防衛研究所 National Institute for Defense Studies
NIDSコメンタリー
特集：「新領域の安全保障」vol. 7
第 371 号　2025 年 4 月 25 日

対外工作機関としての中国公安部

――公開情報分析から辿る、近年の対外的な工作活動とその内在的論理※

地域研究部 中国研究室 研究員　後藤　洋平

政策研究部 サイバー安全保障研究室 研究員　瀬戸　崇志

はじめに―― グローバル化する中国公安部による非公然な対外工作

2025 年 3 月 4 日、米国司法省は、「米国 対 呉海波 他 事件（U.S. v. Wu Haibo et al）」（以下：「呉海波事件」）と呼ばれる公訴事案の起訴状を公表した。同事案は、2016 年から 2023 年にかけての各国への一連のサイバー攻撃事案に関与した罪状で、中国国籍の容疑者計 10 名を起訴している。このうち 8 名は、中国政府機関からの委託を受けた同国の民間企業の従業員だが、残りの 2 名は、中国公安部（以下、「公安部」）の地方機関の要員である[1]。

ここで言う「公安部」とは、中国の「国内」の法執行・防諜機関を司る中央省庁及びその地方機関（公安局/公安庁/公安処）の総称である。表面的には日本の警察庁と都道府県警察の関係にも似た組織構造を取る警察機構である公安部は、国家安全部などと並んで、中国の国内法執行機関・防諜機関の一つと認識されている。

しかし、公安部の任務が、国内のみで完結するのかといえば、必ずしもそうではない。公安部の対外的な任務には、例えば海外に在住する中国国民の犯罪への対処（反腐敗の取締りを逃れた在外自国民の送還及び海外資産の回収を含む）ならびにテロ対策等を目的とした、海外の法執行機関との国際司法共助[2]の取組がある。このほか、「一帯一路」の沿線国であるクロアチア、ラオス、ミャンマー、セルビア、タイなどの治安機関との合同パトロールやソロモン諸島での警察官の訓練[3]をはじめ、各国治安当局との共同訓練・能力構築支援なども実施している。こうした公安部の対外的な任務は、特に習近平政権の成立（2012 年）以降に拡大を続けており、その動静と含意は、多くの体系的・実証的な分析が存在する[4]。

その一方で公安部は、前段で触れた「法執行機関」の国際協力の範疇に収まる活動と並行して、まさに冒頭の「呉海波事件」のような、他国に対する非公然な対外工作にも同時に従事してきた。こうした非公

然な対外工作は、これまでも報道等で耳目を集めることあれども、かかる活動の概要や背後にある内在的論理について、体系的かつ実証的な分析がなされる機会は少なかったといえる。

改めて、公安部とは一体「何者」なのか。なぜ、法執行機関としての顔と、非公然な対外工作機関としての顔が両立しうるのか、こうした問題意識を踏まえて、本稿では、公安部による非公然な対外工作の内在的論理を捉えていきたい。以下では、公安部の沿革・任務を要約する。その後、近年の公安部の物理空間とサイバー空間を通じた非公然な対外工作の主要事例につき、米国司法省等が機密指定を解除した起訴状・宣誓供述書等の公訴資料や、中国企業等から流出した内部文書を含む多様な公開情報（PAI：publicly available information）を駆使しつつ概説する。

1．公安部の概要

公安部は 1949 年、中華人民共和国の成立とともに設立され、幾度かの内部機構の改革を経ながらも、設立以来、その名称と役割が大幅に変更されることはなかった。公安部長は、外交部長や国防部長などと同様、副総理に次ぐ位置付けの国務委員を兼ねており、中国共産党（以下、「共産党」）及び国務院[5]における地位の高さとその役職の重要性が見て取れる。中国では、中央の機関のほか、各地方にも政府機関が存在するが、公安部門も、上級の部門から順に、中央に公安部、省・自治区に公安庁、市（北京市、上海市などの直轄市含む）・県に公安局、より下位の地方機関には処や分局が設置されており、下級の機関は上級機関の指導を受ける[6]。公安部（以下では、下級の機関も含めた総称として使用。特に必要がない限り、以下同様）の HP では、その主な職責として、経済犯罪の捜査、治安管理、刑事犯罪の捜査、サイバーセキュリティの保全、反テロ、違法薬物の取り締まり、国際協力、法制整備等を挙げている[7]。

公安部 HP では明確にされていないが、「刑事（経済）犯罪の捜査」や「反テロ」、「サイバーセキュリティの保全」などの任務には、一般的な刑事犯罪のみならず、共産党の統治を脅かし得る個人・組織の調査・取り締まりも含まれるものと考えられる。むしろ、そうした政治的色合いの事案を担当することが優先度の高い任務として位置付けられていることは、公安部の各種会議等でも強調されている。例えば、2024 年 1 月に開催された全国公安庁局長会議では、「国家の政治安全[8]の防衛」が第二の重要任務（第一の重要任務は、「共産党の絶対的領導の実施」）に挙げられており、その中味として、外部の敵対勢力の浸透・転覆・かく乱・破壊活動の予防・取り締まり、政治的なデマや有害情報の取り締まりを含むネット上の闘争の強化、反テロ・反分裂（台湾、ウイグル、チベット、香港等の「独立分子」への対処が想定）活動の強化、党による民族・宗教政策の貫徹、カルト組織の取り締まりなどが列挙された[9]。

