TORNBERG CONSULTING, LLC

PUBLIC SOURCE PACKET

JULY 2026 TRUMP ELECTION INTERFERENCE INTEL RELEASE: TIME-GATED EVIDENCE DECONFLICTION

SOURCE PACKET 2026-01

17 JULY 2026

Prepared for journalists, researchers, public-interest investigators, oversight professionals, and other consumers conducting independent audit or evidence deconfliction.

PUBLICATION STATUS

Public release. Public, declassified, officially released, judicial, technical, and high-quality investigative materials only. No classified access or privileged government access is represented. Internal Tornberg methodology documents are cited with owner authorization but are not reproduced in full unless separately released.

This source packet supports the companion Tornberg Consulting intelligence tradecraft note and Process Summary Report. It is a source-control and audit product rather than a final substantive assessment. Inclusion of a source does not imply adoption of every claim contained within it.

BLUF

Executive Use and Audit Standard

BOTTOM LINE

Every example raised during the collaborative inquiry is mapped to a controlled source record and an explicit evidentiary status. The packet distinguishes direct support, bounded support, official allegation, contextual relevance, correction, and quarantine so that readers can reproduce the reasoning without treating repetition, legal outcome, or later disclosure as automatic corroboration.

The source packet is designed for mass use and maximum transparency. A reader should be able to locate the underlying document, identify when it existed, determine what it directly establishes, see what it does not establish, and understand why a disputed or numerically precise claim was retained, bounded, corrected, or quarantined.

How to Use This Packet

- Begin with the Example-to-Source Crosswalk in Part III. Each example has a unique EX identifier, an evidentiary status, and one or more source identifiers.
- Use Part IV to locate the full citation, direct-access link, evidentiary use, and principal limitation for each source identifier.
- Use Part V to verify the eight uploaded declassified documents by exact filename, page count, and SHA-256 digest.
- Use Part VI to identify the Tornberg Method standards governing evidence, sources, professional judgment, confidence, baseline maintenance, challenge, and auditability.
- Treat the Quarantine Register in Part VII as a preservation mechanism. Quarantined claims are not discarded, but they are excluded from definitive prose and confidence calculations until the missing controls are satisfied.

Status Vocabulary

Status	Meaning
SUPPORTED	A primary or high-quality source directly supports the bounded proposition stated.
SUPPORTED / BOUNDED	The source supports part of the example, while downstream intent, operational use, scale, coordination, or effect remains inferential.
OFFICIAL ALLEGATION	A charging, warrant, complaint, or official investigative product exposes relevant evidence or allegations. Weight comes from the underlying evidentiary substrate, not procedural status.
CONTEXT	The item informs doctrine, priors, risk, or collection design but does not independently establish the proposition under assessment.
CORRECTED	A source supports a narrower formulation and contradicts or fails to support a broader public claim.
QUARANTINED	The lead remains relevant, but source independence, definitions, dates, aggregation, acquisition method, or bridge evidence is insufficient for definitive use.

SOURCE CONTROL

Controlling Evidence Rules

1. Evidence precedes assessment. Every material factual statement and judgment must be traceable to an identified source or clearly marked inferential basis.

2. Four dates are recorded. Event date, reporting or collection date, earliest demonstrated availability to the relevant analytic team, and public-release date are distinct.

3. Government possession is not author access. Information existing somewhere in government is not presumed available to every production team.

4. Source type matters. A raw IIR, coordinated ICA, agency-only note, technical advisory, indictment, email, hearing, and investigative article do not carry identical evidentiary weight.

5. Legal outcome is metadata. Charges, pleas, convictions, dismissals, and sentences describe judicial disposition. Analytic weight derives from communications, technical records, financial evidence, admissions, access, corroboration, and alternatives.

6. Evidence is staged. Capability, priority, collection, processing, consumer delivery, target development, intent, authorization, action, and effect are assessed separately.

7. Repetition is not corroboration. Derivative reporting from a common origin remains one evidence stream until independently confirmed.

8. Policy response is not proof. Statutes, hearings, regulations, sanctions, and mitigation actions reveal institutional risk perception and authority; they do not automatically prove adversary intent.

9. Later evidence is bounded. Subsequent disclosures may test calibration, collection performance, warning value, and updating. They cannot silently rewrite what was knowable at the earlier cutoff.

10. Quarantine preserves leads. Unresolved numerical or source-dependent claims remain visible without strengthening the baseline.

AUDIT STANDARD

A competent outside researcher using this packet should be able to reproduce the principal temporal classifications, distinguish direct evidence from inference, identify the same unresolved bridges, and explain any disagreement without first guessing how the source was treated.

Source-Class Hierarchy for This Packet

Source class	Primary value	Principal control
Declassified intelligence products	Contemporaneous scope, judgment, confidence, and institutional coordination.	Separate product date, information cutoff, declassification date, and author access.
Internal coordination records	Visible professional disagreement and production process.	A coordination objection does not prove either substantive view.
Judicial/prosecutorial records	Communications, devices, financial records, admissions, attributed conduct.	Evaluate the substrate; preserve allegation status where appropriate.
Technical/cybersecurity reporting	Observed access, capability, infrastructure, TTPs, and mitigation.	Separate feasibility, attempted access, successful collection, operational use, and effect.
Official policy/oversight products	Mandates, recognized problem sets, institutional risk perception.	Avoid circularity and policy-as-proof.
Investigative/OSINT reporting	Chronology, sourcing, network mapping, and context.	Characterize anonymous sources, attribution methods, corroboration, and effect.
Internal Tornberg methodology	Standards governing the inquiry.	Method does not serve as evidence about the underlying actor or event.

CLAIM-TO-SOURCE TRACEABILITY

A. Election and Intelligence-Community Baseline Examples

Example	Example item	Status	Source IDs	Audit note
EX-01	NIC assessment "Cyber Operations Enabling Expansive Digital Authoritarianism" and PRC analysis of state voter-registration data.	SUPPORTED / BOUNDED	IC-01	Direct support for election-specific public-opinion analysis by Chinese intelligence officials. Does not establish deployed influence or vote manipulation.
EX-02	DHS/DOJ joint report on foreign interference related to the 2020 federal elections.	SUPPORTED	IC-03	Use for infrastructure/effect findings only; do not use "no material effect" to negate separate collection or influence questions.
EX-03	2020 Intelligence Community Assessment and majority/minority China judgments.	SUPPORTED	IC-02; UPL-06; UPL-07	Primary baseline and dissent record. Evaluate by cutoff and product type.
EX-04	APT31 indictment as evidence of PRC political and campaign targeting before the 2020 election.	SUPPORTED / BOUNDED	CY-01; CY-02	Supports targeting, collection, and follow-on access. Influence deployment remains unproven in the charged conduct.
EX-05	2022 ICA finding that Beijing tacitly approved bounded efforts to influence selected midterm races.	SUPPORTED / SUBSEQUENT	IC-04	Valid for baseline change and warning calibration, not retroactive proof of 2020 intent.
EX-06	DHS/DOJ 2022 joint report documenting PRC scanning and collection of public voter information.	SUPPORTED	IC-05	Supports continued interest and reconnaissance; no material core-process compromise found.
EX-07	FBI IIR alleging PRC counterfeit-driver's-license mail-ballot scheme.	RAW LEAD / QUARANTINED	EL-01; EL-02; EL-03; EL-04	Preserve as a collection lead. Public handling records reveal unresolved source access, corroboration, and contamination issues; CBP seizures do not bridge the allegation to voting.
EX-08	Graphika "The #Americans" / Spamouflage personas masquerading as U.S. voters.	SUPPORTED OSINT / EFFECT BOUNDED	CY-07	Documents deceptive influence behavior and attribution; limited authentic engagement and no demonstrated material effect.
EX-09	Salt Typhoon political and campaign relevance.	SUPPORTED ESPIONAGE / INFLUENCE UNRESOLVED	CY-03; CY-04	Direct support for telecommunications espionage and targeted communications access. Separate evidence is required for an influence mission.
EX-10	PRC access to approximately 220 million U.S. voter records.	QUARANTINED	EL-05; UPL-01	Do not state as established. Unique-person count, overlap, acquisition method, source independence, and operational use remain uncontrolled.
EX-11	DNI Haines 2024 statements on PRC influence capabilities, emerging technologies, and election threats.	SUPPORTED CONTEXT	IC-06; IC-07; IC-08	Strategic context only; not direct evidence of a particular 2020 operation.

