companies**, leading to a growing number of smaller Chinese enterprises providing cybersecurity and vulnerability research services, and the creation of a remarkably robust and comprehensive hacking contest ecosystem.

These companies often provided services such as cyber ranges or vulnerability research, such as Saining Network, Cyber Kunlun, Chaitin Tech, with business priorities aligning with state capacity development.

Cyber operations services and surveillance is a lucrative market

In 2018, the CCP adopted the Notice on regulating the promotion of cybersecurity competitions, a directive banning Chinese hackers from taking part in hacking competitions abroad. This measure aims to ensure that the discovery of these hackers remains China's property and gives Beijing a strategic advantage.

One hypothesis is that this **directive has encouraged members of Chinese hacker teams to find new sources of income** by participating in **Chinese exploit contests**, such as the Tianfu Cup or the Matrix Cup, or **creating their own start-ups** in response to state requests to outsource cyber operations or surveillance.

Indeed, with the increasing use of technology to monitor their population, Chinese administrations are making this a particularly lucrative market.

These companies focusing on niche digital services are part of a **second wave** of Chinese IT companies' creation. They were often branches of larger companies before becoming independent entities, with members of the hacking team attached to a tech giant launching their own start-up.

They are also **suspected to be involved in state-sponsored operations**. For instance, Qi An Xin is a leader in the cybersecurity industry and was initially part of Qihoo 360 under the name of 360 ESG until 2019. Qi An Xin has close ties with the CCP: it is partly owned by the state-owned enterprise China Electronics Corporation, has been mandated to ensure the cybersecurity of the Beijing Winter Olympics 2022, is a level-1 Technical Support Unit and manages its own vulnerability database, Bu Tian Vulnerability Database. In addition, it is also one of main I-SOON's contractors and investors, a Chinese company involved in state-sponsored espionage operations.

Recruitment in universities

*Universities play an essential role in training and recruiting talents to conduct state-sponsored operations. They also have **research labs participating in the reporting of vulnerabilities** and in the development of offensive capabilities. Finally, they also organise hacking contests to train students and create emulation among the Chinese hackers community.*

In the 2000's, many patriotic hackers came from Chinese universities and were recruited for state-sponsored operations, while still being students. Even today, front companies still post job advertisements on university websites, searching for offensive skills students speaking a foreign language. As stated before, Tan Dailin is a great example of a patriotic hacker being spotted as a student and making a career in offensive cyber operations.

Today, Technical Support Units (TSU) operating for the state compete to recruit the best talents and worry about their skilled engineers leaving the company. In the I-SOON leaks, executives complained about Qi An Xin, another Chinese tech company, trying to attract experienced engineers to recruit them. They also revealed in their conversation that they passed an agreement with Chengdu 404, another Chinese tech company, to not steal talents from each other.

In a 2024 article, Intrusion Truth explained that **graduates from tech schools saturate the Chinese job market**. However, the I-SOON leaks gave a much more **nuanced vision** of employee profiles working for these companies. It revealed that less than 27% of I-SOON employees had an academic degree, indicating that **hackers of some Chinese hack-for-hire companies are not necessarily graduated students from universities** but **rather hackers with practical experience**.

This case cannot be generalised to all Chinese companies operating on the market of cyber ranges, like I-SOON, as this company can be considered as a Level-3 TSU providing less sophisticated services for state-sponsored operations. However, it showed that Chinese tech school students are not necessarily in majority in companies operating for MSS and MPS.

Conclusion

Many actors appear to be involved in state-sponsored cyber operations in the Chinese cyber offensive ecosystem. It ranges from the conduct of operations, the sale of stolen information or initial access to compromised devices to providing services and tools to launch attacks. The **relationships between these military, institutional and civilian players are complementary** and strengthened by the proximity of the individuals part of these different players and the CCP's policy.

Chinese cyber capabilities started to develop within the PLA, with the creation of departments dedicated to information warfare, and among the population with the structuration of patriotic hackers communities in the 1990’s. With changing CCP policies regarding civilian hacker activities, members of these communities have supported China’s cyber capabilities in different ways. Many have either founded or joined IT companies, or collaborated with state actors to develop offensive tools and conduct state-sponsored cyber operations.