中国当局は、政策文書や、各種国家安全に関する法規においても、公安部による対外的な任務を根拠付

けようとしているとみられる。例えば、党中央が 2021 年 1 月に発表した「法治中国の建設に関する規則（2020～2025 年）」では、法執行に関する国際協力への積極的参加、暴力的テロ勢力・民族分裂勢力・宗教過激勢力・薬物密売・密輸・国境を跨ぐ組織犯罪の共同対処、反腐敗の国際的協力など、他国と協力する形で一般犯罪及び党にとって安全保障上の脅威に対処する方針が記載された[10]。また、習政権下で制定されたサイバーセキュリティ法（2016 年）、データセキュリティ法（2021 年）、反電信・ネットワーク詐欺法（2022 年）などの法律においては、公安部（条文上は「公安機関」）が域外での事案を捜査したり、責任の追及を可能にしたりする条文が盛り込まれている[11]。すなわち、相手国が受け入れれば、公安部が国外での法執行を実施することが可能とも解釈することができる。

一連の法規については、中国当局の裁量の広さや、保護法益たる「国家安全」や「公共の利益」などの定義・取り締まりの対象に関する曖昧さ等の問題が指摘できるほか、中国に送られた「被疑者」の人権面での懸念はある。しかし、これら法規を含む中国国内法の域外適用が、他国との間で結んだ条約・協定等に基づき実施された場合、その二国間に限れば、一応の「合法性」が担保できると言えよう。

ただし、公安部は、そうした二国間の条約等が締結されていないか、又は締結されていても中国の人権状況を懸念し、引き渡しに応じない国においても、事実上の強制的手段によって「被疑者」の中国帰還を促しているとみられる[12]。そうしたケースにおいて多用されるのが、「望まざる帰還（involuntary return）」と呼ばれる手法である。スペインの人権団体・セーフガード・ディフェンダーズは、その手法について、①中国に在住するターゲットの家族を人質に取る、②ターゲットに直接的又は間接的に接触し、脅迫や嫌がらせを行う、③ターゲットを海外で拉致する、という 3 つが存在すると指摘する[13]。以下の「海外警察拠点」の節では、公安部が海外に非合法な拠点を設置し、「被疑者」とみなす中国籍の海外在住者に「望まざる帰還」を含む働き掛けを行っている事例を紹介する。

2．海外警察拠点―公安部による違法な域外法執行

（1）「海外 110」[14]の概要

セーフガード・ディフェンダーズは 2022 年 9 月、主として中国の公安局が、世界中で「海外警察拠点」を設置している状況を指摘するレポート「海外 110（110 Overseas）」を発表した。同レポートは、福建省福州市の公安局をはじめ地方都市の公安局が、電信詐欺など越境犯罪を取り締まることなどを目的に、現地に「海外警察サービスステーション（中国語：警僑事務海外服務站。以下では「海外警察拠点」）」を次々に設置していることを、中国側の公開情報等を基に指摘している。同海外警察拠点は、公安局が直接運営しているわけではなく、その公安局が所在する自治体をルーツとする華僑団体が担い手となってい

る。同拠点は、表面的には、現地華僑が、中国での運転免許更新等を実施するサービスを提供することをうたうものの、中国側報道は、「華僑関連の各種犯罪・違法行為を断固取り締まる」ことが目的であると指摘する[15]。同レポートは福州市公安局及び浙江省青田県公安局が設置した海外警察拠点が、31 か国 43 拠点に及ぶとしている。この数字は、セーフガード・ディフェンダーズが同レポートのフォローアップとして発表したレポートにより、53 か国 102 拠点に修正された[16]。

これに関連して、安田峰俊は、中国側が用いる「警僑服務」という単語は 2016 年頃から中国側の公開情報に用いられるようになったと指摘する[17]。さらに、地方の公安局が海外警察拠点を設置する動きを推進した目的は、習近平政権による民間団体介入への動き強化と連動する形で、これまで海外の華僑団体が私的に行っていたトラブル調停や故郷への連絡等の業務に食い込むためであったと分析している[18]。

（2）海外警察拠点を用いた中国反体制派に対する監視・脅迫

海外警察拠点が、運転免許の更新や、一般刑事犯罪の取り締まりのみに利用されていたとしても、同拠点の設置それ自体が、中国も批准している外交関係に関するウィーン条約が規定する、接受国の同意を得ない政府代表機関設置の禁止（第 12 条）に違反する行為である。さらに、同拠点が中国出身の反体制派に対する政治的迫害に利用され、現地国当局から取り締まりを受けた事案も存在する。

米司法省のプレスリリース[19]によると、連邦捜査局（FBI）は 2022 年 10 月、福州市公安局の指示を受け、ニューヨーク市に違法な海外警察拠点が設置されている疑いで華僑団体のオフィスを捜索し、同団体の関係者であった盧建旺と陳金平が公安部のエージェントとコンタクトを取っていたことを確認した。その後の調べで、両名は公安部とのつながりの証拠を隠滅したり、FBI の捜査を妨害したりしようとしていたことが明らかになったため、FBI は 2023 年 4 月、両名は陰謀の罪と捜査妨害の罪で逮捕した[20]。逮捕後、盧が公安部の指示の下、ワシントン D.C.で反中国抗議集会のカウンター集会を組織したこと（2015 年）[21]、米国在住の中国人亡命者に対し、脅迫を用いて中国に戻るよう促したこと（2018 年）、カリフォルニア州在住の中国人民主活動家の身元割り出しの補助を行っていたこと（2022 年。盧は関与を否定）などが明らかになった。

