

Cross-Domain Analysis 15 — Subutai's Gap × Honeypots: Don't Chase, Funnel

The tactic, in one line

Subutai: leave a deliberate gap in the encirclement so the enemy funnels into the killing ground instead of scattering. Cyber: leave a deliberately attractive weak point — a honeypot — so attackers funnel into the instrumented corridor instead of ranging across your network. Don't chase; funnel.

The attacker's recon does the funneling

Attackers look for the easiest route in — that was DaviX's starting observation, and it is the whole mechanism. Anderson: honeypots work because "attackers scanning the Internet looking for [a vulnerable device] find one to attack." You don't herd them; their own search converges on the most attractive target. So the design principle is: build the most attractive target. The trap is not a tripwire you hope they hit — it is the path of least resistance, by construction.

Walkers land on THE LIST

"The upshot is that the honeypot operator gets to see who's attacking what, and how" (Anderson). TTPs, source IPs, tooling, malware samples — the corridor is instrumented, so every walker donates intelligence. That intel feeds the slow pipeline: Lane 1 of the cyber case study took **five years** from intrusion to \$10M bounty. The trap doesn't catch Zhang Yu; it produces the evidence that eventually does. Anderson's research group tracked actors scanning 60,000+ vulnerable devices this way; the Cambridge Cybercrime Centre feeds honeypot-collected attack data to 100+ researchers worldwide.

It catches the cutout layer

Sophisticated operators fingerprint honeypots and walk around them. But opportunistic criminals, botnet herders, recruited teenagers — Report 1008's proxy layer — walk straight in. And per the graph-traversal logic, proxies lead up the chain: each captured cutout is a node whose edges point toward the principals. The trap is a BFS seed generator.

The honest limits

- A honeypot that attackers can use as a launchpad against others becomes **your** liability, not theirs — isolation is the price of the tactic.
- Passive watching is lawful; hacking back generally isn't. The "catch" still runs through law enforcement.
- Deception decays: once attackers know you run honeypots, they get cautious, and the bait needs refreshing.
- NIST CSF 2.0: NOT FOUND — no deception content. It is a governance framework, not a tactics manual. Anderson is the corpus reference.

The convergence

This is one tactic built three times: the wall gap (Lesson 21, Part 7 — "don't chase, funnel"), THE LIST (DoorStrike — walkers get recorded), and now the honeypot corridor. Same shape, three domains: leave the opening, watch the corridor, keep the list.

Verdict

Subutai's gap transfers to cyber deception cleanly — arguably it was **always** a deception tactic wearing a siege tactic's clothes. The funnel principle ("make the trap the easiest route") is the genuine addition: most honeypot literature frames them as alarms, but the stronger design is attraction. CONFIRMED as a transferable tactic, with the limits above.