CLAIM-TO-SOURCE TRACEABILITY

B. Mass PII and Collection-Priority Examples

Example	Example item	Status	Source IDs	Audit note
EX-12	OPM breach affecting federal personnel and background-investigation records.	SUPPORTED / DOWNSTREAM USE BOUNDED	DATA-01; DATA-02; DATA-03	Scale and strategic sensitivity are established. A named "dataset-to-operation" chain is not publicly established.
EX-13	Equifax breach attributed to four PLA officers.	SUPPORTED	DATA-04	Direct state/military attribution and mass PII theft. Voter-profiling use remains inferential.
EX-14	Anthem breach affecting approximately 78.8 million individuals.	SUPPORTED / STATE NEXUS LESS PRECISE	DATA-05; DATA-03	China-based operation and theft are established; public prosecutorial attribution is less institutionally specific than Equifax.
EX-15	Voter-registration data analyzed for 2020 public-opinion analysis.	SUPPORTED	IC-01	Cleanest direct collection-to-processing linkage in the election dataset.
EX-16	DHS/DOJ 2022 PRC scanning and voter-information collection.	SUPPORTED	IC-05	Supports recurring voter-level data interest.
EX-17	Approximate 220 million voter-record aggregate.	QUARANTINED	EL-05	Retain as a lead; exclude from confidence calculations and definitive public prose.
EX-18	APT31 targeting of political officials, candidates, and campaign staff.	SUPPORTED	CY-01; CY-02	Demonstrates political target development and collection capability.
EX-19	Salt Typhoon acquisition of communications metadata and private communications.	SUPPORTED	CY-03; CY-04	Demonstrates operational surveillance; downstream policy or influence application remains undisclosed.
EX-20	UK Electoral Commission compromise and voter-register access.	SUPPORTED	DATA-06	Official allied attribution and direct democratic-institution parallel.
EX-21	i-Soon / contractor-enabled mass data theft and brokering to MSS/MPS bureaus.	SUPPORTED AS ALLEGED EVIDENCE	CY-05; CY-06	Strong public evidence of a state-consumer pipeline; not every intrusion or use was centrally coordinated.

CLAIM-TO-SOURCE TRACEABILITY

C. Covert Influence, Access, and Obfuscation Examples

Example	Example item	Status	Source IDs	Audit note
EX-22	Yaoning "Mike" Sun political campaign, propaganda, surveillance, reporting, and PRC tasking.	SUPPORTED	INF-01; INF-02	Use admissions, communications, and reports as evidence; sentence length is not an analytic weight.
EX-23	Eileen Wang and U.S. News Center propaganda activity.	SUPPORTED BY FILED ADMISSIONS	INF-03	As of 11 May 2026, charged and agreed to plead guilty. Underlying admissions and records carry the analytic weight.
EX-24	Yuanjun Tang MSS tasking and draft-email tradecraft.	SUPPORTED	INF-04; INF-05	Direct closed-loop human collection and reporting example.
EX-25	Christine Fang cultivation of California and Midwestern political figures.	CREDIBLE INVESTIGATIVE REPORTING	INF-08	Well-sourced suspected operation; no public charge. Do not imply wrongdoing by targeted politicians.
EX-26	50 U.S.C. § 3237 annual reports on CCP influence operations.	SUPPORTED INSTITUTIONAL REQUIREMENT	INF-09	Shows enduring official collection/assessment requirement, not proof of every activity listed.
EX-27	House Select Committee June 2026 hearing on economic espionage and subnational influence.	SUPPORTED OVERSIGHT CONTEXT	INF-10	Use witness evidence separately; hearing occurrence is not corroboration of all claims.
EX-28	Thirteen fake consulting websites used to target cleared U.S. personnel.	SUPPORTED AS SUSPECTED OPERATION	CY-10; INF-13	Official seizure/warrant evidence and a prior adjudicated recruitment model; exact downstream use remains bounded.
EX-29	Jamestown/UFWD mapping and claim of more than 2,000 affiliated organizations.	BROAD PATTERN SUPPORTED; NUMBER QUARANTINED	INF-11; INF-12; INF-09	Validate affiliation thresholds, activity status, branches, duplicates, direction, and counting methodology before using the total.
EX-30	Linda Sun's alleged use of New York State government access for PRC/CCP interests.	OFFICIAL ALLEGATION / EVIDENCE-BASED REVIEW	INF-06; INF-07	Evaluate underlying communications, benefits, access changes, and concealment; do not use case disposition as a credibility shortcut.
EX-31	APT31 cyber targeting as supporting infrastructure for political intelligence and potential leverage.	SUPPORTED / APPLICATION BOUNDED	CY-01; CY-02	Political collection is established; influence or coercive deployment requires bridge evidence.

CLAIM-TO-SOURCE TRACEABILITY

D. Collection-to-Operation Linkage Examples

Example	Example item	Status	Source IDs	Audit note
EX-32	Voter-registration data moved from acquisition/access into election-specific public-opinion analysis.	SUPPORTED	IC-01	High-confidence processing linkage; downstream influence application not identified.
EX-33	OPM data cross-referenced to identify covert U.S. personnel.	MODERATE / PUBLICLY INCOMPLETE	DATA-01; DATA-02; DATA-03	Plausible and reported by officials, but public evidence does not expose a specific named resulting operation. Keep at moderate confidence.
EX-34	APT31 political/campaign data prepared for possible influence release.	SUPPORTED AS OPTION CREATION	CY-01; CY-02; IC-03	Information had potential influence utility; official public record does not show deployment for the 2020 result.
EX-35	Salt Typhoon data used for targeted surveillance of political figures.	SUPPORTED SURVEILLANCE	CY-03; CY-04	Collection and operational surveillance are directly linked; separate downstream policy or influence action is not public.
EX-36	Sun and Tang reporting fed PRC/MSS tasking and continuing operations.	SUPPORTED	INF-01; INF-02; INF-04; INF-05	Closed-loop requirement-access-reporting-feedback examples.
EX-37	i-Soon stolen data sold, delivered, or analyzed for MSS/MPS bureaus.	SUPPORTED AS ALLEGED PIPELINE	CY-05; CY-06	Strong evidence through consumer delivery and analysis; final operational action varies by case and is often not public.
EX-38	Equifax and Anthem data used for recruitment, blackmail, voter profiling, or specific operations.	UNRESOLVED	DATA-04; DATA-05; DATA-07	Data utility is clear; exact downstream use should not be asserted without bridge evidence.
EX-39	Fake consulting-front responses used to recruit or extract information from cleared personnel.	SUPPORTED AS SUSPECTED RECRUITMENT	CY-10; INF-13	Operational method is documented; identify specific consumers and exploitation outcomes before claiming effect.