上記の事例から、何が言えるだろうか。他の海外警察拠点の事例にも言えることだが、指示は公安部が出す一方、「法執行」は現地華僑が実行しているということである。公安部に限らず、中国当局はかねてより、華僑を統一戦線工作の対象として取り込み工作を推進しており、華僑団体幹部が中国で当局から表彰を受けたり、共産党が主催するイベントに出席したりといった「栄誉」を受ける一方、台湾問題をめぐる中国の立場を支持する活動に関与するなど、中国当局の意向を汲んだ政治的活動が求められているとされる[22]。盧の事例においても、上記の活動において公安部幹部から表彰を受けたことがあり、公安部から便宜を供与され、そのエージェントとなっていたことが看取される。公安部にとっても、実行者との

関係を否定することで「使い捨て」にすることが可能であり、現地当局から取り締まりを受けた場合のリスクを低減することができるだろう。

3．サイバー攻撃キャンペーン ― I-Soon 社関連情報から捉える 3 つの特徴

公安部は、海外警察拠点を通じた域外法執行活動と並行し、中国国外の様々な標的からの秘密裡の情報収集または脅迫のためのサイバー攻撃の遂行に関与してきた。本稿冒頭で扱った「呉海波事件」の起訴状[23]の内容、この「呉海波事件」の起訴対象者 8 名が所属する中国のサイバーセキュリティ企業「安洵信息技術有限公司（Anxun Information Technology Co. Ltd.）」（通称 I-Soon 社）に関して、2023 年から 2024 年にかけて公知とされてきた情報、そして各国の民間セキュリティ企業・専門家による技術的な分析も組み合わせると、公安部の関与するサイバー攻撃について、特に次の 3 つの特徴が浮かぶ。

第 1 の特徴は、サイバー攻撃の目的・標的にある。前節で触れた海外警察拠点の活動や後述のデジタル影響工作の事例も含め、公安部による非公然な対外工作活動は、現行の共産党統治を不安定化させる言動にあらゆる手段・局面で対処する「政治警察」としての機能に由来する。それゆえに、公安部の関与が疑われるグループによるサイバー攻撃の矛先は、現行の共産党統治に批判的な亡命知識人や民族的・宗教的少数者のほか、こうした勢力を支援する第 3 国の報道機関や市民社会団体に向けられる傾向を持つ。

例えば「呉海波事件」の起訴事由には、公安部と共謀した I-Soon 社従業員が、米国内外に所在する報道機関や宗教団体からの個人情報窃取を通じ、標的個人の言動の監視や所在地・渡航先把握といった情報収集(intelligence collection)のためにサイバー攻撃を活用する事例が幾つか含まれる[24]。こうした情報収集は、その後の公安部（または国家安全部）による、中国国内外での「法執行」活動を支えるターゲティングが目的と捉えうる。また、米国のセキュリティ企業 Recorded Future 社の調査部門による、2024 年 2 月に GitHub 上で公表された I-Soon 社の内部文書[25]の分析によると、同社のサイバー攻撃ツール・インフラや攻撃手法の一部は、従来命名・観測されてきた「Red Alpha」や「Poison CARP」といった攻撃グループとも重複を見せる[26]。両者は、いずれも従来チベット及び新疆ウイグル自治区問題に関連した中国内外の個人・団体からの情報収集に積極的だった攻撃グループである[27]。この点も（I-Soon 社への委託関係を介した）公安部の関与の下でのサイバー攻撃の目的・標的のパターンを傍証するものといえる。

第 2 の特徴は、サイバー攻撃の能力整備・運用の両局面に跨る、中国国内の民間サイバーセキュリティ企業に対する委託関係の存在である。例えば「呉海波事件」の起訴状によると、I-Soon 社は、公安部要員が独力でサイバー攻撃を実施する能力を獲得するための教育訓練の提供に加えて、I-Soon 社の社員自身が、公安部要員の指示に沿ったサイバー攻撃を実施し、その成果物（窃取情報）を公安部に提供すると

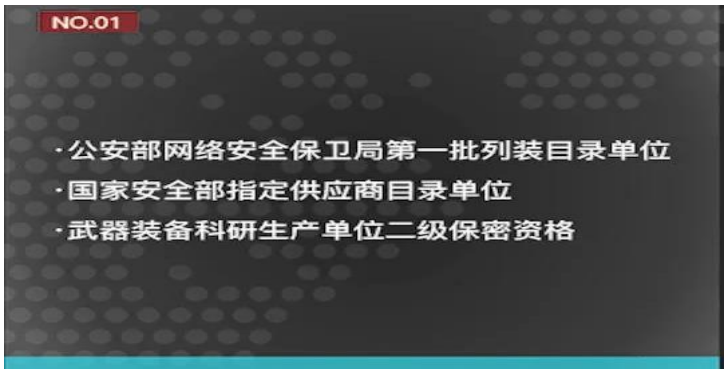
いった、実際のオペレーション（能力運用）の部分まで委託[28]されてきた点が特筆に値する。

