NIDS 防衛研究所 National Institute for Defense Studies
Tokyo Japan
NIDS Commentary
Special Feature: Emerging Security Challenges vol. 7
No. 371 April 25, 2025

The Chinese Ministry of Public Security as an External Influence Agency: Recent Covert Operations and Their Internal Logic as Traced through Open-Source Analysis*

Research Fellow, China Division, Regional Studies Department **GOTO Yohei**
Research Fellow, Cyber Security Division, Policy Studies Department **SETO Takashi**

Introduction: Chinese Ministry of Public Security and its expansion of covert operations beyond the boarder.

On March 4, 2025, the U.S. Department of Justice declassified an indictment in the legal case titled "U.S. v. Wu Haibo et al." (hereinafter: the "Wu Haibo Case"). In this case, a total of ten suspects of Chinese nationality are charged with involvement in a series of cyberespionage against various countries from 2016 to 2023. Eight of the defendants are employees of a private cybersecurity company in China who received a commission from a Chinese government agency, but the remaining two are officers from a local agency of the Ministry of Public Security of China (hereinafter referred to as the "Ministry of Public Security,MPS").[1]

The "MPS" referred to here is a collective term for the central government ministries and agencies in charge of China's "domestic" law enforcement and counterintelligence agencies and their local agencies (public security bureaus/public security agencies/public security offices). The MPS, a police organization with an organizational structure which is superficially similar to the relationship between the National Police Agency and prefectural police in Japan, is recognized as one of China's domestic law enforcement agencies and counterintelligence agencies, along with the Ministry of State Security(MSS) and others.

To be fair, several MPS missions have international aspects. Its oversea missions include, for example, dealing with crimes committed by Chinese nationals living overseas (including the repatriation of Chinese nationals abroad who have escaped anti-corruption crackdowns and the recovery of overseas assets) and working with overseas law enforcement agencies on international judicial assistance[2] for the purpose of counterterrorism measures. In addition, it implements joint training and capacity-building support, etc. with security authorities in many countries, including joint patrols with security agencies in Croatia, Laos, Myanmar, Serbia, Thailand, and other countries in the areas covered by the Belt and Road Initiative, and police officer training in the Solomon Islands.[3] These external missions of the MPS have continued to expand, especially since the establishment of the Xi Jinping administration (2012), and there have been many systematic and empirical analyses of their nature and implications.[4]

On the other hand, beyond the activities that fall within the scope of international law-enforcement

cooperation in the previous paragraph, the MPS has also engaged in several covert and clandestine operations beyond its jurisdiction, combining various intelligence collection and influence measures both through physical and cyber domains. The Wu Haibo Case represents one of the good examples of MPS's complex scheme of covert (influence) and clandestine(espionage) operations in recent years. Although they have caught journalistic attention in media coverage, little attention has been paid to systematic and empirical review of the MPS's as an China's national security apparatus and internal logics behind the expansion of their covert and clandestine activities in the foreign countries.

Against these backdrops, this commentary begins with and deep dives into the two-fold questions: (1)"what exactly is the MPS?" and (2) "why has the MPS been involved in covert operations abroad?". The second questions can be paraphrased as "what does explain their internal logic behind growing MPS's involvement to covert operations beyond its border, given it was originally designed and has been operating as a domestic law enforcement and counterintelligence apparatus? ". Reflecting these questions, the structure of the commentary is as follows. First, we summarize the history and mission of the MPS. After that, we will utilize diverse publicly available information (PAI), including declassified judicial documents such as indictments from the U.S. Department of Justice and leaked documents from Chinese private companies, etc., to give a general explanation about the major examples of the MPS's covert operations through physical space and cyberspace in recent years.

1. Overview of the MPS

The MPS was established in 1949 when the People's Republic of China was founded, and although it has undergone several internal organizational reforms, its name and role have not changed significantly since its establishment. Along with the Minister of Foreign Affairs and the Minister of National Defense, etc., the Minister of Public Security also serves as a State Councilor, who is ranked only behind the vice premiers, which shows the high status and importance of the position in the Chinese Communist Party (CCP) and the State Council.[5] In China, government agencies exist in each region in addition to the central institutions, and the public security departments, in order from the highest to lowest level departments, are the MPS at the center, the public security agencies in provinces and autonomous regions, the public security bureaus in cities (including direct-administered municipalities such as Beijing and Shanghai) and counties, and the offices and sub-bureaus established in the lower-level local agencies. The lower-level agencies receive the guidance of the higher-level agencies.[6] The website of the MPS (below this is used as a collective term which includes the lower-level agencies. The same shall apply thereafter unless otherwise necessary) states that its main duties are the investigation of economic offenses, security management, investigation of criminal offenses, preservation of cybersecurity, counterterrorism, crackdowns on illegal drugs, international cooperation, development of legal systems, etc.[7]

It is not made clear on the MPS website, but it is thought that the missions of "investigation of criminal (economic) offenses," "counterterrorism," "preservation of cybersecurity," etc. include not only general

criminal offenses but also investigations of and crackdowns on individuals and organizations which could threaten the rule of the CCP. Actually, the fact that taking charge of such cases with a political flavor is positioned as a high-priority mission has been emphasized at various meetings of the MPS. For example, at the National Public Security Agency and Bureau Directors Meeting held in January 2024, "defense of the nation's political security"[8] was listed as the second most important mission (the most important mission was "implementing the absolute leadership of the CCP"), and the main tasks listed included preventing and cracking down on infiltration, subversion, disruption, and sabotage by external hostile forces, strengthening online struggles including cracking down on political disinformation and harmful information, strengthening counterterrorism and anti-secession activities (anticipating having to deal with "separatist forces" in Taiwan, the Uyghur Autonomous Region, Tibet, Hong Kong, etc.), carrying through the Party's ethnic and religious policies, and cracking down on cult organizations.[9]

It is apparent that the Chinese authorities are attempting to establish a basis for external missions by the MPS in policy documents and a full range of laws concerning national security. For example, the Plan on Building the Rule of Law in China (2020 to 2025) published by the CCP Central Committee in January 2021 stated a policy of taking action on general crimes and threats to the security of the party in the form of cooperation with other countries, including active participation in international cooperation concerning law enforcement, joint efforts to combat violent terrorist forces, ethnic separatist forces, religious extremist forces, drug trafficking, smuggling, and cross-border organized crime, international cooperation on anti-corruption, etc.[10] Furthermore, in laws such as the Cybersecurity Law (2016), the Data Security Law (2021), and the Law on Combating Telecom and Online Fraud (2022), etc. enacted under the Xi administration, clauses are incorporated allowing the MPS ("public security agencies" in the text of the laws) to investigate incidents and pursue liability extraterritorially.[11] In other words, this can be interpreted to mean that the MPS may implement law enforcement outside China if another country allows it.

It can be indicated that problems with these laws include the broad discretion of the Chinese authorities, the ambiguous definitions of the interests protected by law of "national security" and "public interest" and the ambiguity of the targets of crackdowns, and in addition concerns about the human rights of "suspects" sent to China. However, we can conclude that in the case that the extraterritorial application of Chinese domestic law, is implemented based on treaties, agreements, etc. concluded with another country, its "legality" can be guaranteed if it is limited to application between those two countries.

However, it is apparent that the MPS is encouraging the repatriation of "suspects" to China by de facto coercive means even in countries where such bilateral treaties, etc. have not been concluded, or in countries such treaties have been concluded but the countries do not agree to extradition due to concerns about the human rights situation in China.[12] A technique which is often used in these kinds of cases is "involuntary returns." Safeguard Defenders, a human rights organization in Spain, has pointed out that three forms of this technique exist: (i) taking family members of the target living in China as hostages, (ii) contacting the target directly or indirectly and threatening or harassing them, (iii) kidnapping the target on foreign soil.[13] In the following section on "overseas police bases," we introduce examples of the Ministry of Public Security establishing illegal bases overseas to persuade people with Chinese nationality living

overseas who are regarded as "suspects" to return to China, including by means of "involuntary returns."