CLAIM-TO-SOURCE TRACEABILITY

E. Cross-Domain, Physical Positioning, and "Toe-Hold" Examples

Example	Example item	Status	Source IDs	Audit note
EX-40	Fufeng corn-milling project approximately 12 miles from Grand Forks AFB.	SUPPORTED THREAT JUDGMENT	LAND-02; LAND-03	Air Force threat judgment is authoritative; public evidence does not identify an executed espionage operation.
EX-41	MineOne cryptocurrency mining property within one mile of F.E. Warren AFB.	SUPPORTED	LAND-01	Strongest official physical-access case; significant risk and divestment are established, completed surveillance is not.
EX-42	Blue Hills Wind / Laughlin AFB land and wind-project concerns.	SUPPORTED CONTEXT / OPERATIONAL INTENT UNRESOLVED	LAND-06; LAND-07	Property scale and military/grid concerns are documented; full CFIUS evidence and precise intent remain nonpublic.
EX-43	PRC-linked agricultural land spatial clustering near military installations at higher-than-random rates.	QUARANTINED HYPOTHESIS	LAND-03; LAND-04; LAND-05	AFIDA data quality is inadequate for a strong claim without entity resolution, geocoding, denominators, matched controls, and duplicate removal.
EX-44	2023 PRC high-altitude surveillance balloon and prior global balloon activity.	SUPPORTED CAPABILITY; SUCCESSFUL U.S. COLLECTION CLAIM CORRECTED	LAND-08; LAND-09	Deployed surveillance platform is established. Official record cited here does not support the claim that it collected sensitive intelligence despite U.S. mitigation.
EX-45	Volt Typhoon prepositioning in civilian critical infrastructure supporting military operations.	SUPPORTED	CY-08; CY-09	Persistent access and contingency risk are established; activation and destructive effect did not occur in the cited record.
EX-46	Smithfield and Syngenta ownership plus precision-agriculture data as a possible dual-use pathway.	COMMERCIAL FACTS SUPPORTED; INTELLIGENCE USE UNPROVEN	AGR-01; AGR-02; AGR-03; LAND-03	Acquisitions are documented. No included source establishes that these assets were used for intelligence collection or military-site monitoring.
EX-47	Camp Grayling photography and concealment during a military exercise.	SUPPORTED SUSPICIOUS CONDUCT; PRC DIRECTION UNPROVEN	LAND-10	Charges concern conspiracy, false statements, and evidence destruction; public record does not establish PRC state tasking.
EX-48	Expanded CFIUS and state scrutiny as an indicator.	SUPPORTED POLICY RESPONSE / NOT PROOF	LAND-04; LAND-05; LAND-03	Use as evidence of institutional risk perception and regulatory adaptation, not independent corroboration of adversary intent.

DISTRIBUTED PRIMARY RECORD

Uploaded Declassified Document Register

The following files were supplied directly for the engagement. Hashes allow recipients to verify that a distributed copy is byte-for-byte identical to the file reviewed. Full-page redactions and declassification markings are part of the public record and materially limit source-level adjudication.

ID	Full citation / distributed filename	SHA-256	Use note
UPL-01	Central Intelligence Agency. "Summary of Select Intelligence Reporting from 2004-2020 on Venezuela's Electronic Voting Manipulation Capabilities." CIA Note, 29 June 2026. Approved for public release 10 July 2026. 6 pages. File: CIA Note - Venezuela Machines Intel Memo_29JUNE2026_DECLASS_REDACTED.pdf	4a7be62c0901e6de3b0cfee37046ea5ece1a79a0e647d6f4cdae659705148594	Primary uploaded record; use according to product type and information cutoff.
UPL-02	Central Intelligence Agency. "China: Cyber Activities Probably Prelude to Election Espionage." WIRe current-intelligence article, 1 July 2020. Declassified 10 July 2026. 2 pages. File: CIA Wire Memo Summer 2020 DECLASS REDACTED.pdf	1be94e7fa86a729a2c16266fd32ed1947793903b5fa50577c9648c697dc0c48b	Primary uploaded record; use according to product type and information cutoff.
UPL-03	Cybersecurity and Infrastructure Security Agency. "Election Report." Technical and operational review, 13 July 2026. Public release. 6 pages. File: CISA Election Report - FINAL.pdf	3c6db961603260a77dce4548b7e5a7f5a6fd2b964345ab4a46eb1d3c61485c22	Primary uploaded record; use according to product type and information cutoff.
UPL-04	Office of the Director of National Intelligence / National Intelligence Council. "Everyone's favorite topic." Internal email, 23 December 2021. Declassified 3 July 2026. 1 pages. File: EMAIL_Everyone's favorite topic_23DEC2021_DECLASS_REDACTED.pdf	efa073c1baba2f629a41e0c29841a15acf00dc1b7c4ea62fa9e0b208a69619fe	Primary uploaded record; use according to product type and information cutoff.
UPL-05	Federal Bureau of Investigation / National Intelligence Council. "FW: ICA Comments." Internal coordination email, 30 December 2020. Declassified 10 July 2026. 2 pages. File: EMAIL_ICA.CommentsReMinorityView_30DEC2020_DECLASS REDACTED.pdf	d393d981518232384b3ca27d077ee5337876d873bd0399a07f98f8e1f5cc432b	Primary uploaded record; use according to product type and information cutoff.
UPL-06	National Intelligence Council. "Foreign Threats to 2020 U.S. Federal Elections." National Intelligence Council Assessment, NICA 2020-06885D, 19 August 2020. Declassified 3 July 2026. 8 pages. File: NICA_ Foreign Threats to 2020 US election_19AUG2020 - DECLASS_REDACTED.pdf	6e22be494ee83716d2251e71c253ea6d78048694886b7006ce449a336aa9882b	Primary uploaded record; use according to product type and information cutoff.
UPL-07	National Intelligence Council. "Making the Case That China Has Taken Some Steps to Influence the Presidential Election." National Intelligence Council Memorandum - Alternative Analysis, NICM 2020-09381, 16 October 2020. Declassified 3 July 2026. 7 pages. File: NICM_ChinaStepsToInfluenceElection_16OCT2020_DECLASS_REDACTED.pdf	a16aec843fddd6c525251ab4e4b2b2be1e5cee9aeca4b7bae6a59c9bf3bb2a6d	Primary uploaded record; use according to product type and information cutoff.
UPL-08	National Intelligence Council. "Vulnerabilities in U.S. 2020 Election Infrastructure." National Intelligence Council Memorandum, NICM 2020-003, 15 January 2020. Declassified 16 March 2026; approved for public release 3 July 2026. 5 pages. File: NICM_VulnerabilitiesInUS2020ElectionInfrastructure_15JAN2020_DECLASS_REDACTEDed.pdf	9105174603df72f1c9142b8e0bb56e1e036dc6d4f3dbaf559aada1e2b7e22d4c	Primary uploaded record; use according to product type and information cutoff.