具体的には「呉海波事件」の起訴状では、I-Soon 社が「少なくとも 31 以上の地方政府（provinces and municipalities）おける公安部または国家安全部の関係部局から、43 件以上の委託を受けてきた」[29]との公訴事実が記載されている。また、I-Soon 社の公式 HP の資料等を利用した 2023 年 10 月の公開情報調査によると、同社は各々の地方機関を含む公安部と国家安全部を顧客としていることや、公安部サイバーセキュリティ局（公安部網絡安全保衛局）への製品納入等を認められた事業者であることを積極的に宣伝してきた[30]。これらは I-Soon 社の、特に公安部からの有力な事業委託先としての地位を示す。

第 3 の特徴は、能力整備・運用における「地方機関」の自律性である。かつて I-Soon 社の HP では、中国全土に所在する約 43 の地方公安機関との取引関係が堂々と宣伝されてきた[31]。また図表 2 は、2024 年 2 月に、GitHub 上で公表された I-Soon 社の契約実績リストだが、左から 3・6・7 列目の記載を併せてみると、32 件の契約の内訳は「公安」が 18 件と最多である。そして、この「公安」または「安全」に分類される契約の多くは、各種フロント企業経由のものも含め、公安部や国家安全部の地方機関を最終顧客とする。これらは、いわゆる中国による国家支援型のサイバー攻撃能力は、必ずしも集権的管理下にはなく、公安部や国家安全部の「地方機関」を含む分権的なエコシステムに支えられていることを示す[32]。

こうした「地方機関」と、その事業委託先・フロント企業等を含めた重層的なネットワークからなる能力の整備・運用モデルは、運用保全へのリスク管理の観点等から、サプライヤーの限定や能力運用の内製化の誘因が強い欧米諸国の軍隊・情報機関のサイバー攻撃能力の整備・運用のモデル[33]とは大きく異なる。この点は中国のサイバー攻撃能力を分析・把握するうえでの固有の課題を提起しているといえよう。

図表 1：I-Soon 社 HP[34]での公安部・国家安全部による納入実績の宣伝



出典：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.

図表 2：GitHub 上で公表された I-Soon 社の契約実績リスト（2016 年-2018 年頃）

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钡业务系统采购合同》	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钡业务系统
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	2017031301	企业	/	《网站渗透测试技术服务》（未回签）	食乐小球渔积分管理（深圳）有限公司	食乐小球渔积分管理（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》	云南省巍山县公安局	巍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	GATWAZDTZ201803	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

出典：2024 年 2 月 16 日に GitHub 上で公表された、I-Soon 社文書の画像ファイルを基に執筆者作成（赤枠は強調のため執筆者追記）。本リストと同様のデータを活用している過去の調査報道等については、例えば次を参照。「Web 特集：追跡 中国・流出文書 4 『公安』」日本放送協会（NHK）、2024 年 10 月 2 日、https://www3.nhk.or.jp/news/html/20241002/k10014588431000.html（2025 年 4 月 12 日アクセス）；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）

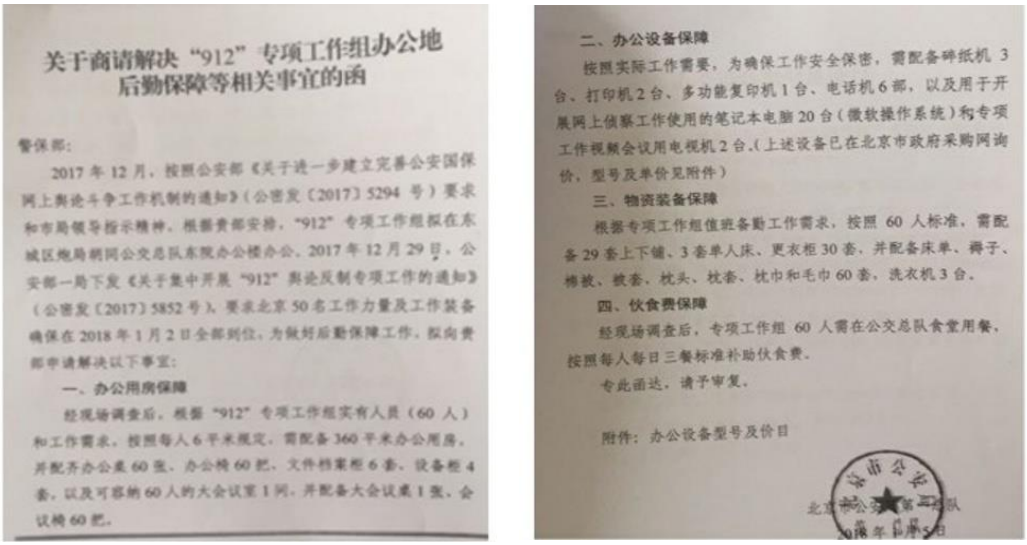
4．デジタル影響工作―― 912 特別行動ワーキンググループ

公安部は、ソーシャル・ネットワーク・サービス（SNS）での悪意ある情報拡散といった、サイバー空間の機能を媒介とした影響工作（以下、「デジタル影響工作」[35]）にも着手してきた。ここでは、公安部のデジタル影響工作の沿革・発展を捉えるうえで、「912 特別行動ワーキンググループ（九一二専項工作[小]組）（912-SPWG：912 Special Project Working Group）」（以下、「912-SPWG」）について触れておきたい。

912-SPWG とは、2023 年 4 月 17 日付で米司法省判断により機密指定が解除された「米国 対 白雲鵬他 事件（US v. Yunpeng Bai, et al.）[36]」（以下：「白雲鵬事件」）の公訴資料を通じて存在が暴露された、公安部の隷下のプロジェクト・チームである（図表 3-1）。「白雲鵬事件」は、この 912-SPWG に所属する