2. Overseas police bases: Illegal extraterritorial law enforcement by the MPS

(1) Overview of 110 Overseas[14]

In September 2022, Safeguard Defenders published 110 Overseas, a report which pointed out that "overseas police bases" have been established throughout the world mainly by the public security bureaus of China. The report pointed out based on publicly available information, etc. in China that the public security bureau in Fuzhou City, Fujian Province and also public security bureaus in other regional cities were establishing a series of "overseas police service stations (Chinese: 警僑事務海外服務站; hereinafter referred to as "Overseas Police Stations")" locally with the purpose of cracking down on cross-border crimes such as telecommunications fraud, etc. These Overseas Police Stations are not directly operated by the public security bureaus; they are run by overseas Chinese organizations with roots in the municipalities where the public security bureaus are located. On the surface, the bases claim to provide services for local overseas Chinese to renew their driver's licenses in China, etc. but Chinese media reports point out that their purpose is to "resolutely crack down on various crimes and illegal activities related to overseas Chinese."[15] This report stated that the Overseas Police Bases established by the Fuzhou Public Security Bureau and the Qingtian County Public Security Bureau in Zhejiang Province had reached 43 bases in 31 countries. In the report published by Safeguard Defenders as a follow-up to this report, this figure was amended to 102 bases in 53 countries.[16]

In relation to this, YASUDA Minetoshi pointed out that the term "警僑服務" [police services] used by the Chinese side began to be used in publicly available information by the Chinese side from about 2016.[17] Moreover, Yasuda presents the analysis that the purpose of promoting moves by local public security bureaus to establish Overseas Police Stations was to take on the operations which had previously been carried out privately by overseas Chinese organizations, such as mediating disputes, contacting hometowns, etc., in a form linked to the strengthening of moves toward private organization intervention by the Xi Jinping administration.[18]

(2) Surveilling and threatening Chinese dissidents using Overseas Police Stations

Even if the Overseas Police Stations are only being used for the renewal of driver's licenses and cracking down on general criminal offenses, the establishment of the stations itself is an act in violation of the prohibition of the establishment of government representative offices without the consent of the receiving State, as stipulated in the Vienna Convention on Diplomatic Relations (Article 12), which has also been ratified by China. Moreover, there are also cases in which the stations are used for political persecution of dissidents born in China and then were cracked down on by the authorities in the local country.

According to a press release from the U.S. Department of Justice,[19] in October 2022 the Federal Bureau of Investigation (FBI) searched the office of an overseas Chinese organization on the suspicion that it had received instructions from the Fuzhou Public Security Bureau to establish an illegal Overseas Police Stations in New York City, and confirmed that "Harry" Lu Jianwang and Chen Jinping, people involved in the organization, had been in contact with agents of the MPS In the subsequent investigation, it became clear that the two men had been destroying evidence of their connections to the MPS and attempting to obstruct the FBI investigation, so on April 2023 the FBI arrested them on charges of conspiracy and obstructing an investigation.[20] After his arrest, it became clear that Lu had followed the instructions of the MPS to organize a counter-rally to an anti-China protest rally in Washington D.C. (2015),[21] use threats to urge a Chinese exile living in the United States to return to China (2018), and help the Chinese government to locate a pro-democracy activist of Chinese descent living in California (2022; Lu denied involvement), etc.

What can we conclude from the above example? As can also be said about other examples of Overseas Police Stations, although the instructions are given by the MPS, the "law enforcement" is carried out by local overseas Chinese. Not only the MPS, but also the other Chinese authorities have long been promoting work to incorporate overseas Chinese as targets of united front work, and while leaders of overseas Chinese organizations receive the "honor" of receiving awards from the authorities in China and attending events hosted by the CCP, it is said that they are also required to engage in political activities that reflect the will of the Chinese authorities, such as involvement in activities that support China's position on the Taiwan Issue.[22] This can be seen in the example of Lu.He received an award from a MPS official for the above activities and was given favors by the MPS and became its agent. For the MPS, denying any relationship with the perpetrators allows them to be "disposable," which reduces the risks in the case that the perpetrators are cracked down on by local authorities.

3. Cyber operations: analysis of MPS capability generation and employment from declassified, leaked, and open-source information regarding i-Soon.

In parallel with its extraterritorial law enforcement activities through Overseas Police Stations, the MPS has been carrying out cyber operations for the purpose intelligence-collection and influencing a variety of targets outside China. The following three characteristics are salient about the MPS affiliated cyber operations, triangulating the declassified indictment of the Wu Haibo Case[23], publicly available information from 2023 to 2024 about Chinese cybersecurity vendor Anxun Information Technology Co. Ltd. (also known as i-SOON), to which eight of the defendants in the Wu Haibo Case belonged, and other technical threat-intelligence reporting from the Western cybersecurity companies and experts.

The first characteristic is the targets (victims) of cyber operations and plausible motivations behind deduced from the pattern. Reflecting the previous section, MPS covert operations beyond China's jurisdiction are consistent with its role as a "political police force" which takes action by all necessary means

and in all situations against words or actions which may destabilize the current CCP rule. Following the same logic, reportedly MPS-affiliated cyber operations tend to target political dissident as well as ethnic and religious minorities groups in the third countries, who are critical of the current CCP rule. In line with this pattern, MPS targeting also include foreign media organizations and civil society organizations which support these dissidents .

For example, the charges in the Wu Haibo Case include several examples of i-SOON employees, in collusion with the MPS, carrying out series of cyber espionage campaigns to collect intelligence, such as surveilling the words and actions of target individuals and understanding their locations and travel destinations, through the theft of personal information from media organizations and religious organizations located in the United States and abroad.[24] Such intelligence collection patterns can be interpreted as having the purpose of targeting to support subsequent "law enforcement" activities by the MPS(or the Ministry of State Security) both in and outside of China. Furthermore, Inksit Group, the threat-intelligence research unit of the U.S. security company Recorded Future, published an technical analysis of the internal documents of i-SOON leak data on GitHub in February 2024[25]. The report revealed that some technical feature of operational tools and infrastructure of i-SOON's hacking as a services showed overlaps with the ones of threat actors previously named as RedAlpha and Poison CARP.[26] Both RedAlpha and Poison CARP are threat actors which have been active in collecting intelligence from individuals and organizations in and outside China related to the Tibet and Xinjiang Uygur Autonomous Region issues.[27] Given its strong outsourcing relationship with i-SOON (mentioned below), these overlap in tradecrafts and targeting patterns constitutes circumstantial evidence of the plausible motivations behind the MPS' involvement in extensive cyber espionage campaigns beyond its border.

The second characteristic is MPS conducts of outsourcing to a private cybersecurity company in China, ranging from their capability development for hacking to actual operations on behalf of MPS itself. For example, according to the Wu Haibo Case indictment, i-SOON provided education and training to enable the MPS officers to develop the ability to carry out hacking on their own. It is, however, more noteworthy that the outsourcing of actual operations management, such as i-SOON employees carrying out hacking vis-à-vis MPS collection requirements and providing the results to the MPS officers.[28]

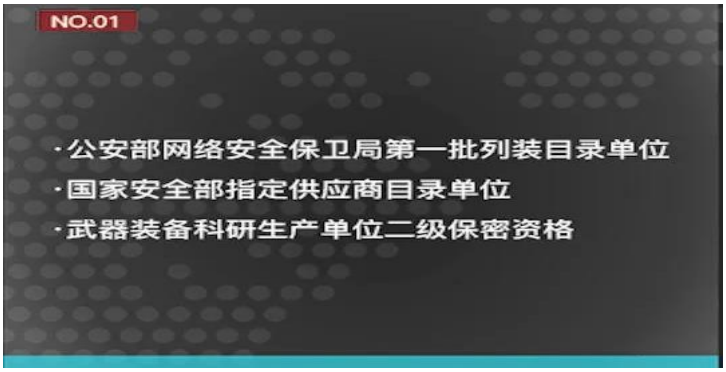
The Wu Haibo Case indictment, for example, includes a fact supporting the charge that i-SOON "worked with at least 43 different MSS or MPS bureaus in at least 31 separate provinces and municipalities in China."[29] Furthermore, a October 2023 study of publicly available information such as judicial document in China and official website of i-SOON illustrated the company has actively advertised the fact that its customers include the MPS, the MSS and their respective local agencies and the fact that it is is a certified supplier for national security-related products to the Cyber Security and Defense Bureau of the MPS.[30] These facts suggests i-SOON's status as a powerful subcontractor for the MPS in particular.

