

Cross-Domain Analysis: Cybersecurity × China State-Sponsored Activity

The four patterns under test (from Report 1008)

1. The feeling-out round — light jabs testing range and reactions; nobody throws them for nothing.
2. Gray-zone tipping — operations below the war threshold, nearly spilling over.
3. Protest hijacking — a violent 1% attaches to a legitimate 99%.
4. Proxies all the way down — cutouts at every layer; deniability is the product.

Pattern 1: Proxies all the way down — STRONGEST MATCH

✓ ✓

CT report: recruited teenagers, hired criminals, visa students, anonymous Telegram accounts. Nobody holds the matches themselves.

Cyber lanes:

- Lane 1: Shanghai Firetech and Shanghai Powerock as MSS "enabling companies" — the DOJ's term for front firms that let intelligence services "obscure [their] hand." Contractors, not officers, do the hacking.
 - Lane 2: corporate layering as deniability — a California company (TP-Link Systems Inc.) with a Shenzhen-born brand, a Vietnam plant running on Chinese components, built by a Chinese military-linked contractor. Each corporate layer is a cutout.
 - Lane 3: freight forwarders in Malaysia and Singapore, false end-user paperwork, the alias "Jackie Lui." Commercial cutouts doing exactly what the Telegram-recruited arsonists do in the kinetic domain.
- The cross-domain discovery: same function, different material. Terrorism lanes use **people** as cutouts; cyber lanes use **companies**. Deniability is the product in both — engineered, layered, deliberate.

Pattern 2: Feeling-out jabs / pre-positioning — STRONG MATCH ✓ ✓

CT report: light jabs testing what the other side responds to; round one exists because later rounds are coming.

Cyber lanes:

- Lane 2: Volt Typhoon / Flax Typhoon compromising home routers = access banked with no immediate payoff. That is a feeling-out jab in pure form: touch the infrastructure, learn the terrain, decide later.
- Lane 3: a three-year smuggling run (2023–2026) is a probe of enforcement — each shipment tests what gets through.
- Lane 1: HAFNIUM's indiscriminate compromise (12,700+ US orgs) as mass access collection before any specific objective.

Caution (don't force the metaphor): in the boxing frame, jabs imply later haymakers. In cyber, the pre-positioning is often the **end state**, not a prelude — persistent access doesn't need "later rounds." The pattern transfers; the telos doesn't always.

Pattern 3: The attribution gap as strategy — STRONG MATCH ✓✓

CT report: every layer is a cutout, so no single incident can be pinned cleanly enough to force a war.

Cyber lanes: the legal system visibly **bends around** the attribution gap —

- TP-Link: states sue under consumer-protection law (deceptive marketing) because criminal state-sponsorship attribution is unreachable. The national-security motive wears a consumer-fraud costume.
- Zhang Yu: a \$10M RFJ bounty exists precisely because arrest is impossible (he's in China). The bounty is what you use when the handcuffs can't reach.
- Lui: prosecuted as a **smuggler**, not as a Chinese agent — the charge is what the evidence can carry, not what the suspicion suggests.

Both domains show the same adaptation: when you can't prove the top of the chain, you prosecute whatever layer the evidence **can** hold.

Pattern 4: The hijacked substrate — CANDIDATE ONLY ⚠

CT report: the violent 1% attaches to the legitimate 99%; the march is real, the fire isn't theirs.

Cyber candidate: botnets — thousands of innocent routers and servers doing an attacker's work while their owners notice nothing. The structural rhyme is real: innocent substrate, tiny operator set, the many unknowingly serving the few.

But the arrow points the other way: in France the 1% are the **actors** and the 99% the **cover**; in a botnet the masses are the **instrument** and the few the **beneficiaries**. Same shape, inverted direction. Mark this CONTESTED, not confirmed — it's suggestive, not established.

Verdict

The one-line finding: strip away the domain — bombs vs. bytes — and the constant is **deniability engineering**: cutout people, cutout companies, and legal systems forced to prosecute the layer they can reach instead of the layer that matters.