管理責任者・実務担当者となる公安部第 1 局・第 5 局・第 11 局要員[37]ならびに北京市公安局要員を含めて合計 34 名を、米国内外の個人・団体を標的としたデジタル影響工作ならびに関連する余罪で起訴している[38]。同事案の公訴資料の内容は、各国の民間企業・研究機関による公開情報調査の結果等とも照らし合わせることで、公安部のデジタル影響工作の様相について 3 つの示唆を与えてくれる。

図表 3-1：FBI が証拠品として提出した 912-SPWG の物品調達等の記録



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。

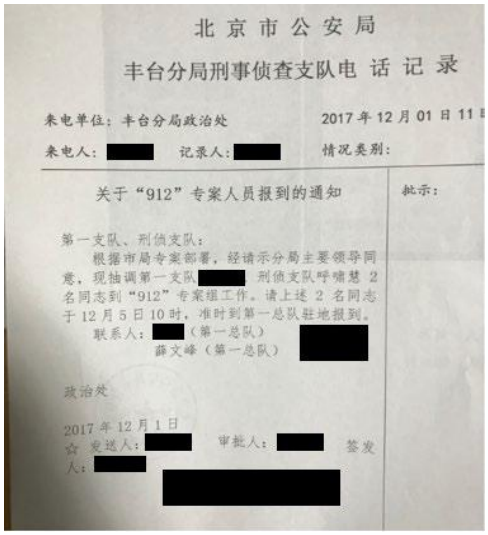
专此函达，请予审复。

附件：办公设备型号及价目

出典：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)

第 1 に、912-SPWG の組織編制である。「白雲鵬事件」の公訴資料によれば、同事案の起訴対象となった 34 名は、北京市公安局の施設内に置かれた司令グループ（command group）要員となる。この北京市の司令グループは、公安部の「912（特別）プロジェクト」と呼ばれる事業の中核だが、他方で中国全土の 15 以上の省等の地方公安機関からも「912」プロジェクトへの要員が派遣（図表 3-2）されており、同工作が中央からの指示に基づく全国的な規模のものであることが示されている[39]。

図表 3-2：FBI が証拠品として提出した 912 工作に関する人事関連の文書



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。

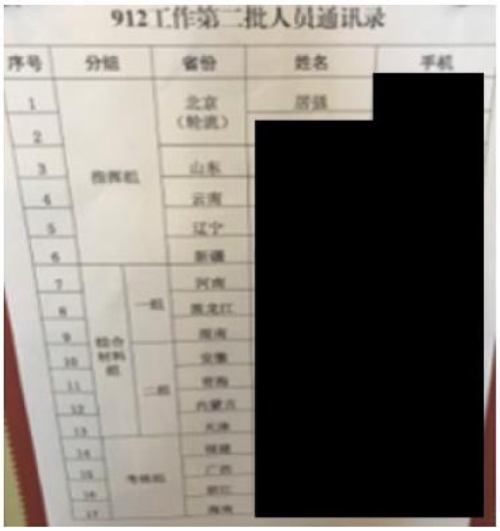
联系人：[redacted]（第一总队）

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

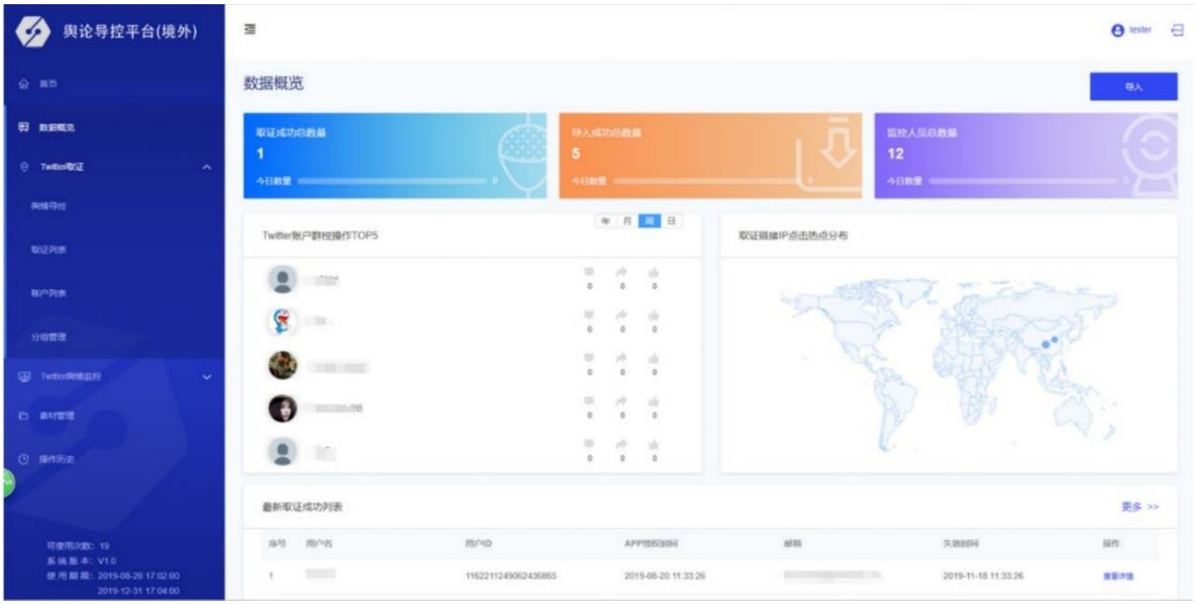
序号	分组	省份	姓名	手机
1		北京（轮流）	[redacted]	[redacted]
2				
3	指挥组	山东		
4		云南		
5		辽宁		
6		新疆		
7		河南		
8	综合材料组	一组	黑龙江	
9			湖南	
10			安徽	
11		二组	湖南	
12			内蒙古	
13			天津	
14			福建	
15		考核组	广西	
16			浙江	
17			海南	