The third characteristic is the autonomy of "local agencies" in the capability development and employment. Archived i-SOON's website used to boldly advertise that it has business relationships with approximately 43 of the MPS local agencies located throughout China.[31] Furthermore, Figure 2 shows a list of i-SOON's contract achievements published on GitHub in February 2024. Looking at the statements

in the third, sixth, and seventh columns from the left, the breakdown of the 32 contracts shows that "public security" accounts for the greatest number of contracts, with 18. Moreover, for most of the contracts classified as "public safety" or "(national) security," including those contracts via a range of front companies, the final customers are local agencies of the MPS or the MSS. These facts illustrate that Chinese-state sponsored cyber operations are not necessarily under centralized control but are supported by a decentralized ecosystem, including the "local agencies" of the MPS and the MSS.[32]

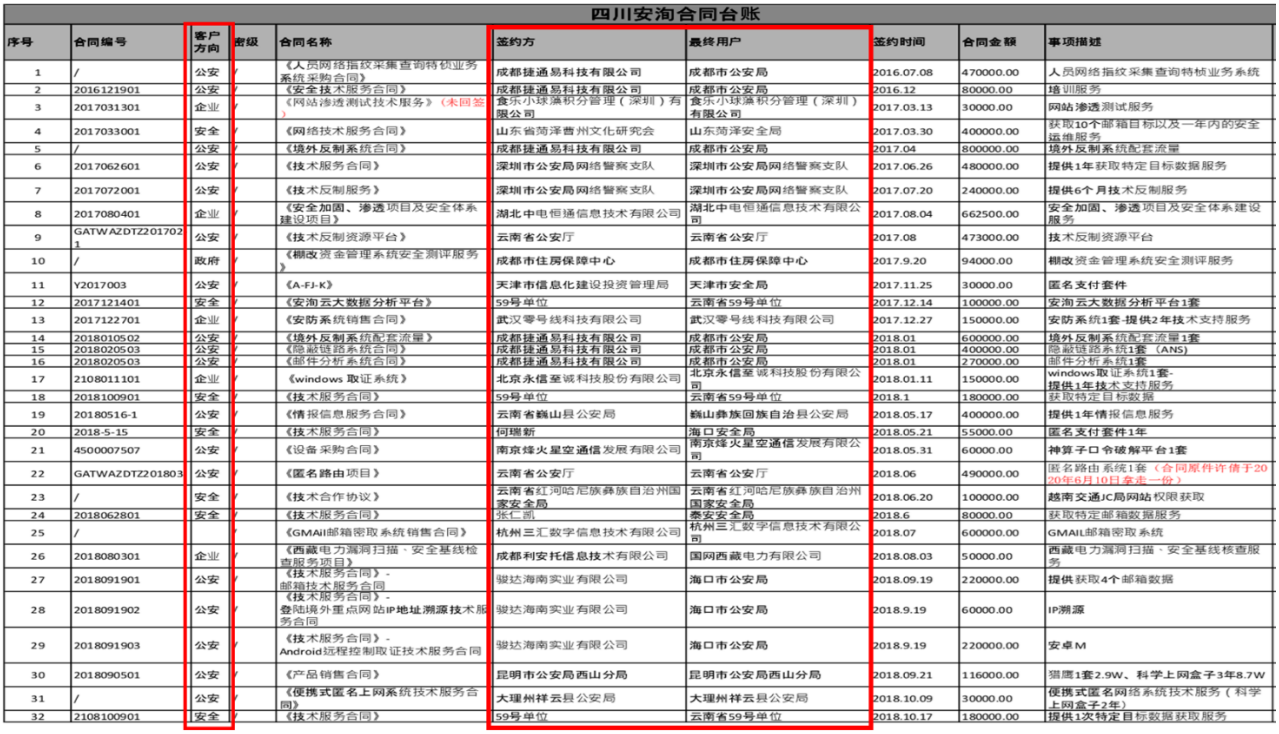
The MPS capability generation and employment model, supported by multi-layered network between "local agencies" and their business subcontractors, front companies, etc., differs greatly from the ones of militaries and intelligence services of liberal democracies, in which prefers in-housed capability generation and direct operational control from operations security(OpSEC) perspective.[33] The difference in the governance of offensive cyber capabilities and operations raises a unique challenge faced when analyzing and ascertaining the cyberattack capabilities of China.

Figure 1: Publicity on the i-SOON website about supplier qualification by the MPS and the MSS[34]



Source: Natto Team. "I-SOON: Another Company in the APT41 Network." Natto Thoughts (blogs), October 27, 2023. https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41.

Figure 2: List of i-SOON's contract achievements published on GitHub (about 2016-2018)



