TORNBERG CONSULTING, LLC

PUBLIC INTELLIGENCE PRODUCT

THREATS & WARNINGS: IMPLICATIONS FOR ELECTION INTEGRITY

Companion Graphic Deck to the July 2026 Election Interference Intelligence Digest

PUBLIC INTELLIGENCE GRAPHIC DECK 2026-01

17 JULY 2026

PUBLICATION STATUS

PUBLIC RELEASE. This companion deck distills key baseline shifts, threats, warning indicators, and protective priorities identified through the Tornberg Analytic Process. Cross-reference sourcing is contained in Tornberg Public Source Packet 2026-01 and Uploaded Document Register DOC-01–DOC-08.

Prepared for journalists, researchers, election-security practitioners, and public-interest investigators.

THREATS & WARNINGS: IMPLICATIONS FOR ELECTION INTEGRITY

Slide 1 of 3 | Revised Baseline

Companion graphic to the July 2026 Election Interference Intelligence Digest

Previously Justifiable Public Baseline

- *No public evidence showed that the PRC materially altered election infrastructure, changed votes, or compromised ballots.*
- *PRC cyber collection and political interest were recognized, but election-directed intent remained disputed.*
- *Election-integrity discussion focused heavily on technical compromise and less on the broader influence environment.*

Newly Informed Tornberg Baseline

- *U.S. voter and election-relevant information formed an identifiable subset of a broader PRC state-level collection priority.*
- *PRC channels have demonstrated pathways from collection to analysis to operational support, including political and influence-related activity.*
- *The threat to election integrity is broader than vote-tabulation security: it includes data access, political targeting, narrative legitimacy, and critical enabling infrastructure.*

KEY IMPLICATION

Election integrity should be treated as a whole-system resilience problem, not solely as a question of whether votes were changed.

Cross-reference sourcing: Tornberg Public Source Packet 2026-01 and Uploaded Document Register DOC-01–DOC-08.

THREATS & WARNINGS: IMPLICATIONS FOR ELECTION INTEGRITY

Slide 2 of 3 | Actionable Findings & Mitigation Priorities

Companion graphic to the July 2026 Election Interference Intelligence Digest

1. Voter Data Is a Strategic Target

Finding: PRC collection priorities include voter and election-relevant information.

Mitigation Focus:
Reduce bulk access, audit repositories, and monitor scraping or purchase pathways.

2. Registration Integrity Reduces Fraud Pathways

Finding: Harvested personal data can support identity resolution, profiling, and fraud-enabling pathways.

Mitigation Focus: Secure the registration process so only registered and validated voters carry forward into later stages.

3. Campaigns Are Collection Targets

Finding:
Campaign staffs, officials, and political networks have been targeted by PRC-linked actors.

Mitigation Focus:
Treat campaigns and local officials as counterintelligence and cybersecurity targets.

4. Proxy Influence Is Proven Tradecraft

Finding:
Fronts, cutouts, local intermediaries, and disguised messaging have been used to shape access.

Mitigation Focus:
Map foreign-linked access networks, funding, and messaging channels.

5. Simpler Systems Reduce Exposure

Finding: Digital dependencies, telecom links, and technologically enabled ballot or count systems can expand exploitable avenues of attack.

Mitigation Focus: Limit attack surfaces wherever possible and favor simpler, validated, less technology-dependent voting and counting processes.

6. Legitimacy Is an Attack Surface

Finding:
True or false compromise claims can erode trust even when votes are not changed.

Mitigation Focus:
Preserve audit-ready evidence, chain of custody, and rapid public validation.

Warning Standard

The revised baseline justifies immediate protective attention to data, identity, access, infrastructure, and public-confidence seams—without requiring proof that votes were changed.

Cross-reference sourcing: Tornberg Public Source Packet 2026-01 and Uploaded Document Register DOC-01–DOC-08.

THREATS & WARNINGS: IMPLICATIONS FOR ELECTION INTEGRITY

Slide 3 of 3 | Immediate Warning Areas & Reporting Leads

Companion graphic to the July 2026 Election Interference Intelligence Digest

Immediate Warning Areas

- Anomalous access to voter-registration data or public-facing election systems
- Identity-fraud pathways, counterfeit documents, or absentee-ballot validation gaps
- Coordinated proxy messaging or local political influence tied to PRC interests
- Campaign and official targeting through cyber, telecom, or commercial cutouts
- Foreign-linked access near critical infrastructure or other election-support nodes

Lines of Reporting to Follow

- Which voter-data repositories remain easiest to aggregate, scrape, or purchase?
- How are voter-roll integrity, chain of custody, and identity verification being monitored?
- What vendor, telecom, or third-party dependencies create exploitable seams?
- Where do local access networks intersect with PRC-linked entities or messaging fronts?
- Which agencies own which part of the problem—and where are the seams in coordination?

STRATEGIC IMPLICATION

Election integrity is simultaneously a counterintelligence, cybersecurity, data-governance, and public-confidence problem. Timely defensive action depends on recognizing all four dimensions together.

This product highlights urgent decision areas, not prescriptive solutions.

Cross-reference sourcing: Tornberg Public Source Packet 2026-01 and Uploaded Document Register DOC-01–DOC-08.