



ACH Matrix

Bryna Milligan

9 September 2025

1 Introduction

2 Hypotheses and Evidence

From Erangi:

Most Likely: H2 (State B) - Fewest disconfirming inconsistencies

Plausible but Problematic: H1 (State A) - Strong confirming evidence but significant inconsistencies suggest false flag possibility

Unlikely: H3 (Criminal) - Core behavioral inconsistency with no ransom demand

Least Likely: H4 (Hactivist) - Multiple capability inconsistencies

3 ACH Matrix

| H1: attacks carried out by State A's intelligence service State B, a regional rival criminal ransomware group protesting climate inaction | H2: attacks carried out by H3: attacks were the work of H4: attacks were the work of hactivists | | |
|--|---|--|--|
| Row 1 | | | |
| Row 2 | | | |
| Row 3 | | | |
| Row 4 | | | |
| Row 5 | | | |
| Row 6 | | | |

Table 1: Placeholder caption

4 Probabilities

1. **Malware Resemblance:** Strongly supports **H1** (State A's intelligence service) but suggests modifications that complicate attribution.

2. **Infrastructure Overlap:** While it overlaps with criminal ransomware groups, this evidence does not strongly support the ransomware hypothesis due to the absence of a ransom demand.

3. **Hactivist Manifesto:** Strongly supports **H4** (hactivists), indicating a potential motive related to climate activism.

4. **Intelligence Intercepts:** Strongly supports **H2** (State B), suggesting strategic interest in exploiting vulnerabilities.

5. **No Ransom Demands:** This evidence *weakens* the hypothesis of a criminal ransomware group significantly, as it deviates from expected behavior.

6. **Knowledge of Industrial Control Systems:** Strongly supports **H1**, indicating that a state actor with expertise is likely involved.

Conclusion: The absence of a ransom demand indeed weakens the likelihood of H3 (criminal ransomware group) being responsible for the attack. The analysis suggests that **H1** (State A's intelligence service) and **H2** (State B) remain strong contenders, while **H4** (hacktivists) is supported by the manifesto but lacks broader corroborating evidence.

5 Appendix