四川安洵合同台账

序号	合同编号	客户方向	密级	合同名称	签约方	最终用户	签约时间	合同金额	事项描述
1	/	公安	/	《人员网络指纹采集查询特侦业务系统采购合同》	成都捷通易科技有限公司	成都市公安局	2016.07.08	470000.00	人员网络指纹采集查询特侦业务系统
2	2016121901	公安	/	《安全技术服务合同》	成都捷通易科技有限公司	成都市公安局	2016.12	80000.00	培训服务
3	201703130 1	企业	/	《网站渗透测试技术服务》（未回签）	食乐小球藻积分管理（深圳）有限公司	食乐小球藻积分管理（深圳）有限公司	2017.03.13	30000.00	网站渗透测试服务
4	2017033001	安全	/	《网络技术服务合同》	山东省菏泽曹州文化研究会	山东菏泽安全局	2017.03.30	400000.00	获取10个邮箱目标以及一年内的安全运维服务
5	/	公安	/	《境外反制系统合同》	成都捷通易科技有限公司	成都市公安局	2017.04	800000.00	境外反制系统配套流量
6	2017062601	公安	/	《技术服务合同》	深圳市公安局网络警察支队	深圳市公安局网络警察支队	2017.06.26	480000.00	提供1年获取特定目标数据服务
7	2017072001	公安	/	《技术反制服务》	深圳市公安局网络警察支队	深圳市公安局网络警察支队	2017.07.20	240000.00	提供6个月技术反制服务
8	2017080401	企业	/	《安全加固、渗透项目及安全体系建设项目》	湖北中电恒通信息技术有限公司	湖北中电恒通信息技术有限公司	2017.08.04	662500.00	安全加固、渗透项目及安全体系建设服务
9	GATWAZDTZ2017021	公安	/	《技术反制资源平台》	云南省公安厅	云南省公安厅	2017.08	473000.00	技术反制资源平台
10	/	政府	/	《棚改资金管理系统安全测评服务》	成都市住房保障中心	成都市住房保障中心	2017.9.20	94000.00	棚改资金管理系统安全测评服务
11	Y2017003	公安	/	《A-FJ-K》	天津市信息化建设投资管理局	天津市安全局	2017.11.25	30000.00	匿名支付套件
12	2017121401	安全	/	《安洵云大数据分析平台》	59号单位	云南省59号单位	2017.12.14	100000.00	安洵云大数据分析平台1套
13	2017122701	企业	/	《安防系统销售合同》	武汉零号线科技有限公司	武汉零号线科技有限公司	2017.12.27	150000.00	安防系统1套-提供2年技术支持服务
14	2018010502	公安	/	《境外反制系统配套流量》	成都捷通易科技有限公司	成都市公安局	2018.01	600000.00	境外反制系统配套流量1套
15	2018020503	公安	/	《隐蔽链路系统合同》	成都捷通易科技有限公司	成都市公安局	2018.01	400000.00	隐蔽链路系统1套（ANS）
16	2018020503	公安	/	《邮件分析系统合同》	成都捷通易科技有限公司	成都市公安局	2018.01	270000.00	邮件分析系统1套
17	2108011101	企业	/	《windows 取证系统》	北京永信至诚科技股份有限公司	北京永信至诚科技股份有限公司	2018.01.11	150000.00	windows取证系统1套-提供1年技术支持服务
18	2018100901	安全	/	《技术服务合同》	59号单位	云南省59号单位	2018.1	180000.00	获取特定目标数据
19	20180516-1	公安	/	《情报信息服务合同》	云南省鹤山县公安局	鹤山彝族回族自治县公安局	2018.05.17	400000.00	提供1年情报信息服务
20	2018-5-15	安全	/	《技术服务合同》	何瑞新	海口安全局	2018.05.21	55000.00	匿名支付套件1年
21	4500007507	公安	/	《设备采购合同》	南京烽火星空通信发展有限公司	南京烽火星空通信发展有限公司	2018.05.31	60000.00	神算子口令破解平台1套
22	GATWAZDTZ20180 3	公安	/	《匿名路由项目》	云南省公安厅	云南省公安厅	2018.06	490000.00	匿名路由系统1套（合同原件许倩于2020年6月10日拿走一份）
23	/	安全	/	《技术合作协议》	云南省红河哈尼族彝族自治州国家安全局	云南省红河哈尼族彝族自治州国家安全局	2018.06.20	100000.00	越南交通JC局网站权限获取
24	2018062801	安全	/	《技术服务合同》	张仁凯	泰安安全局	2018.6	80000.00	获取特定邮箱数据服务
25	/		/	《GMail邮箱密取系统销售合同》	杭州三汇数字信息技术有限公司	杭州三汇数字信息技术有限公司	2018.07	600000.00	GMail邮箱密取系统
26	2018080301	企业	/	《西藏电力漏洞扫描、安全基线检查服务项目》	成都利安托信息技术有限公司	国网西藏电力有限公司	2018.08.03	50000.00	西藏电力漏洞扫描、安全基线核查服务
27	2018091901	公安	/	《技术服务合同》-邮箱技术服务合同	骏达海南实业有限公司	海口市公安局	2018.09.19	220000.00	提供获取4个邮箱数据
28	2018091902	公安	/	《技术服务合同》-登陆境外重点网站IP地址溯源技术服务合同	骏达海南实业有限公司	海口市公安局	2018.9.19	60000.00	IP溯源
29	2018091903	公安	/	《技术服务合同》-Android远程控制取证技术服务合同	骏达海南实业有限公司	海口市公安局	2018.9.19	220000.00	安卓M
30	2018090501	公安	/	《产品销售合同》	昆明市公安局西山分局	昆明市公安局西山分局	2018.09.21	116000.00	猫鹰1套2.9W、科学上网盒子3年8.7W
31	/	公安	/	《便携式匿名上网系统技术服务合同》	大理州祥云县公安局	大理州祥云县公安局	2018.10.09	30000.00	便携式匿名网络系统技术服务（科学上网盒子2年）
32	2108100901	安全	/	《技术服务合同》	59号单位	云南省59号单位	2018.10.17	180000.00	提供1次特定目标数据获取服务

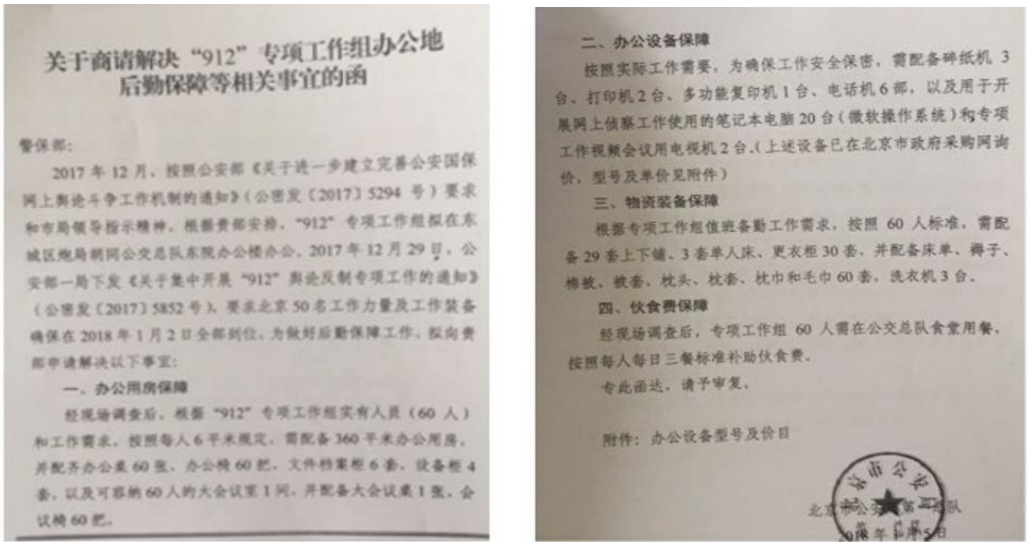
Source: Prepared by the authors based on an image file of the i-SOON documents published on GitHub on February 16, 2024 (red lines added by the authors for emphasis). Regarding past investigative reports, etc. utilizing the same kind of data as this list, please refer for example to the following: Web Special Feature: Tracking China's Leaked Documents 4 "Public Security", Japan Broadcasting Corporation (NHK) [Web 特集：追跡 中国・流出文書 4 『公安』], October 2, 2024 https://www3.nhk.or.jp/news/html/20241002/k10014588431000.html (accessed April 12, 2025); Arianne Bleiweiss, "I-Soon Leak: KELA's Insights," KELA Cyber Threat Intelligence, March 7, 2024, https://www.kelacyber.com/blog/i-soon-leak-kelas-insights/ (accessed April 12, 2025)

4. Cyber-enabled influence operations: 912 Special Project Working Group

The MPS has also started cyber-enabled influence operations, namely the spreading of disinformation on social network services (SNSs)[35]. Here, we will briefly discuss the 912 Special Project Working Group (912-SPWG) (hereinafter referred to as the "912-SPWG") in order to better understand the history and development of the MPS's digital influence operations.

The 912-SPWG is a project team under the command lof the MPS, whose existence was revealed through the indictment titled "US v. Yunpeng Bai, et al."[36] (hereinafter: the "Yunpeng Bai Case"), which were declassified at the discretion of the U.S. Department of Justice on April 17, 2023 (Figure 3-1). The Yunpeng Bai Case indicts a total of 34 individuals, including officers from the First, Fifth, and Eleventh Bureaus of the MPS, who are persons responsible for management and persons in charge of operations assigned to the 912-SPWG,[37] and officers from the Beijing Municipal Public Security Bureau, for cyber-enabled influence operations targeting individuals and organizations in and outside the United States, and other related crimes.[38] Triangulating publicly available information by private companies and existing scholarly literature, the content of the indictment provide three indications about the nature of the MPS's cyber-enabled influence operations.