出典：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)

第 2 に、912-SPWG の任務と具体的な活動実態である。まず「白雲鵬事件」の公訴資料は、2020 年 3 月頃の公安部の内部文書の存在に言及する[40]。その上で 912-SPWG の主要任務を「中国政府・共産党のプロパガンダ・言説を様々な SNS で宣伝するオンライン空間認識管理 (online perception management)キャンペーンを実施し、政府と共産党のプロパガンダ・言説を多岐に渡る SNS で促進し、これに挑戦する言論の信用失墜や対抗言説での圧倒により、批判者を威嚇し沈黙させる」[41]ことと評価する。

そのうえで公訴資料は、2021 年以降に 912-SPWG 要員が関与してきたとされるデジタル影響工作の具体例[42]を示すが、このうちの幾つかの事例の内容（標的・時期・手法等）は、過去に民間セキュリティ企業や研究機関が「Spamouflage」（または「DRAGONBRIDGE」）と呼称してきた中国政府機関の関与が疑われてきたデジタル影響工作の内容とも一部が重複する[43]。また、第 3 節で触れた I-Soon 社の社員を対象とした「呉海波事件」の起訴状も、I-Soon 社が公安部に Twitter（現：X）アカウントの窃取機能を含むデジタル影響工作用ツール（図表 4）を納品してきた事実を指摘する[44]。この他の公安部の関与が疑われる関連事案の分析結果[45]や図表 3 の行政文書の起案日も総合すると、公安部は遅くとも 2017 年頃から 2020 年頃までに、デジタル影響工作の能力整備と運用に着手してきたことはほぼ確実といえる。

図表 4：I-Soon 社が公安部に納入したとされるデジタル影響工作ツールの画像



出典：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).

最後に、中国の対外的な影響工作をめぐる、公安部と、他の党・政府機関の有機的なネットワークである。「白雲鵬事件」の公訴書状では、例えば 912-SPWG と、中国共産党統一戦線工作部ならびに国家安全部との関係が言及されている。前者については、公訴資料では 912-SPWG 要員である襲岳（Xi Yue） と覃金燕（Tan Jinyan）の 2020 年 6 月頃のチャットの記録の存在が言及され、そこでは「(襲岳が）非常に多くの統一戦線工作部の要員との仕事をこなす必要があることを嘆いている」[46]との言及がある。この点は、党機関たる統一戦線工作部が、公安部のデジタル影響工作に一定の影響力を行使してきたことを示唆する。

後者の国家安全部との関係では、例えば 2010 年代後半以降の同部による「狐狩り」[47]作戦の標的であった「被害者 1（Victim-1)」やその支援者につき、912-SPWG が運用する SNS アカウントを活用して得た標的情報を国家安全部に提供するなど、主に情報収集・ターゲティング面の支援を及ぼしてきた旨の記述がある[48]。こうした活動様式は、第 3 節で触れた公安部関連のサイバー攻撃の傾向にも共通する。すなわち公安部や国家安全部が、サイバー空間を媒介とする各種の作戦能力を、第 1 節・第 2 節で触れたような物理空間での域外法執行活動を支援する手段としても重視していることを示している。

5．おわりに―― 公安部による非公然な対外工作の内在的論理

以上のとおり、公安部は物理・サイバー空間の双方における非公然な対外工作を強化してきた。それでは、元来は犯罪の取締りを主たる任務とする法執行機関であるはずの公安部が、他国に対する非公然な工作活動にも関与してきた背景とは、一体何であろうか。

一つの手掛かりは、習国家主席が 2014 年に提唱し、中国の安全保障をめぐる基本的な概念となった「総体的国家安全観」であると考えられる。習国家主席は、総体的国家安全観の文脈において、外部の安全と内部の安全を共に重視すべきであると指摘している[49]。すなわち、国内の安全に対する脅威は、国外からもたらされ得るという問題意識を示したものと言えよう。公安部が取り締まる対象に引き付けて考えると、国境を跨ぐ刑事犯罪は、まさに中国国内の治安に対する脅威となっている。また、反腐敗の取り締まりから海外に逃れた元官僚・党幹部などは、潜在的に共産党統治を脅かす存在になる。さらに、民主化運動が外国と結びつく形で発生するとの見方が中国で主流を占めつつある中[50]、海外の反体制的傾向を有する中国人も、公安部にとっては、国内の反体制派同様、取り締まるべき存在と映るだろう。

このように公安部としては、国内外、さらに物理・サイバー空間を問わず、共産党統治の脅威になる存在は、「法執行」又は「懲罰」の対象とみなしているものとみられる。実際に公安部関係者の中にも、総体的国家安全観に基づく対外的（中国語原文は「涉外」と表現）犯罪の取り締まりの必要性を説く見方が存在する[51]。こうした総体的国家安全観から演繹的に導かれた、共産党統治を守る「政治警察」の機能を追求する観点からは、公安部にとっては「国内」と「国外」という地理的区分や当該活動の性質は、自身の警察機構としての任務の外延を縛るものではないということだろう。