When Xi Jinping came into power, he **turned the principle of Military-Civil Fusion into a national strateg**y to make China a “cyber powerhouse”. It led to major reforms of the PLA in 2015 and 2024 and the adoption of important laws regarding Chinese hackers and vulnerability disclosure, including the Notice on regulating the promotion of cybersecurity competitions or the RMSV. Chinese state-sponsored operations evolved towards **more discretion and larger scales of targets**. Attribution also became harder, with the appearance of new clusters of activity, while historical China-nexus APTs disappeared. **APTs attributed to the PLA were less visible, while APTs related to the MSS, often relying on front companies or Chinese IT businesses, became most common in investigation reports.**

Sekoia assesses that paying **attention to the content of strategic plans and the activity of Chinese IT companies**, especially in terms of research of vulnerability, is likely to help anticipate state-sponsored operations against specific countries or sectors of activity. The different roles of provinces in the conduct of state-sponsored cyber operations and the degree of involvement of private actors are also topics that should be investigated more deeply to improve our understanding of the Chinese cyber threat.

The role of private companies in state-sponsored operations raises a question about the current model of clusterization used in cyber threat intelligence. Indeed, this model is based on trying to associate a cluster of malicious activity to a concrete entity, helping to understand the motivations for an attack and to assess the cyber capabilities of states. Regarding state-sponsored operations, these clusters are often associated with government or military units. However, with China using private companies to conduct part of their operations, the **attribution game** has increased in difficulty. Indeed, I-SOON leaks highlighted that several units related to the PCC can rely on a similar service or platform sold by a private company to conduct an operation.

Therefore, it may be relevant to consider that a China-nexus APT is likely to be a **mix of private and state actors cooperating** to conduct an operation, rather than strictly being associated with a specific unit.

List of references

"A comprehensive analysis of I-Soon's commercial offering" - *Harfang Lab*, March 2024

"A Survey of Reported Chinese Espionage, 2000 to the Present" - *CSIS*, Mach 2023

"Adam Kozy Testimony" - Adam Kozy, February 2022

"A Addis-Abeba, le siège de l'Union africaine espionné par Pékin" - *Le Monde*, Ghalia Kadiri and Joan Tilouine, January 2018

"APT41: Dual Espionage and Cyber Crime Operation" - *Mandiant*, August 2019

"Business Priorities of Chinese Cyber Range Providers Go Hand in Hand with State Cyber Capability Development" - *Natto Thoughts*, Eugenio Benincasa and Dakota Cary, October 2024

" Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" - *National Security Archive*, Bryan Krekel and Northrop Grumman, October 2009

"Capture the (red) flag: An inside look into China's hacking contest ecosystem" - *Atlantic Council*, Eugenio Benincasa and Dakota Cary, October 2024

"CCleanup: A Vast Number of Machines at Risk" - *Cisco Talos*, Edmund Brumaghin, Warren Mercer, Craig Williams, September 2017

"China's 2021 anti-privacy operation helps clean up cyberspace" - Xinhua, September 2021

"China's Military Cyber Operations" - *BlackHat Asia 2024*, Pukhraj Singh, April 2024

"China turns to private hackers as it cracks down on online activists on Tiananmen Square anniversary" - *University of Maryland, Baltimore County (UMBC)*, Christopher K. Tong, June 2024

"Chinese APTs: Interlinked networks and side hustles" - *Intrusion Truth*, July 2022

"Chinese Tactics" - US Department of the Army, August 2021

"Demand for qualified experts rises as companies look to protect themselves" - *Chinadaily*, Cao Yin, November 2021

"DodgeBox: A deep dive into the updated arsenal of APT41 | Part 1" - *Zscaler*, Yin Hong Chang, Sudeep Singh, July 2024

"Feature: Qi-Anxin: A Chinese cybersecurity guardian" - *Xinhua*, August 2024

"Front Company or Real Business in China's Cyber Operations" - *Natto Thoughts*, May 2024

"From Vegas to Chengdu: Hacking contests, Bug bounties, and China's Offensive Cyber Ecosystem" - CSS ETH Zürich, Eugenio Benincasa, June 2024

"From World Champions to State Assets: The Outsized Impact of a Few Chinese Hackers" - *War on the Rocks*, Eugenio Benincasa, September 2024

"Gaming Public Opinion" - *Australian Strategic Policy Institute (ASPI)*, Albert Zhang, Tilla Hoja, Jasmine Latimore, April 2023

"Hotspot Analysis A one-sided Affair: Japan and the People's Republic of China in Cyberspace" - *CSS CYBER DEFENSE PROJECT, ETH Zürich*, Stefan Soesanto, January 2020

"Intervention 60525: China: Internet 'Clean-up' Policy announced" - *Global Trade Alert*, January 2017

"Is the CCP the biggest APT?" - *Intrusion Truth*, August 2024 "i-SOON: Kicking off the Year of the Dragon with Good Luck … or Not", *Natto Thoughts*, February 2024

"John Chen Testimony" - *Center For Intelligence Research and Analysis*, John Chen, February 2022