Figure 3-1: Records of goods procurement, etc. by the 912-SPWG presented by the FBI as evidence



关于商请解决"912"专项工作组办公地后勤保障等相关事宜的函

警保部：

2017年12月，按照公安部《关于进一步建立完善公安国保网上舆论斗争工作机制的通知》（公密发〔2017〕5294号）要求和市局领导指示精神，根据贵部安排，"912"专项工作组拟在东城区炮局胡同公交总队东院办公楼办公，2017年12月29日，公安部一局下发《关于集中开展"912"舆论反制专项工作的通知》（公密发〔2017〕5852号），要求北京50名工作力量及工作装备确保在2018年1月2日全部到位，为做好后勤保障工作，拟向贵部申请解决以下事宜：

一、办公用房保障

经现场调查后，根据"912"专项工作组实有人员（60人）和工作需求，按照每人6平米规定，需配备360平米办公用房，并配齐办公桌60张、办公椅60把、文件档案柜6套、设备柜4套，以及可容纳60人的大会议室1间，并配备大会议桌1张、会议椅60把。

二、办公设备保障

按照实际工作需要，为确保工作安全保密，需配备碎纸机3台、打印机2台、多功能复印机1台、电话机6部，以及用于开展网上侦察工作使用的笔记本电脑20台（微软操作系统）和专项工作视频会议用电视机2台。（上述设备已在北京市政府采购网询价，型号及单价见附件）

三、物资装备保障

根据专项工作组值班备勤工作需求，按照60人标准，需配备29套上下铺、3套单人床、更衣柜30套，并配备床单、褥子、棉被、被套、枕头、枕套、枕巾和毛巾60套，洗衣机3台。

四、伙食费保障

经现场调查后，专项工作组60人需在公交总队食堂用餐，按照每人每日三餐标准补助伙食费。

专此函达，请予审复。

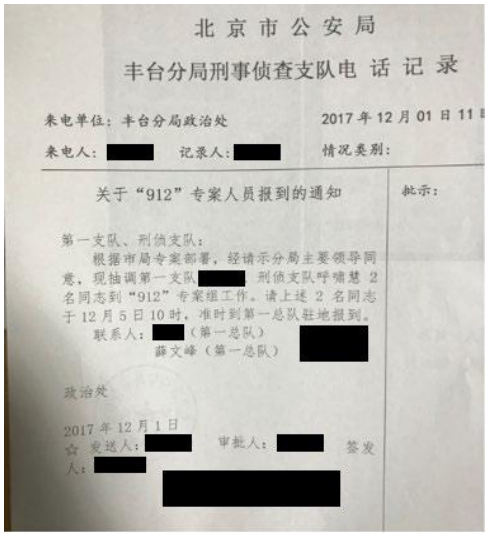
附件：办公设备型号及价目

Source: United States v. Yunpeng Bai, et al., No. 23-MJ-0334 (SJB) (District Court, E.D. New York Unsealed April 17 2023), 13. https://web.archive.org/web/20250204065726/https://www.justice.gov/d9/2023-04/squad_912_-_23-mj-0334_redacted_complaint_signed.pdf (archived February 4, 2025) (accessed April 16, 2025)

Firstly, the organizational structure of the 912-SPWG. According to the indictmentfor the

Yunpeng Bai Case, the 34 individuals indicted in the case were officers of a command group located within the facilities of the Beijing Municipal Public Security Bureau. This Beijing City command group is the core of the MPS's project called the "912 (Special) Project," but, on the other hand, officers were also dispatched to the "912" Project from the local public security agencies of more than 15 provinces and other jurisdictions throughout China (Figure 3-2), indicating that the operation was on a nationwide scale and based on instructions from the central government*.[39]

Figure 3-2: Personnel-related documents concerning 912 operations submitted by the FBI as evidence


北京市公安局

丰台分局刑事侦查支队电话记录

来电单位：丰台分局政治处　　2017年12月01日11

来电人：[redacted]　记录人：[redacted]　情况类别：

关于"912"专案人员报到的通知　　批示：

第一支队、刑侦支队：

根据市局专案部署，经请示分局主要领导同意，现抽调第一支队[redacted]刑侦支队呼啸慧2名同志到"912"专案组工作。请上述2名同志于12月5日10时，准时到第一总队驻地报到。

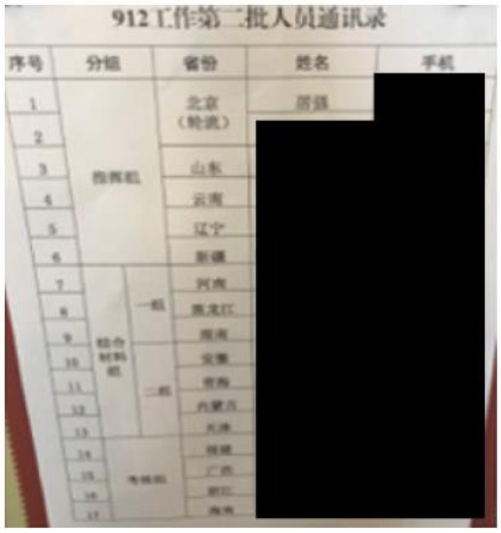
联系人：[redacted]（第一总队）

薛文峰（第一总队）[redacted]

政治处

2017年12月1日

☆ 发送人：[redacted]　审批人：[redacted]　签发人：[redacted]


912工作第二批人员通讯录

序号	分组	省份	姓名	手机
1		北京（轮流）	顾强	[redacted]
2				
3	指挥组	山东		
4		云南		
5		辽宁		
6		新疆		
7		河南		
8	综合材料组	一组	黑龙江	
9			湖南	
10			安徽	
11		二组	甘肃	
12			内蒙古	
13			天津	
14		考核组	福建	
15			广西	
16			浙江	
17			海南	

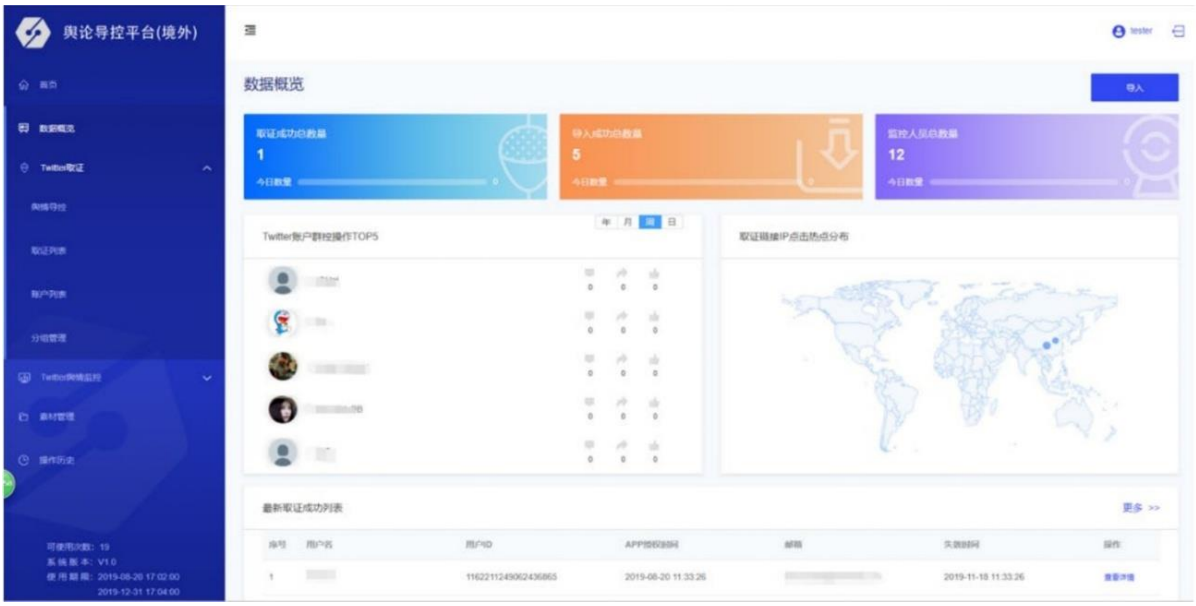
Source: United States v. Yunpeng Bai, et al., No. 23-MJ-0334 (SJB) (District Court, E.D. New York Unsealed April 17 2023), 15, 18. https://web.archive.org/web/20250204065726/https://www.justice.gov/d9/2023-04/squad_912_-_23-mj-0334_redacted_complaint_signed.pdf (archived February 4, 2025) (accessed April 16, 2025)