Uploaded-Document Treatment Notes

ID	Treatment note
UPL-01	Retrospective CIA-only summary of selected reporting on Venezuelan electronic-voting capabilities and alleged plans. Valuable for capability, historical reporting, and analytic limitations; it is not an IC-coordinated reassessment and does not establish U.S. election manipulation.
UPL-02	CIA current-intelligence article dated 1 July 2020. Useful for campaign-target collection and the distinction between espionage-enabling access and deployed influence.
UPL-03	CISA technical synthesis of activities conducted from roughly 2019 through 2025. Disaggregate findings by underlying test or incident date; vulnerabilities do not prove exploitation or altered results.
UPL-04	Retrospective 2021 internal email raising consistency and change-management questions. It does not independently establish that either the earlier or later judgment was correct.
UPL-05	FBI coordination comments documenting objections about intent, sourcing, source descriptions, parity, speculative language, and collection gaps. Evaluate each objection separately.
UPL-06	19 August 2020 NIC assessment and contemporaneous baseline. Its information cutoff governs contemporary tradecraft review.
UPL-07	16 October 2020 alternative analysis. Preserves a formal low-to-medium-confidence warning interpretation; not an IC-coordinated majority product.
UPL-08	15 January 2020 foundational vulnerabilities memorandum. Separates capability and potential impact from specific adversary plans and intent.

PUBLIC SOURCE REGISTER

Intelligence and election baseline

ID	Full citation and direct access	Direct evidentiary use	Limits / temporal treatment
IC-01	National Intelligence Council. "Cyber Operations Enabling Expansive Digital Authoritarianism." National Intelligence Council Assessment, 7 April 2020; declassified by the Director of National Intelligence in October 2022. URL: https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Cyber-Operations-Enabling-Expansive-Digital-Authoritarianism-20200407--2022.pdf Accessed: 17 July 2026.	Direct IC evidence that Chinese intelligence officials analyzed voter-registration data from multiple U.S. states for public-opinion analysis concerning the 2020 election; broader assessment of bulk personal-data exploitation.	Establishes analysis and mission utility, not a deployed election-influence operation or material electoral effect.
IC-02	Office of the Director of National Intelligence. "Foreign Threats to the 2020 U.S. Federal Elections." Intelligence Community Assessment, March 2021. URL: https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf Accessed: 17 July 2026.	Core coordinated IC baseline; majority and minority judgments concerning PRC election influence and interference; information cutoff through 31 December 2020.	Finished intelligence, not underlying source reporting. Later evidence cannot be imported into its contemporary evidence base without demonstrated access.
IC-03	U.S. Department of Justice and U.S. Department of Homeland Security. "Key Findings and Recommendations from the Joint Report of the Attorney General and the Secretary of Homeland Security on Foreign Interference Related to the 2020 U.S. Federal Elections." March 2021. URL: https://www.dhs.gov/sites/default/files/publications/21_0311_key-findings-and-recommendations-related-to-2020-elections_1.pdf Accessed: 17 July 2026.	Official impact assessment concerning election infrastructure, voting, registration, tabulation, and material effect.	A no-material-impact finding does not adjudicate separate questions of intelligence collection, influence, preparation, unsuccessful activity, or policy shaping.
IC-04	Office of the Director of National Intelligence. "Foreign Threats to the 2022 U.S. Elections." Intelligence Community Assessment, declassified 11 December 2023 and publicly released 18 December 2023. URL: https://www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf Accessed: 17 July 2026.	High-confidence assessment of bounded PRC efforts to influence selected 2022 races and change in operating posture relative to earlier cycles.	Subsequent behavior; useful for baseline change and warning calibration, not proof of specific 2020 intent.
IC-05	U.S. Department of Justice and U.S. Department of Homeland Security. "Foreign Interference Targeting Election Infrastructure or Political Organization, Campaign, or Candidate Infrastructure Related to the 2022 U.S. Federal Elections." December 2023. URL: https://www.dhs.gov/sites/default/files/2023-12/1_b_%20Memo%20DOJ%20and%20DHS%20Approved_508c.pdf Accessed: 17 July 2026.	Official 2022 impact assessment; documents suspected PRC scanning and collection of publicly available voter information while finding no material compromise of core election processes.	Does not establish the downstream operational use of collected voter data.
IC-06	Avril Haines, Director of National Intelligence. "Opening Statement as Delivered to the Senate Select Committee on Intelligence for An Update on Foreign Threats to the 2024 Elections." 15 May 2024. URL: https://www.dni.gov/index.php/newsroom/congressional-testimonies/congressional-testimonies-2024/3823-dni-haines-opening-statement-as-delivered-to-the-ssci-for-an-update-on-foreign-threats-to-the-2024-elections Accessed: 17 July 2026.	Official context on foreign election threats, influence apparatus, emerging technology, and IC election-security work.	Public testimony is strategic context, not a source-specific adjudication of the 2020 China dispute.
IC-07	Avril Haines, Director of National Intelligence. "Opening Statement as Delivered on the 2024 Annual Threat Assessment of the U.S. Intelligence Community." 11 March 2024. URL: https://www.dni.gov/index.php/newsroom/congressional-testimonies/congressional-testimonies-2024/3798-dni-haines-opening-statement-as-delivered-on-the-2024-annual-threat-assessment-of-the-u-s-intelligence-community Accessed: 17 July 2026.	Official context on foreign malign influence and the use of generative artificial intelligence.	Broad threat context; not direct evidence of a particular PRC operation.
IC-08	Foreign Malign Influence Center. "FMI Primer: Foreign Malign Influence and Elections, Highlights, Volume 2." October 2024. URL: https://www.dni.gov/files/FMIC/documents/products/10-18-24_Report_FMI-Primer-Vol-2-Public-Release.pdf Accessed: 17 July 2026.	Controlled public definition and examples of subversive, undeclared, coercive, and criminal foreign malign influence.	Doctrinal and contextual; does not independently prove an operation.

PUBLIC SOURCE REGISTER

Mass data and collection priority

ID	Full citation and direct access	Direct evidentiary use	Limits / temporal treatment
DATA-01	U.S. Government Accountability Office. "Information Security: OPM Has Improved Controls, but Further Efforts Are Needed." GAO-17-614, 3 August 2017. URL: https://www.gao.gov/assets/gao-17-614.pdf Accessed: 17 July 2026.	Official scale and nature of the OPM breaches, including 21.5 million affected background-investigation records.	Does not identify a publicly confirmed downstream PRC operation produced by the data.
DATA-02	U.S. Government Accountability Office. "Information Security: OPM Has Implemented Many of GAO's 80 Recommendations, but Over One-Third Remain Open." GAO-19-143R, 13 November 2018. URL: https://www.gao.gov/assets/gao-19-143r.pdf Accessed: 17 July 2026.	Clarifies the related personnel-record and background-investigation compromises and affected populations.	Administrative and security review; not attribution or operational-use proof.
DATA-03	Federal Bureau of Investigation. Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States." Remarks, 7 July 2020. URL: https://www.fbi.gov/news/speeches-and-testimony/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states Accessed: 17 July 2026.	Official public attribution/context connecting PRC actors to major U.S. data thefts, including OPM and health data.	Strategic speech summarizes official judgments; consult incident-specific technical and judicial sources for precise propositions.
DATA-04	U.S. Department of Justice. "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax." 10 February 2020. URL: https://www.justice.gov/archives/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking Accessed: 17 July 2026.	Direct prosecutorial attribution to four PLA officers and the theft of sensitive information concerning roughly 145 million Americans.	Charges expose evidence and allegations; they do not by themselves establish downstream voter profiling or influence use.
DATA-05	U.S. Department of Justice. "Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People." 9 May 2019. URL: https://www.justice.gov/archives/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including Accessed: 17 July 2026.	Scale, data types, China-based operation, and exfiltration of Anthem PII.	Public charging product does not provide the same direct PLA/MSS attribution as Equifax and does not establish a voter-related purpose.
DATA-06	U.K. National Cyber Security Centre. "China State-Affiliated Actors Target UK Democratic Institutions and Parliamentarians." 25 March 2024. URL: https://www.ncsc.gov.uk/news/china-state-affiliated-actors-target-uk-democratic-institutions-parliamentarians Accessed: 17 July 2026.	Official U.K. attribution of compromise involving Electoral Commission email and Electoral Register data.	Direct allied parallel; does not establish use of the data to change election outcomes.
DATA-07	U.S. Department of Justice. "Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries." 11 April 2025. URL: https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive Accessed: 17 July 2026.	Official statement of national-security risks from foreign access to bulk sensitive personal and government-related data.	Policy framework and risk model; not evidence that a particular stolen dataset was operationally used.