"Made in China 2025" - *Institute for Security and Development Policy*, June 2018

"Matrix Cup: Cultivating Top Hacking Talent, Keeping Close Hold on Results" - *Natto Thoughts*, Eugenio Benincasa and Natto Team, July 2024

"40 Officers of China's National Police Charged in Transnational Repression Schemes Targeting U.S. Residents | United States Department of Justice" - *United States Department of Justice*, April 2023

"Operation Crimson Palace: Sophos threat hunting unveils multiple clusters of Chinese state-sponsored activity targeting Southeast Asian government" - *Sophos*, Paul Jaramillo, Morgan Demboski, Mark Parsons, Sean Gallagher, June 2024

"Operation ShadowHammer: A High Profile Supply Chain Attack" - *Securelist*, GREAT, AMR, April 2019

"President Xi Jinping warns of disaster if Sino-US relations sour" - *SCMP*, Teddy Ng, Kwong Man-ki, July 2014

"Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally | United States Department of Justice" - *United States Department of Justice*, September 2020

"Shadowpad - a Masterpiece of Privately Sold Malware In Chinese Espionage" - *SentinelLABS*, Yi-Jhen Hsieh, Joey Chen, August 2021

"Sleight of hand: How China weaponizes software vulnerabilities" - *Atlantic Council*, Dakota Cary and Kristin Del Rosso, September 2023

"State Security Departments: the birth of China's nationwide state security system" - Deserepi, Alex Joske, 2023

"Sophos' Pacific Rim: Defense Against Nation-State Adversaries" - *Sophos*, October 2024

"Technology Support Unit Cooperation Plan" - *CNNVD*

"The old school hackers behind APT41" - *Intrusion Truth*, July 2022

"The PLA Strategic Support Force: A 'Joint' Force for Information Operations" - *Center for Intelligence Research and Analysis*, John Chen, Kieran Green, Joe Mc Reynolds, June 2021

"Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010; Targets Bordering Asian Countries" - *Recorded Future*, Insikt Group, June 2021

"Translation: Notice on Regulating the Promotion of Cybersecurity Competitions" - *Center for Security and Emerging Technology*, May 2021

"Truth and reality with Chinese characteristics" - *Australian Strategic Policy Institute (ASPI)*, Dr. Samantha Hoffman, Tilla Hoja, Yvonne Lau, Lilly Min-Chen Lee, May 2024

"Unmasking CamoFei" - *Team T5*, Still Hsu, Zih-Cing Liao, 2024

"Unplugging PlugX: Sinkholing the PlugX USB worm botnet" - *Sekoia.io,* TDR, Félix Aimé, Charles M., April 2024

"U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage" - *United States Department of Justice*, May 2014

"2023 Strategic Support Force Information Technology Force Direct Recruitment Officers Promotional Brochures" - *Weixin*, March 2023

"Wicked Rose and the NCPH Hacking Group" - Ken Dunham, Jim Melnick, 2012

"Wuhan Xiaoruizhi Class of '19" - *Intrusion Truth* - July 2023

About Sekoia.io TDR team

TDR is the Sekoia Threat Detection & Research team. Created in 2020, TDR provides exclusive Threat Intelligence, including fresh and contextualised IOCs and threat reports for the Sekoia SOC Platform. TDR is also responsible for producing detection materials through a built-in Sigma, Sigma Correlation and Anomaly rules catalogue.

TDR is a team of multidisciplinary and passionate cybersecurity experts, including security researchers, detection engineers, reverse engineers, and technical and strategic threat intelligence analysts.

Threat Intelligence analysts and researchers are looking at state-sponsored & cybercrime threats from a strategic to a technical perspective to track, hunt and detect adversaries. Detection engineers focus on creating and maintaining high-quality detection rules to detect the TTPs most widely exploited by adversaries.

About Sekoia.io

Sekoia.io is the European cybertech, leading provider of Extended Detection and Response (XDR) solutions based on Cyber Threat Intelligence (CTI). Its mission is to provide businesses and public organizations with the best protection technologies against cyber attacks.

By combining threat anticipation through knowledge of attackers (Sekoia Intelligence) with automation of detection and response, the Sekoia SOC platform (Sekoia Defend – XDR) provides security teams a unified view and total control over their information systems. Its interoperability with third-party solutions and compliance with international technical standards enable organizations to take full advantage of their existing technologies.

Sekoia.io gives its customers the means to focus their human resources on high value-added missions, optimize their cyber-defense strategy and regain the advantage against advanced cyber threats.

Find more publications on blog.sekoia.io

Please don’t hesitate to provide your feedback on our publications by clicking here.
You can also contact us at tdr@sekoia.io for further discussions.