Secondly, the mission and actual specific activities of the 912-SPWG. The first point is that the indictment of the Yunpeng Bai Case mentions the existence of internal documents from the Ministry of Public Security from about March 2020.[40] In addition, it evaluates the primary purpose of the 912-SPWG to be to "conduct online perception management campaigns that promote the propaganda and approved narratives of the PRC government and the CCP on various social media platforms, while attempting to intimidate and silence their critics by discrediting their speech or overwhelming it with counternarratives."[41]

In addition, the indictment presents specific examples of cyber-enabled influence operations from 2021 onward which are thought to be attributed to officers of the 912-SPWG,[42] and the targets, timeline, and techniqueof several of these examples partially overlaps with those of the past cyber-enabled influence operations by threat-actors named "Spamouflage" (or

"DRAGONBRIDGE"), which private security companies and research institutions attributed it to be part of Chinese government-led disinformation campaign.[43] Furthermore, the indictment of the Wu Haibo Case against employees of i-SOON (see section 3) points out the fact that i-SOON had delivered to the MPS tools for cyber-enabled influence operations, including functions for hacking Twitter (now "X") accounts (Figure 4).[44] Taking into account the related cases with the suspected involvement of the MPS[45] and the drafting dates of the administrative documents in Figure 3, we can conclude that it is almost certain that the MPS had developed their capabilities and embarked on cyber-enabled influence operation by no later than about 2017 to 2020.

Figure 4: Image of cyber-enabled influence operations tools i-SOON is thought to have delivered to the Ministry of Public Security



Source: United States v. Wu Haibo, et al., No. 24 CRIM 687 (United States District Court, Southern District of New York unsealed March 5, 2025), 9, https://www.justice.gov/usao-sdny/media/1391751/dl (accessed April 16, 2025).

Finally, there is the organic network between the MPS and other party and government agencies around China's external influence operations. The indictment of the "Yunpeng Bai Case" mentions, for example, the relationship between 912-SPWG and the Chinese Communist Party's United Front Work Department (UFWD) and the MSS. Regarding the former, the indictment mentions the existence of a intercepted record of an online chat between Xi Yue and Tan Jinyan, officers of the 912-SPWG, in about June 2020, and mention that "(Xi Yue) lamented having to work recently with so many people from the UFWD" in the chat.[46] This point suggests that the UFWD, a party organization, has been exercising some degree of influence on the operational management of

MPS cyber-enabled influence operations..

As for the relationship with the MSS, the indictment describes the fact that the 912-SPWG has been providing intelligence and targeting supports, for example, providing to the MSS information about the potential targets of political repression leveraging SNS accounts under the control of 912-SPWG, including one of the cases about Victim-1, who was the target of Fox Hunt[47] operations from the second half of the 2010s onward.[48] The form of these activities match the trends in cyber operations related to the MPS discussed in section 3. In other words, this shows that the MPS and the MSS place importance on a full spectrum of operational capabilities in/through cyberspace and regard cyber-enabled capabilities as a means of supporting extraterritorial law enforcement in physical space as discussed in section 1 and section 2.

5. Conclusion: The internal logic of the covert external influence operations by the MPS

As mentioned above, the MPS has strengthened its covert external influence operations in both physical and cyberspace. So what does explain the logic behind the MPS, which is essentially supposed to be a law enforcement agency whose main mission is to crack down on crime, becoming involved in covert operations against other countries?

One clue is thought to be the "Holistic Approach to National Security" proposed by President Xi in 2014, which has become a fundamental concept for China's national security. President Xi has pointed out that importance should be placed on both external security and internal security in the context of the holistic view of national security.[49] In other words, we can conclude that he expressed an awareness of the problem that threats to domestic security can come from outside the country. Focusing on crackdowns by the MPS, criminal offenses that cross national borders have truly become a threat to China's domestic security. Furthermore, former bureaucrats and party officials, etc. who have fled overseas to avoid anti-corruption crackdowns potentially pose a threat to the CCP's rule. Moreover, as the view that democratization movements arise in a form connected with foreign countries is becoming mainstream in China,[50] the MPS will likely see overseas Chinese with anti-regime tendencies as people who should be cracked down on in the same way as domestic dissidents.

Therefore, it can be seen that the MPS considers any entity that poses a threat to the CCP's rule, whether domestic or foreign, and whether in physical space or cyberspace, to be subject to "law enforcement" or "punishment." Actually, there are some MPS officials who advocate for the need

to crack down on external (the expression "涉外" is used in the original Chinese text) crimes based on the holistic view of national security.[51] This means that from the perspective of pursuing the functions of a "political police" that protect the CCP's rule, which are derived deductively from this holistic view of national security, the geographical division between "domestic" and "overseas" and the nature of the activities in question do not restrict the extension of the MPS's own mission as a police organization.

While the expansion of these external influence operations by the MPS is a clear trend, there are still much room for future research about the MPS's covert influence operations, such as the division of labor with the MSS, which is responsible for similar activities, and, in case of specific activities, the authority and discretion of local agencies and whether or not the central government is in control of the operations, among others. We can conclude that the examples from recent years generally explained in this paper suggest that the MPS is in fact an actor supporting external influence operations based on China's Holistic Approach to National Security in the same way as other public organizations such as the UFWD, the MSS, and the People's Liberation Army, and that it also has value as a subject of research from this perspective.

(Document completed on April 16, 2025)

* This paper adopts a co-authoring system under which Mr. Goto from the China Division is responsible for section 1 and section 2 and Mr. Seto from the Cyber Security Division is responsible for section 3 and section 4. However, the two authors jointly wrote the Introduction and the Conclusion and jointly collated and verified the content of the analyses based on both English language and Chinese language information sources.

1 U.S. Attorney's Office, Southern District of New York, "10 Chinese Nationals Charged With Large-Scale Hacking Of U.S. And International Victims On Behalf Of The Chinese Government" U.S. Department of Justice, March 4, 2025, https://www.justice.gov/usao-sdny/pr/10-chinese-nationals-charged-large-scale-hacking-us-and-international-victims-behalf.

2 Martin Purbrick, "Future Global Policeman? The Growing Extraterritorial Reach of PRC Law Enforcement", China Brief, Vol.22, Issue 9, May 13, 2022 12.

3 Daniel Fu, "The Long Arm of the Law(less): The PRC's Overseas Police Stations", China Brief, Vol.23, Issue 11, June 13, 2023 29-30.

4 Existing studies analyzing the international law enforcement cooperation of the MPS and other Chinese authorities from the perspective of expanding the external influence of China, etc. include Eric Green et al. "The Global Security Initiative: China's International Policing Activities", The International Institute for Strategic Studies, October, 2024; Sheena Chestnut Greitens, "China's Use of Nontraditional Strategic Landpower in Asia", *Parameters*, 54, No.1, 2024; MASUO Chisako T. [益尾知佐子], "China's Domestic Governance and Security Strategy: The Diffusion of Chinese-style Police and Its Implication for the International Order [中国の国内統治と安全保障戦略－中国型警察の普及と国際秩序]", *International Affairs* (No.715, October 2023), and others.

5 The State Councilors are positioned as second-ranked among the leaders of the nation together with the Vice Premiers of the State Council and the Vice Chairmen of the National People's Congress, and are considered roughly equivalent to the members of the Politburo of the CCP. (The Paper, October 12, 2014, https://www.thepaper.cn/newsDetail_forward_1270347).

6 Article 43 of the People's Police Law (enacted in 1995), a law which regulates the activities of security agencies (the people's police), including the Ministry of Public Security, contains the provision that the people's police organs at higher levels shall exercise supervision over the law enforcement activities by the police organs at lower levels.