PUBLIC SOURCE REGISTER

Cyber and political targeting

ID	Full citation and direct access	Direct evidentiary use	Limits / temporal treatment
CY-01	U.S. Department of Justice. "Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Political Officials." 25 March 2024. URL: https://www.justice.gov/archives/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived Accessed: 17 July 2026.	MSS-linked APT31 political, campaign, government, journalist, and critic targeting; technical progression and potential influence utility.	DOJ expressly distinguished charged hacking from proof that the conduct furthered a U.S. influence operation.
CY-02	United States v. Zhao Guangzong et al. Indictment, U.S. District Court for the Eastern District of New York, unsealed 25 March 2024. URL: https://www.justice.gov/usao-edny/media/1345131/dl Accessed: 17 July 2026.	Underlying allegations, victim categories, targeting methods, and technical records for APT31.	Unadjudicated allegations should be assessed proposition by proposition; downstream influence application remains bounded.
CY-03	Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency. "Joint Statement from FBI and CISA on the People's Republic of China Targeting of Commercial Telecommunications Infrastructure." 13 November 2024. URL: https://www.fbi.gov/news/press-releases/joint-statement-from-fbi-and-cisa-on-the-peoples-republic-of-china-targeting-of-commercial-telecommunications-infrastructure Accessed: 17 July 2026.	Official confirmation of broad PRC telecommunications espionage, call-record theft, access to some private communications, and lawful-intercept information.	Establishes espionage and surveillance; does not by itself establish an election-influence operation.
CY-04	Cybersecurity and Infrastructure Security Agency and partners. "Enhanced Visibility and Hardening Guidance for Communications Infrastructure." December 2024. URL: https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure Accessed: 17 July 2026.	Technical and mitigation context for PRC telecommunications compromises commonly associated with Salt Typhoon.	Defensive guidance; attribution and target-specific claims should be grounded in accompanying official statements.
CY-05	U.S. Department of Justice. "Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns." 5 March 2025. URL: https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global Accessed: 17 July 2026.	Official description of a distributed hacker-for-hire ecosystem serving MSS and MPS consumers, including speculative theft, sale, and analysis.	Not every contractor intrusion was centrally tasked or part of a single campaign.
CY-06	United States v. Wu Haibo et al. Indictment, U.S. District Court, unsealed 5 March 2025. URL: https://www.justice.gov/opa/media/1391901/dl Accessed: 17 July 2026.	Specific alleged data-to-consumer pathways, government bureau customers, sale of stolen information, and paid analysis.	Downstream operational action by each recipient bureau is not always publicly visible.
CY-07	Graphika Research Team. "The #Americans: Chinese State-Linked Influence Operation Spamouflage Masquerades as U.S. Voters to Push Divisive Online Narratives Ahead of 2024 Election." 3 September 2024. URL: https://www.graphika.com/reports/the-americans Accessed: 17 July 2026.	High-quality open-source documentation of deceptive U.S.-voter personas and divisive political narratives attributed to a PRC state-linked network.	Open-source attribution; reported activity generally achieved limited authentic engagement and does not establish material electoral effect.
CY-08	U.S. Department of Justice and Federal Bureau of Investigation. "U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure." 31 January 2024. URL: https://www.fbi.gov/news/press-releases/us-government-disrupts-botnet-peoples-republic-of-china-used-to-conceal-hacking-of-critical-infrastructure Accessed: 17 July 2026.	Official evidence of Volt Typhoon infrastructure, concealment, and targeting of U.S. critical infrastructure.	Establishes access and prepositioning concern; does not establish that destructive action was executed.
CY-09	Cybersecurity and Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation, and international partners. "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure." Cybersecurity Advisory AA24-038A, 7 February 2024. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a Accessed: 17 July 2026.	Technical evidence of persistent access, living-off-the-land tradecraft, and infrastructure sectors relevant to U.S. force projection.	Technical advisory supports capability and preparation; intent and activation require separate assessment.
CY-10	U.S. Department of Justice and Federal Bureau of Investigation. "Justice Department, FBI Disable 13 Websites Backed by Suspected Chinese Agents That Sought Sensitive U.S. Information from Security Clearance Holders." 10 June 2026. URL: https://www.justice.gov/opa/pr/justice-department-fbi-disable-13-websites-backed-suspected-chinese-agents-sought-sensitive Accessed: 17 July 2026.	Official description and warrant-based allegations concerning deceptive consulting fronts, fabricated identities, and recruitment of cleared personnel.	The public record describes suspected PRC-backed recruitment; exact downstream use of every response is not publicly established.