こうした公安部による対外工作の拡大は明白な潮流としてありながらも、同様なを担う国家安全部との役割分担や、具体的な活動を担う際の地方機関の権限・裁量や中央からの統制の有無など、公安部の対外工作には、依然として不透明な部分が多い。本稿において概説してきた近年の事例は、公安部が、実は統一戦線工作部、国家安全部、人民解放軍といった他の公的機関と同様に、中国の総体的国家安全観に基づく対外的な工作を支えるアクターであり、そうした観点からの研究対象としても価値を有していることを示唆しているといえよう。

（2025 年 4 月 16 日 脱稿）

※ 本稿は、中国研究室後藤が 1 節・2 節、サイバー安全保障研究室瀬戸が 3 節・4 節に責任を負う分担執筆制を採りつつ、序論・結論の執筆ならびに英語・中国語の双方の情報源による分析内容の照合は共同で担当した。

[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] 中国の対外的影響力拡大などの観点から、公安部を含む中国当局の国際的法執行協力を分析した研究として、Eric Green etal. “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;益尾知佐子「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」『国際問題』（No.715、2023 年 10 月）などが存在。
[5] 国務委員は、国家の指導者層（国家領導人）のうち、国務院副総理や全人代副委員長とともに副職級に位置付けられており、これは、共産党の中央政治局委員等とおおむね同等とされる（澎湃新聞、2014 年 10 月 12 日、https://www.thepaper.cn/newsDetail_forward_1270347）。
[6] 公安部も含む治安機関（人民警察）の活動を規律する人民警察法（1995 年制定）第 43 条は、上級機関は下級機関の法執行活動を監督する旨規定。
[7] 公安部 HP、http://www.mps.gov.cn:8080/。
[8] 政治安全とは、共産党による統治と社会主義体制の安全を守ることとされる（松田康博「中国による『政治安全』と国内安全保障体制」日本国際問題研究所研究レポート第 11 号、2021 年 5 月 6 日、https://www.jiia.or.jp/research-report/post-102.html）。
[9] 「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」公安部 HP、2024 年 1 月 14 日、https://www.mps.gov.cn/n2254314/n2254315/n2254317/n8928114/n8928175/c9391083/content.html。
[10] 「中共印発 『法治中国建設規則（2020～2025 年）』」中国政府網、2021 年 1 月 10 日、https://www.gov.cn/zhengce/2021-01/10/content_5578659.htm。
[11] サイバーセキュリティ法では、域外（香港、マカオ、台湾含む。以下同じ）の個人・組織が中国の情報インフラに攻撃・侵入した場合、公安部が当該個人・組織に制裁を実施できる旨規定（第 75 条）。データ安全法では、中国域外におけるデータ処理が、中国の国家安全、公共の利益等を侵害した場合、法に基づき責任追及する旨規定（第 2 条）されるほか、公安部、国家安全機関（部）に犯罪捜査を理由とした調査権限を付与（第 35 条）。反電信・ネットワーク詐欺法では、中国域外の個人・組織が中国内で電信・ネットワーク詐欺を行った場合又はそのためのほう助を行った場合の責任追及を可能にする旨規定（第 3 条）しているほか、公安部が反電信・ネットワーク詐欺業務をリードする旨規定（第 6 条）。
[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] （1）の内容は、特に断りがない限り、Ibid.の記載に基づく。なお、中国では日本同様、警察（公安）に通報する際の番号は 110。
[15] 中国長安網（中央政法委員会の公式メディア）、2022 年 7 月 29 日、http://www.chinapeace.gov.cn/chinapeace/c100049/2022-07/29/content_12654617.shtml; Ibid, 12.。
[16] 他の地方の拠点設置状況なども加味して修正（Safeguard Defenders, “Patrol and Persuade: A follow-up investigation to 110 Overseas”, December 2022 5-7）。
[17] 安田峰俊『戦狼中国の対日工作』文春新書（2023 年）33 頁。
[18] 同上、34-35 頁。
[19] 以下の内容は、特に断りがない限り、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 に基づく。
[20] その後の裁判で、盧は無罪になった一方、陳には有罪が宣告された（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] 盧はこの活動の結果、公安部幹部から表彰された模様（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] 2024 年 2 月に GitHub 上で公表された I-Soon 社の内部文書（2025 年 4 月現在、原文は GitHub 上からは削除済）の流出経緯やその内容に関する詳細な分析は、例えば次を参照。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] 両グループの過去のキャンペーンの詳細は例えば次を参照。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] この点は、2024 年 2 月 19 日時点の I-Soon 社の公式 HP のアーカイブから確認できる。以下を参照。「合作伙伴—警企合作」安洵信息技術有限公司 HP、2024 年 2 月 19 日アーカイブ、https://web.archive.org/web/20240219105947/http://www.i-soon.net/pc_partner.html （2025 年 4 月 16 日アクセス）

[32] 特に中国のサイバー攻撃能力整備・運用のエコシステムの特殊性については、以下の先行研究も参照。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] 運用保全リスクの管理や法令遵守の要請に規定された、欧米の民主主義国における軍事組織・インテリジェンス機関のサイバー攻撃能力の整備・運用モデルについては、以下の先行研究を参照。瀬戸崇志「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—」『安全保障戦略研究』第 4 巻第 2 号（2024 年 3 月）184-186 頁; Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber Force* (London: Hurst Publishers, 2022), 8-10, 147-161.