7 Ministry of Public Security website: http://www.mps.gov.cn:8080/.

[8] Political security is considered to mean protecting the rule of the Communist Party and the security of the socialist system (MATSUDA Yasuhiro [松田康博], "China's 'Political Security' and Domestic Security System [中国による『政治安全』と国内安全保障体制]", *Japan Institute of International Affairs Research Report* No. 11, May 6, 2021 https://www.jiia.or.jp/research-report/post-102.html).

[9] "National Public Security Agency and Bureau Directors Meeting held: sacred duties fulfilled faithfully, hard work for promoting Chinese-style modernization and contribution to the public security force [全国公安庁局長会議召開 忠実履行神聖職責 力扎実穏健推進中国式現代化貢献公安力量]", Ministry of Public Security website, January 14, 2024, https://www.mps.gov.cn/n2254314/n2254315/n2254317/n8928114/n8928175/c9391083/content.html.

[10] "Chinese Communist Party Publication: Plan on Building the Rule of Law in China (2020 to 2025) [中共印発 『法治中国建設規則（2020～2025年)』]", *www.gov.cn* [中国政府網], January 10, 2021, https://www.gov.cn/zhengce/2021-01/10/content_5578659.htm.

[11] In the Cybersecurity Law there is a provision to the effect that in the case that extraterritorial (including Hong Kong, Macao, and Taiwan; the same below) individuals or organizations attack or intrude into the information infrastructure of China, the MPS may impose sanctions on said individuals and organizations (Article 75). In the Data Security Law, there is a provision to the effect that data processing outside China which harms the national security of China, the public interest, etc. is to be pursued for legal responsibility in accordance with law (Article 2), and in addition investigation authority is granted to the MPS and state security organs (departments) when the investigation of crimes is the reason (Article 35). In the Law on Combating Telecom and Online Fraud, there is a provision to the effect that pursuing legal responsibility is allowed in the case that individuals and organizations outside China carry out or aid and abet telecom and online fraud inside China (Article 3), and in addition there is a provision to the effect that the MPS shall lead the anti-telecom and network fraud operations (Article 6).

[12] Purbrick, "Future Global Policeman?", 14.

[13] Safeguard Defenders, "110 Overseas: Chinese Transnational Policing Gone Wild", September 2022, revised version was released October 29, 2022, 4.

[14] Unless otherwise noted, the content of (1) is based on the Ibid. descriptions. Note that in China, just as in Japan, the number for calling the police (public security) is 110.

[15] China Peace [中国長安網] (the official media outlet of the Central Political and Legal Affairs Commission), July 29, 2022 http://www.chinapeace.gov.cn/chinapeace/c100049/2022-07/29/content_12654617.shtml; Ibid, 12.

[16] Revised to take into account the status of establishment of bases of other regions. (Safeguard Defenders, "Patrol and Persuade: A follow-up investigation to 110 Overseas", December 2022 5-7).

[17] Minetoshi Yasuda [安田峰俊], "Wolf Warrior China's Operations Against Japan [戦狼中国の対日工作]", *Bunshun Shinsho* (2023), 33.

[18] Ibid, 34-35.

[19] Unless otherwise noted, the following content is based on Office of Public Affairs, "Two Arrested for Operating Illegal Overseas Police Station of the Chinese Government", U.S. Department of Justice, April 17, 2023, https://www.justice.gov/archives/opa/pr/two-arrested-operating-illegal-overseas-police-station-chinese-government.

[20] In the subsequent trial, Lu was acquitted and Chen was found guilty (U.S. Attorney's Office, Eastern District of New York, "Two Arrested for Operating Illegal Overseas Police Station of the Chinese Government", U.S. Department of Justice, December 18, 2024, https://www.justice.gov/usao-edny/pr/new-york-city-resident-pleads-guilty-operating-secret-police-station-chinese).

[21] As a result of these activities, Lu seems to have received an award from a Ministry of Public Security official (U.S. Department of Justice, "Two Arrested for Operating Illegal Overseas Police Station of the Chinese Government").

[22] Safeguard Defenders, "110 Overseas", 11.

[23] United States v. Wu Haibo, et al., No. 24 CRIM 687 (United States District Court, Southern District of New York unsealed March 5, 2025), https://www.justice.gov/usao-sdny/media/1391751/dl

[24] Ibid., 11-19.

[25] For detailed analyses concerning the background to the leak of the internal documents of i-SOON published on GitHub in February 2024 (as of April 2025, the original documents had been deleted from GitHub) and the content of the documents, refer for example to the following: Robinson, "I-SOON Leak"; Arianne Bleiweiss, "I-Soon Leak: KELA's Insights", KELA Cyber Threat Intelligence, March 7, 2024, https://www.kelacyber.com/blog/i-soon-leak-kelas-insights/; BushidoToken, "Lessons from the ISOON Leaks", *@BushidoToken Threat Intel* (blog) (BushidoToken, February 22, 2024), https://blog.bushidotoken.net/2024/02/lessons-from-isoon-leaks.html.

[26] Insikt Group. "Attributing I-SOON: Private Contractor Linked to Multiple Chinese State-Sponsored Groups." Recorded Future, March 20, 2024, 1-2, https://go.recordedfuture.com/hubfs/reports/cta-2024-0320.pdf.

[27] For the details of the past campaigns of the two groups, refer for example to the following: Insikt Group. "RedAlpha Conducts Multi-Year Credential Theft Campaign Targeting Global Humanitarian, Think Tank, and Government Organizations." Recorded Future, August 16, 2022. https://go.recordedfuture.com/hubfs/reports/ta-2022-0816.pdf.; Marczak, Bill, et.al. "Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits." Citizen Lab Research Report No. 123, University of Toronto, September 2019.

[28] United States v. Wu Haibo, et al., 2-10.; U.S. Attorney's Office, "10 Chinese Nationals Charged With Large-Scale Hacking"

[29] Ibid., 3, para. 4.

[30] Natto Team. "I-SOON: Another Company in the APT41 Network." Natto Thoughts (blogs), October 27, 2023. https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41.

[31] This point can be confirmed from the archive of the i-SOON official website as of February 19, 2024. Refer to the following: "Cooperative Partners

— Police Cooperation [合作伙伴－警企合作]", Anxun Information Technology Co. Ltd. website, February 19, 2024 archive, https://web.archive.org/web/20240219105947/http://www.i-soon.net/pc_partner.html (accessed April 16, 2025)

[32] Refer to the following previous studies regarding the special characteristics of China's cyberattack capability development and operation ecosystem in particular: Piotr Malachiński & World Watch team, "The Hidden Network: How China Unites State, Corporate, and Academic Assets for Cyber Offensive Campaigns." Orange Cyberdefense, November 24, 2024, https://research.cert.orangecyberdefense.com/hidden-network/report.html; Coline Chavane and Sekoia TDR Team, "A Three Beats Waltz: The Ecosystem behind Chinese State-Sponsored Cyber Threats." Sekoia.IO, November 13, 2024, https://blog.sekoia.io/a-three-beats-waltz-the-ecosystem-behind-chinese-state-sponsored-cyber-threats/.

[33] Refer to the following previous studies regarding models for the development and operation of the cyberattack capabilities of military organizations and intelligence agencies in Western democratic countries, as specified in operations security risk management and legal compliance requirements. SETO Takashi [瀬戸崇志], "Development and operation of offensive cyber capabilities by the "cyber militaries" of democratic nations: A comparative case study focusing on the process of "dual integration" in the U.S. and Dutch militaries [民主主義国家の「サイバー軍」による攻勢的サイバー作戦能力の整備と運用—米軍とオランダ軍における「二重の統合」の過程に着目した比較事例研究—]", *Security & Strategy* Vol. 4, No. 2 (March 2024) 184-186; Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber Force* (London: Hurst Publishers, 2022), 8-10, 147-161.