PUBLIC SOURCE REGISTER

Covert influence and access

ID	Full citation and direct access	Direct evidentiary use	Limits / temporal treatment
INF-01	U.S. Department of Justice. "Political Operative Sentenced to 48 Months in Federal Prison for Acting as Covert Agent of the People's Republic of China." 10 February 2026. URL: https://www.justice.gov/opa/pr/political-operative-sentenced-48-months-federal-prison-acting-covert-agent-peoples-republic Accessed: 17 July 2026.	Direct admissions and official account of Yaoning "Mike" Sun's tasking, campaign access, propaganda, surveillance, reporting, and work for PRC officials.	Sentence length is procedural metadata; analytic value derives from admissions, communications, tasking, and corroborating records.
INF-02	United States v. Yaoning Sun. Criminal Complaint and Affidavit, U.S. District Court for the Central District of California, filed December 2024. URL: https://www.justice.gov/archives/opa/media/1381256/dl Accessed: 17 July 2026.	Underlying messages, reports, intermediary relationships, and alleged foreign tasking in the Sun matter.	Complaint allegations should be distinguished from admitted facts and independently corroborated evidence.
INF-03	U.S. Attorney's Office, Central District of California. "Arcadia Mayor Federally Charged with Acting as Illegal Agent of the People's Republic of China." 11 May 2026. URL: https://www.justice.gov/usao-cdca/pr/arcadia-mayor-federally-charged-acting-illegal-agent-peoples-republic-china Accessed: 17 July 2026.	Filed information and plea agreement in which Eileen Wang agreed to admit covert PRC direction and undisclosed propaganda activity through U.S. News Center.	As of the cited release, Wang had agreed to plead guilty; procedural status does not determine the weight of the underlying admissions and records.
INF-04	U.S. Department of Justice. "Man Pleads Guilty to Conspiring to Act as Illegal Agent of the Chinese Government in the United States." 16 September 2025. URL: https://www.justice.gov/opa/pr/man-pleads-guilty-conspiring-act-illegal-agent-chinese-government-united-states Accessed: 17 July 2026.	Admitted MSS tasking, reporting on U.S.-based dissidents and political activity, and continued collection cycle.	Primarily demonstrates intelligence collection and transnational repression; policy-influence effect requires additional evidence.
INF-05	U.S. Attorney's Office, Southern District of New York. "Queens Man Arrested for Operating as an Illegal Agent of the Chinese Government in the United States." 21 August 2024. URL: https://www.justice.gov/usao-sdny/pr/queens-man-arrested-operating-illegal-agent-chinese-government-united-states Accessed: 17 July 2026.	Charging record describing shared draft-email accounts, encrypted communications, tasking, and reporting in the Yuanjun Tang case.	Charging allegations; later plea supports the core agency relationship, but each factual detail should still be traced to the evidentiary record.
INF-06	U.S. Department of Justice. "Former High-Ranking New York State Government Employee Charged with Acting as an Undisclosed Agent of the People's Republic of China and the Chinese Communist Party." 3 September 2024. URL: https://www.justice.gov/usao-edny/pr/former-high-ranking-new-york-state-government-employee-charged-acting-undisclosed Accessed: 17 July 2026.	Official allegations that Linda Sun used state-government access to alter access, messaging, and assistance in response to PRC/CCP requests.	Pending or charged conduct is not established by disposition; use the underlying communications and records and preserve the allegation status.
INF-07	United States v. Linda Sun and Christopher Hu. Indictment, U.S. District Court for the Eastern District of New York, filed 3 September 2024. URL: https://www.justice.gov/d9/2024-09/sun_and_hu_indictment.pdf Accessed: 17 July 2026.	Detailed alleged acts, concealment, benefits, and governmental-access pathways.	Unadjudicated; does not establish that all favorable policy conduct resulted from foreign direction.
INF-08	Bethany Allen-Ebrahimian and Zach Dorfman. "Exclusive: Suspected Chinese Spy Targeted California Politicians." Axios, 8 December 2020. URL: https://www.axios.com/2020/12/08/china-spy-california-politicians Accessed: 17 July 2026.	Year-long, multi-source investigative account of Christine Fang's suspected cultivation of local and rising political figures.	High-quality investigative reporting with anonymous intelligence sourcing; no public charge or adjudication. Targeted politicians were not thereby shown to be collaborators.
INF-09	United States Code. 50 U.S.C. § 3237, "Annual Reports on Influence Operations and Campaigns in the United States by the Chinese Communist Party." Current through 17 June 2026. URL: https://uscode.house.gov/view.xhtml?req=%28title%3A50+section%3A3237+edition%3Aprelim%29 Accessed: 17 July 2026.	Statutory institutionalization of recurring IC reporting on CCP and UFWD influence structures, tasking, organizations, and targeting of officials and candidates.	A statutory collection and reporting requirement is evidence of an institutional problem set, not proof of every enumerated activity.
INF-10	U.S. House Select Committee on the Chinese Communist Party. "China's Economic Espionage and Subnational Influence in the United States." Hearing, 25 June 2026. URL: https://chinaselectcommittee.house.gov/about/events/hearing-advisory-china-s-economic-espionage-and-subnational-influence-in-the-united-states Accessed: 17 July 2026.	Official hearing record identifying allegations, expert frameworks, and policy concerns regarding state and local influence.	Witness statements require source-by-source evaluation; the hearing itself is not independent proof of each claim.
INF-11	Alexander Bowe. "China's Overseas United Front Work: Background and Implications for the United States." U.S.-China Economic and Security Review Commission, 24 August 2018. URL: https://www.uscc.gov/sites/default/files/Research/China%27s%20Overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf Accessed: 17 July 2026.	Official commission staff study of United Front structures, influence mechanisms, and overseas mission.	Affiliation, contact, funding, direction, and agency are distinct; the report does not justify treating every community organization as a controlled actor.
INF-12	Jamestown Foundation. "The United Front System: Mapping China's Global Influence Operations." Report, accessed 17 July 2026. URL: https://jamestown.org/wp-content/uploads/Jamestown_UF_Report.pdf Accessed: 17 July 2026.	Open-source mapping and network-development context for UFWD-linked organizations.	The precise "more than 2,000 organizations" aggregate is quarantined unless counting rules, duplication controls, activity status, and affiliation thresholds are independently validated.

ID	Full citation and direct access	Direct evidentiary use	Limits / temporal treatment
INF-13	U.S. Department of Justice. "Singaporean National Pleads Guilty to Acting in the United States as an Illegal Agent of Chinese Intelligence." 24 July 2020. URL: https://www.justice.gov/archives/opa/pr/singaporean-national-pleads-guilty-acting-united-states-illegal-agent-chinese-intelligence Accessed: 17 July 2026.	Admitted use of a false consulting company and professional networking sites to recruit U.S. military and government personnel for MSS-directed reporting.	Demonstrates a recurring recruitment model; not direct evidence that the same operators ran the 2026 website network.

PUBLIC SOURCE REGISTER

Election-related raw reporting

ID	Full citation and direct access	Direct evidentiary use	Limits / temporal treatment
EL-01	U.S. Senate Committee on the Judiciary, Chairman Charles E. Grassley. "Grassley Releases Records Showing FBI Headquarters Interfered with Alleged Chinese Election Interference Probe." 1 July 2025. URL: https://www.grassley.senate.gov/news/news-releases/grassley-releases-bombshell-records-showing-fbi-headquarters-interfered-with-alleged-chinese-election-interference-probe-to-shield-christopher-wray-from-political-blowback Accessed: 17 July 2026.	Congressional release and framing of an FBI IIR, recall, source-handling correspondence, and internal process concerns.	Committee characterization is not independent corroboration of the underlying ballot-fraud allegation.
EL-02	Federal Bureau of Investigation records produced to the U.S. Senate Judiciary Committee concerning the 2020 China-related Intelligence Information Report, source recontact, recall, and internal communications. Released 1 July 2025. URL: https://www.grassley.senate.gov/imo/media/doc/fbi_iir_email_productions_to_chairman_grassley.pdf Accessed: 17 July 2026.	Primary internal correspondence documenting source-access concerns, possible open-source contamination, recall, and follow-up efforts.	The records expose handling and validation issues; they do not establish that the alleged ballot scheme occurred.
EL-03	Federal Bureau of Investigation. Intelligence Information Report concerning alleged PRC production/export of fraudulent U.S. driver's licenses for an election-related mail-ballot scheme, circulated in 2020 and publicly released through Senate Judiciary Committee processes in 2025. URL: https://www.grassley.senate.gov/download/fbi-albany-iir-provided-to-chairman-grassley Accessed: 17 July 2026.	Raw confidential-human-source reporting alleging a specific operation.	High-consequence, low-maturity lead. Public record shows unresolved source access, corroboration, and contamination concerns. It is unsuitable as proof absent validation.
EL-04	U.S. Customs and Border Protection. "Over 19K Fraudulent IDs Seized by CBP Officers in Chicago." 27 July 2020. URL: https://www.cbp.gov/newsroom/local-media-release/over-19k-fraudulent-ids-seized-cbp-officers-chicago Accessed: 17 July 2026.	Official evidence of 19,888 counterfeit driver's licenses seized, many arriving from China and Hong Kong.	Establishes a counterfeit-document stream, not a connection between those documents and voting or the FBI source allegation.
EL-05	Public claim and later-declassified references concerning PRC access to approximately 220 million U.S. voter records, 2020-2026.	Preserves a lead concerning very large-scale voter-record access and analysis.	QUARANTINED. The public record does not yet establish unique-person count, dataset overlap, acquisition method, source independence, or operational use. Do not publish as established fact.