[34] この図表-1 と同様の内容は、2024 年 2 月 19 日時点の I-Soon 社の公式 HP のアーカイブからも確認できる。以下を参照。「関于我們—発展歴程」安洵信息技術有限公司 HP、2024 年 2 月 19 日アーカイブ、https://web.archive.org/web/20240219105939/http://www.i-soon.net/aboutUs_history.html （2025 年 4 月 16 日アクセス）

[35] 当該概念に関しては次のような文献を参照。一田和樹 他 『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』（原書房、2023 年）; 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）. なお、この「白雲鵬事件」の公訴関連書類は、2025 年 4 月 16 日時点では米司法省 HP からのリンクが切断されているが、同年 2 月 4 日時点上のアーカイブ済の URL（上記参照）から原文を確認できる。

[37] United States v. Yunpeng Bai, et al, 12, para. 15. 公訴書類によれば、ここでいう第 1 局とは国内防諜/亡命政治犯抑圧等担当、第 5 局は刑事犯罪捜査担当、そして第 11 局はネットワーク/インターネット安全を担当する部局とされる。

[38] 次を参照 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. 公訴書状によれば、捜査過程で収集したとされる「2020 年 3 月の公安部の提言書（an MPS proposal from March 2020）」と呼ばれる文書（原文非公開）があり、同書は「殆どの諸外国報道が中国に対してネガティブであり、Twitter 上のコンテンツが中国と共産党への攻撃の約 80%を構成」との認識を前提に「Twitter を含む諸外国のソーシャル・メディア・プラットフォームでの不満分子の活動を監視するための対抗措置の制度化 」との提言を含む。

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

[42] Ibid., 10-11, para. 13. ここで具体的に挙げられているデジタル影響工作キャンペーンの事例は、大きく分けて次のようなものである（[]内は主たる展開時期を示す）（1）新型コロナ感染症（COVID-19）の発生起源説に関連する偽情報・中国起源説への対抗言説の形成 [2020 年 8 月頃- 1 年以上]（2）南シナ海問題・米国のアフガニスタン撤退等を題材とした、米国の国際社会の安定への寄与能力の失墜と、地域秩序の安定化に責任を負うプレイヤーとしての中国の台頭を強調する言説の形成 [2021 年 8 月頃]、(3)2020 年 5 月に米国の警察官に殺害されたジョージ・フロイド（George Floyd）氏の 2 周忌に関連して、米国法執行機関の暴力性、人種差別問題その他の社会問題を暴露し、強調する言説の拡散 [2022 年 5 月頃]、（4）米国と欧州の同盟協力深化や対露圧力強化が、ロシア・ウクライナ戦争の状況や、ウクライナ支援国の経済状況を悪化させている由の言説・偽情報を

拡散[2022 年 5 月頃]、(5)米独立記念日・米国中間選挙シーズンに伴う米国内の人種差別、パンデミック対応、国内社会の分断などがいずれも深刻な状態であることを強調する言説の拡散[2022 年 7 月頃]。

[43] それゆえに、この 912-SPWG に関する公訴書類の公表以降、Meta 社のアナリスト等から、Spamouflage による過去のキャンペーンの一部については公安部に帰属する可能性が高いとの評価が示されるに至った。次を参照。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] 例えば、江蘇州塩城市の地方公安機関の関与が疑われてきたデジタル影響工作の事例について、豪州戦略政策研究所の次の分析を参照。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.　公訴書状の起案者である FBI の特別捜査官は、この会話の時期を踏まえて、これらが COVID-19、香港問題、ジョージ・フロイド殺害事案をめぐる米国政府の対応ならびに 2020 年の米国大統領選挙をめぐる影響工作に関する調整であった可能性が高いとの見方を示している

[47] 汚職を含む経済犯罪に関与した疑いをかけられた者が海外に逃亡した場合、その人物の中国への送還及び当該人物が不正に蓄財したとみられる海外資産を回収することを目的とした、公安部を含む中国当局による「反腐敗」の一環。「狐狩り」は、2014 年以降毎年実施されており、公安部は 2024 年段階の「成果」について、世界 120 か国から 9,000 人の容疑者を送還させ、約 490 億人民元相当の資産を回収したと主張（「公安部部署開展"猎狐 2024"専項行動」公安部 HP、2024 年 4 月 23 日、https://www.mps.gov.cn/n2254314/n2254487/c9547365/content.html）。

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

[49] 中共中央党史和文献研究院 編『習近平関于総体国家安全観論述摘編』（北京：中央文献出版社、2018 年）、4 頁。

[50] 山口信治「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 2022 年 1 月、1-2 頁。

[51] 李鋭・陸穎「深入貫徹習近平法治思想不断加強公安渉外法治建設」『公安研究』2025 年第 2 期、9 頁。李は上海市公安局法制総隊副隊長、陸は同総隊に所属する隊員。

PROFILE

後藤　洋平

地域研究部 中国研究室研究員

専門分野：中国をめぐる安全保障など

PROFILE

瀬戸　崇志

政策研究部 サイバー安全保障研究室 研究員

専門分野：インテリジェンス、サイバー・情報領域と安全保障など

防衛研究所企画部企画調整課

直　通：03-3260-3011
代　表：03-3268-3111（内線 29177）
防衛研究所 Web サイト：www.nids.mod.go.jp