[34] Content similar to this Figure-1 can be confirmed from the archive of the i-SOON official website as of February 19, 2024. Refer to the following: "About us— Development history [関于我們－発展歴程]", Anxun Information Technology Co. Ltd. website, February 19, 2024 archive, https://web.archive.org/web/20240219105939/http://www.i-soon.net/aboutUs_history.html (accessed April 16, 2025)

[35] Refer to the following references concerning cyber-enabled influence operationsICHIDA Kazuki [一田和樹] et al., "Online Public Opinion Manipulation and Digital Influence Operations: Making the "Invisible Hand" Visible [ネット世論操作とデジタル影響工作—「見えざる手」を可視化する]" (*Hara Shobo*, 2023); Jelena Vićić and Richard Harknett, "Identification-Imitation-Amplification: Understanding Divisive Influence Campaigns through Cyberspace", *Intelligence & National Security* 39, no. 5 (July 28, 2024): 897–914.

[36] United States v. Yunpeng Bai, et al., No. 23-MJ-0334 (SJB) (District Court, E.D. New York Unsealed April 17 2023), https://webcf.waybackmachine.org/web/20250204065726/https://www.justice.gov/d9/2023-04/squad_912_-_23-mj-0334_redacted_complaint_signed.pdf. (archived February 4, 2025) (accessed April 16, 2025). Note that the link from the U.S. Department of Justice website to the documents related to the indictment in this Yunpeng Bai Case was a dead link as of April 16, 2025, but the original documents can be confirmed from the archived URL as of February 4 the same year (refer above).

[37] United States v. Yunpeng Bai, et al., 12, para. 15. According to the indictment documents, the First Bureau referred to here is in charge of domestic counterintelligence/suppression of exiled political offenders, etc., the Fifth Bureau is in charge of investigations into criminal offenses, and the Eleventh Bureau is considered to be the division in charge of network/Internet security.

[38] Refer to the following: U.S. Attorney's Office, Eastern District of New York, "34 Officers of People's Republic of China National Police Charged with Perpetrating Transnational Repression Scheme Targeting U.S. Residents", U.S. Department of Justice, April 17, 2023, https://www.justice.gov/usao-edny/pr/34-officers-peoples-republic-china-national-police-charged-perpetrating-transnational.

[39] United States v. Yunpeng Bai, et al., 12-18.

[40] United States v. Yunpeng Bai, Ibid., 8, para. 9. According to the indictment letter, there is a document called "an MPS proposal from March 2020)" thought to have been collected in the investigation process (the original document has not been released), and this document includes the proposal of "instituting countermeasures to monitor dissent on foreign social media platforms, including Twitter" predicated on the perception that "most foreign reports about the PRC are negative, and that Twitter content accounts for approximately 80 percent of the attacks on the PRC and the CCP."

[41] Ibid., 37, para. 59.

[42] Ibid., 10-11, para. 13. Examples of digital influence operations campaigns specifically raised here can be broadly categorized as follows (the information inside the square brackets indicates the main period in which the campaigns were rolled out) (1) False information related to the theory of the origin of the new coronavirus disease (COVID-19) and the formation of a counter-narrative to the theory that it originated in China [over one year from about August 2020] (2) Formation of a narrative emphasizing the decline of the United States' ability to contribute to the stability of the international community and the rise of China as a player responsible for stabilizing the regional order, taking up the South China Sea issue and the U.S. withdrawal from Afghanistan as examples. [about August 2021], (3) Dissemination of a narrative exposing and emphasizing the brutality of U.S. law enforcement agencies, racial discrimination, and other social issues in relation to the second anniversary of the death of Mr. George Floyd, who was killed by a U.S. police officer in May 2020 [about May 2022], (4) Disseminating a narrative and false information that the deepening allied cooperation between the United States and Europe and the strengthening of pressure on Russia are worsening the situation in the Russia-Ukraine war and the economic situation of countries that support Ukraine. [about May 2022], and (5) The dissemination of a narrative emphasizing that racial discrimination in the United States, the response to the pandemic, and social divisions within the country are all in a serious state during the U.S. Independence Day and the midterm election season [about July 2022].

[43] For that reason, since publication of the indictment documents concerning 912-SPWG, analysts at Meta and others have arrived at the assessment that some of the past campaigns using Spamouflage are likely attributable to the MPS. Refer to the following: Alexander Martin, "Chinese Law Enforcement Linked to Largest Covert Influence Operation Ever Discovered", *Recorded Future*, August 29, 2023, https://therecord.media/spamouflage-china-accused-largest-covert-influence-operation-meta; Katie Paul, "Meta Pins Pro-China Influence Campaign on Chinese Law Enforcement", *Reuters*, August 29, 2023, https://www.reuters.com/technology/meta-pins-spamouflage-influence-

campaign-chinese-law-enforcement-2023-08-29/.

[44] United States v. Wu Haibo, et al., 8-9.

[45] For example, refer to the following analysis by the Australian Strategic Policy Institute regarding an example of digital influence operations with the suspected involvement of a local public security agency in Yancheng City, Jiangsu Province. Albert Zhang, Tilla Hoja, and Jasmine Latimore, "Gaming Public Opinion: The CCP's Increasingly Sophisticated Cyber-Enabled Influence Operations", Australian Strategic Policy Institute, April 2023, 14–18, http://www.aspi.org.au/report/gaming-public-opinion.

[46] United States v. Yunpeng Bai, 39–40, para. 64. The FBI special agent who prepared the indictment letter expressed the view that based on the timing of this communication this coordination likely included topics related to the U.S. government's response to the COVID-19 pandemic, developments in Hong Kong, the murder of George Floyd, and the influence operations in the 2020 U.S. presidential election.

[47] This is part of the "anti-corruption" campaign by the Chinese authorities, including the MPS, which has the purpose of repatriating to China any persons suspected of involvement in economic offenses, including corruption, who have fled overseas, and recovering overseas assets which are thought to have been illegally accumulated by those persons. Fox Hunt has been implemented every year since 2014 and the MPS claims that its "outcomes" as of 2024 are the repatriation of 9,000 suspects from 120 countries around the world and the recovery of assets worth approximately 49 billion renminbi ("The MPS Deploys Fox Hunt 2024 Special Operation [公安部部署開展"猎狐2024"専項行動]" MPS website, April 23, 2024, https://www.mps.gov.cn/n2254314/n2254487/c9547365/content.html).

[48] United States v. Yunpeng Bai, 57-63.

[49] Institute of Party History and Literature of the Central Committee of the Chinese Communist Party ed. "Xi Jinping on the Holistic Approach to National Security [習近平関于総体国家安全観論述摘編]" (Beijing: *Central Party Literature Press*, 2018), 4.

[50] YAMAGUCHI Shinji [山口信治], "The Ideological Struggle of China's Xi Jinping Regime: Opposition to Peace Evolution and Color Revolutions and International Discourse Power [中国・習近平政権のイデオロギーをめぐる闘争—和平演変・カラー革命への対抗と国際的話語権－]", *Roles Report*, No.17 January 2022, 1-2.

[51] LI Rui [李鋭] and LU Ying [陸穎], "Deep Implementation of Xi Jinping's Thoughts on the Rule of Law and Continuous Strengthening of the Construction of the Rule of Law in the Public Security Field [深入貫徹習近平法治思想不断加強公安渉外法治建設]", *Policing Studies* Vol.2 2025, 9. Li is the Deputy Head of the Legal Affairs Unit of the Shanghai Public Security Bureau and Lu is a member of that unit.

PROFILES

GOTO Yohei

Research Fellow, China Division, Regional Studies Department

Areas of Expertise: China's diplomatic and security policy, etc.

SETO Takashi

Research Fellow, Cyber Security Division, Policy Studies Department

Areas of Expertise: intelligence, cyber and information warfare, security, etc.

Planning and Coordination Office

National Institute for Defense Studies
Telephone (direct) : 03-3260-3011
Telephone (general) : 03-3268-3111 (ext. 29177)
National Institute for Defense Studies website: www.nids.mod.go.jp