PUBLIC SOURCE REGISTER

Land, positioning, and infrastructure

ID	Full citation and direct access	Direct evidentiary use	Limits / temporal treatment
LAND-01	U.S. Department of the Treasury. "Statement on the President's Decision Prohibiting the Acquisition of Certain Real Property of Cheyenne Leads by MineOne Cloud Computing Investment I L.P." 13 May 2024. URL: https://home.treasury.gov/news/press-releases/jy2335 Accessed: 17 July 2026.	Official presidential divestment action concerning PRC-majority-owned cryptocurrency mining property within one mile of F.E. Warren AFB and foreign-sourced equipment capable of facilitating surveillance or espionage.	Establishes a significant national-security risk, not publicly confirmed surveillance already conducted.
LAND-02	U.S. Department of the Air Force. Letter concerning the proposed Fufeng Group project near Grand Forks Air Force Base, 27 January 2023. URL: https://www.hoeven.senate.gov/wp-content/uploads/media/doc/USAIRFORCE-FUFENG-LETTER-HOEVEN.pdf Accessed: 17 July 2026.	Authoritative Air Force judgment that the proposed project presented a significant threat with near- and long-term risks to operations.	Underlying threat evidence is not public; the letter does not establish an observed espionage operation.
LAND-03	U.S. Government Accountability Office. "Foreign Investments in U.S. Agricultural Land: Enhancing Efforts to Collect, Track, and Share Key Information Could Better Identify National Security Risks." GAO-24-106337, 18 January 2024. URL: https://www.gao.gov/assets/gao-24-106337.pdf Accessed: 17 July 2026.	Official review of AFIDA data, foreign agricultural land, proximity risks, data gaps, duplication, and weak verification.	Data-quality findings prevent strong clustering claims without independent cleaning, beneficial-ownership resolution, and matched-control analysis.
LAND-04	U.S. Department of the Treasury. "Treasury Issues Final Rule Expanding CFIUS Coverage of Real Estate Transactions Around More Than 60 Military Installations." 1 November 2024. URL: https://home.treasury.gov/news/press-releases/jy2708 Accessed: 17 July 2026.	Official expansion of review jurisdiction within one- and 100-mile radii around listed installations.	Policy response evidences institutional risk perception and authority, not adversary intent in any individual transaction.
LAND-05	U.S. Department of the Treasury. "CFIUS Real Estate Instructions (Part 802)" and Geographic Reference Tool, current following the November 2024 final rule. URL: https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-real-estate-instructions-part-802 Accessed: 17 July 2026.	Regulatory geography and audit tool for proximity analysis.	A property's location within jurisdiction does not establish an intelligence purpose.
LAND-06	Office of U.S. Senator John Cornyn. Letter and public materials concerning the proposed Blue Hills Wind project near Laughlin Air Force Base, 2020-2024. URL: https://www.cornyn.senate.gov/wp-content/uploads/2024/07/Letter-re-Blue-Hills-Wind-Project.pdf Accessed: 17 July 2026.	Congressional concerns regarding approximately 130,000 acres, low-level military training routes, grid access, ownership, and mitigation.	Congressional concern is not independent proof of espionage. Publicly available material does not fully expose CFIUS evidence or mitigation terms.
LAND-07	Lara Seligman. "A Chinese Wind Farm in Texas Raises Eyebrows." Foreign Policy, 25 June 2020. URL: https://foreignpolicy.com/2020/06/25/texas-chinese-wind-farm-national-security-espionage-electrical-grid/ Accessed: 17 July 2026.	High-quality reporting on ownership, project scale, military aviation, grid, and national-security concerns surrounding the Laughlin-area project.	Investigative context; does not establish a confirmed intelligence operation.
LAND-08	U.S. Department of Defense. "General Says Chinese Surveillance Balloon Now Over Center of U.S." 3 February 2023. URL: https://www.defense.gov/News/News-Stories/Article/article/3288103/general-says-chinese-surveillance-balloon-now-over-center-of-us/ Accessed: 17 July 2026.	Official confirmation of a maneuverable PRC surveillance platform crossing the continental United States near sensitive sites.	Later official accounts stated U.S. countermeasures prevented collection of sensitive intelligence during the transit; claims of successful collection despite mitigation are not supported here.
LAND-09	U.S. Department of Defense. "Military and Security Developments Involving the People's Republic of China 2023." Annual report to Congress, 19 October 2023. URL: https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-military-and-security-developments-involving-the-peoples-republic-of-china.pdf Accessed: 17 July 2026.	Strategic and technical context for the PLA high-altitude balloon program and global surveillance use.	Broad defense assessment; not evidence linking land purchases, cyber access, and balloons into one centrally controlled campaign.
LAND-10	U.S. Attorney's Office, Eastern District of Michigan. "United States Attorney's Office Issues 2024 Annual Report." 17 January 2025, discussion of charges against five Chinese nationals related to a 2023 visit near Camp Grayling. URL: https://www.justice.gov/usao-edmi/pr/united-states-attorneys-office-issues-2024-annual-report Accessed: 17 July 2026.	Official summary of alleged photography of military equipment and later conspiracy, false-statement, and evidence-destruction conduct.	Public record does not establish PRC government direction or an intelligence-service relationship.

PUBLIC SOURCE REGISTER

Agriculture and dual-use context

ID	Full citation and direct access	Direct evidentiary use	Limits / temporal treatment
AGR-01	Shuanghui International Holdings Limited and Smithfield Foods, Inc. "Shuanghui International and Smithfield Foods Complete Strategic Combination, Creating a Leading Global Pork Enterprise." 26 September 2013. URL: https://www.prnewswire.com/news-releases/shuanghui-international-and-smithfield-foods-complete-strategic-combination-creating-a-leading-global-pork-enterprise-225395622.html Accessed: 17 July 2026.	Documents the Chinese acquisition of Smithfield as commercial and ownership context.	Does not establish intelligence access, precision-agriculture exploitation, or proximity-driven intent.
AGR-02	Syngenta. "ChemChina Announces the Definitive End Results of the Tender Offers for Syngenta." 2017. URL: https://www.syngenta.com/media/media-releases/2017/chemchina-announces-definitive-end-results-tender-offers-syngenta Accessed: 17 July 2026.	Documents ChemChina's acquisition of Syngenta as agricultural-technology ownership context.	Does not independently establish U.S. precision-agriculture data transfer to PRC intelligence consumers.
AGR-03	Federal Trade Commission. "FTC Approves Final Order with China National Chemical Corporation and Syngenta AG, Preserving Competition in U.S. Markets for Three Pesticides." June 2017. URL: https://www.ftc.gov/news-events/news/press-releases/2017/06/ftc-approves-final-order-china-national-chemical-corporation-syngenta-ag-preserving-competition-us Accessed: 17 July 2026.	Official U.S. regulatory confirmation of the ChemChina-Syngenta transaction and U.S. market implications.	Competition review; not evidence of intelligence use.

TORNBERG METHOD

Internal and Public Methodology Source Register

ID	Full citation	Methodological use	Release / limitation
TM-01	Tornberg Consulting, LLC. TORNBERG Organizational Framework and Tradecraft Standards. Version 0.1 (Working Draft). 14 July 2026. Internal methodology document cited with owner authorization.	Organizational architecture; Discovery, Collection, Source Management, Analysis, Quality, Red Team, and Knowledge Management functions; TS-1110 through TS-1150 evidence standards; TS-1210 through TS-1230 professional judgment, confidence, and baseline standards; TS-1310 through TS-1350 intellectual integrity and auditability.	Internal working doctrine. Citation does not represent government endorsement and the full draft is not reproduced in this public packet unless separately released.
TM-02	Tornberg Consulting, LLC. TORNBERG CONSULTING Structured Analytic Products. Version 0.1 (Working Draft). 14 July 2026. Internal methodology document cited with owner authorization.	Structured analytic technique governance, independent judgment before group convergence, evidence matrices, source dependency, human review gates, update triggers, challenge, and product integration.	Internal working doctrine subject to revision.
TM-03	Tornberg Consulting, LLC. Time-Gated Evidence Deconfliction. Intelligence Tradecraft Note 2026-01. 17 July 2026. Public release.	Four-date evidence control, knowledge-availability classes, two-reading model, production-and-judgment reconstruction matrix, quarantine, and public audit checklist.	Method product; does not adjudicate the underlying political controversy.
TM-04	Tornberg Consulting, LLC. Application of the Tornberg Method to Time-Gated Evidence Deconfliction. Process Summary Report 2026-01. 17 July 2026. Public release.	Framework-to-output traceability; Discovery, Collection, Analysis, Production, Review, Adaptation, challenge functions, and auditability standard.	Process description; not independent evidence concerning PRC activity or IC judgments.

Method-to-Packet Traceability

Doctrine	Requirement	Visible packet feature
TS-1110 / TS-1120	Evidence precedes assessment; observation, inference, and assessment remain distinct.	Status vocabulary; example crosswalk; direct-use and limitation columns.
TS-1130 / TS-1140	Source characterization and source deconfliction.	Full source register; source classes; derivative-source cautions; IDs and provenance.
TS-1150	Unknowns remain unknown.	Quarantine Register and bounded-language rules.
TS-1210 / TS-1220	Professional judgment and confidence follow evidence.	Professional judgment used to generate gaps; no cross-disciplinary or legal-outcome confidence inflation.
TS-1230	Evidence reinforces, refines, contradicts, or replaces the baseline.	Time-gated crosswalk and retrospective-use notes.
TS-1310 through TS-1350	Objectivity, intellectual honesty, challenge, humility, transparency.	Competing explanations, correction entries, hashes, audit instructions, and revision conditions.
FS100 / FS200	Collection requirements and source management.	Gap-driven source expansion; source IDs; provenance; URLs; file-integrity digests.
FS300 / FS500 / FS600	Analysis, quality, and structured challenge.	Evidence-stage separation; detectability; Red Team, Devil's Advocacy, alternative analysis, and Cassandra distinction.
SAT governance	Independent review before convergence; consensus does not increase evidentiary strength.	Cassandra and panel outputs treated as discovery inputs rather than corroboration.
Time-Gated Evidence Deconfliction	Four-date control, author-access classes, two readings, quarantine.	Controlling structure of this public packet.

CONTROLLED UNCERTAINTY

Quarantine and Correction Register

ID	Claim under review	Missing control / bridge evidence	Permitted use
Q-01	Approximately 220 million U.S. voter records obtained or accessed by the PRC.	Unique persons vs. records; overlap; acquisition method; public/purchased/scraped/stolen distinctions; source independence; operational use.	Retain as a lead. Do not use as established scale or as evidence of election manipulation.
Q-02	More than 2,000 UFWD-linked organizations across multiple Western countries.	Affiliation threshold; formal tasking; active vs. historical status; branch counting; duplicate entities; geography; methodology.	Use the broad network proposition; exclude the precise aggregate pending validation.
Q-03	PRC-linked agricultural land clusters near U.S. military installations at higher-than-random rates.	Clean AFIDA data; beneficial ownership; parcel geocoding; denominators; matched controls; target density; market variables; duplication.	Treat as a testable spatial hypothesis, not a finding.
Q-04	The 2023 balloon collected sensitive intelligence despite U.S. mitigation.	Official collection assessment and payload results.	Corrected: use evidence of deployed surveillance capability and route; do not state successful sensitive collection during the transit on the cited record.
Q-05	OPM data directly identified and exposed named U.S. covert personnel.	Specific target, fusion method, consumer, resulting action, and independent confirmation.	Moderate hypothesis / reported official assessment; not a closed public evidence chain.
Q-06	Equifax, Anthem, Smithfield, Syngenta, or precision-agriculture data were used for voter profiling or a specific influence operation.	Data repository, fusion workflow, query logs, tasking, consumer delivery, target package, or follow-on action.	Commercial ownership and data theft are established separately; downstream operational use remains unproven.
Q-07	Laughlin-area land acquisition was an intelligence operation.	Foreign tasking, noncommercial financing, technical collection equipment, anomalous data flows, surveillance activity, or consumer reporting.	Maintain competing commercial, dual-use, opportunistic, and deliberate-access explanations.
Q-08	Camp Grayling conduct was PRC-directed intelligence collection.	State tasking, communications with handlers, financing, prior targeting, or delivery to a government consumer.	Suspicious access and concealment are supported; foreign-government direction is not.

AUDIT AND RELEASE

Mass-Audit Checklist

- ☐ **1.** Can every material example be traced from an EX identifier to one or more full source citations?
- ☐ **2.** Has the precise proposition supported by each source been stated more narrowly than the surrounding public narrative?
- ☐ **3.** Are event, reporting, author-availability, and public-release dates separated where they matter?
- ☐ **4.** Has repeated reporting been deconflicted to the originating evidence stream?
- ☐ **5.** Are raw reporting, coordinated intelligence, technical findings, judicial evidence, policy products, and journalism characterized differently?
- ☐ **6.** For legal materials, has the underlying evidentiary substrate been evaluated rather than relying on charge, plea, conviction, dismissal, or sentence?
- ☐ **7.** Are capability, priority, collection, processing, intent, operational action, and effect separately identified?
- ☐ **8.** Does every negative judgment consider whether contrary activity would likely have been detected?
- ☐ **9.** Are subsequent events used for calibration and baseline change rather than imported backward?
- ☐ **10.** Are numerical aggregates defined, deduplicated, and independently sourced?
- ☐ **11.** Are policy responses treated as institutional risk indicators rather than proof?
- ☐ **12.** Are allegations, admissions, technical observations, and assessments visibly distinguished?
- ☐ **13.** Are the strongest ordinary and adversarial alternative explanations preserved?
- ☐ **14.** Is every quarantined claim paired with the evidence required to release it from quarantine?
- ☐ **15.** Can a critical reader disagree without first guessing how the evidence was handled?

RELEASE THRESHOLD

Do not publish a definitive claim merely because a coherent narrative can be constructed. Publish the evidentiary status, temporal gate, source dependence, missing bridge evidence, strongest unresolved alternative, and condition that would revise the judgment.

Distribution Package Integrity

When distributing this packet with the underlying uploaded documents, recipients should verify the SHA-256 digests in Part V. Hyperlinked public sources may change location or be archived after publication; preservation of local copies should comply with copyright, records-management, and distribution authorities.

Internal Tornberg working doctrine is cited for methodological transparency. Public release of this packet does not automatically authorize reproduction of internal methodology documents beyond fair quotation and citation. The two companion public Tornberg products may be distributed according to their own attribution and reproduction notices.

TORNBERG CONSULTING, LLC

Evidence should be strong enough to survive disagreement.

Public release | Source Packet 2026-01 | 17 JULY 2026