

# Tabletop Scenario: China as Aggressor

Scenario Title: Operation Dragon's Claw

**Overview:** In this scenario, China initiates a sophisticated cyber operation, codenamed "Operation Dragon's Claw," targeting the technological sector of a rival nation. The primary objective is the theft of intellectual property related to next-generation telecommunications technology, aiming to bolster China's global technological and economic dominance.

**Targets:** The primary targets include research institutions and technology corporations in the rival nation, specifically those involved in the development of cutting-edge telecommunications infrastructure.

**Attack Sequence:**

1. Initial Reconnaissance: Utilize social engineering and phishing campaigns to gain initial access to the networks of targeted institutions and corporations.
2. Lateral Movement: Once inside, deploy custom malware to explore the network, identify valuable data repositories, and establish persistent access.
3. Data Exfiltration: Stealthily extract intellectual property related to telecommunications technologies, ensuring to cover tracks to avoid detection.
4. Deployment of Ransomware: As a secondary objective and to obscure the true intent of the operation, deploy ransomware to disrupt operations and draw attention away from the theft.

**Tactical Objectives:**

- Accelerate China's development in telecommunications, reducing dependency on foreign technology.
- Undermine the competitive advantage of the rival nation in the global technology market.

# Tabletop Scenario: China as Victim

## Scenario Title: Operation Firewall Breach

### Overview:

China becomes the target of a sophisticated cyber attack aimed at disrupting its energy sector. The attack is suspected to be orchestrated by a rival nation-state as a form of geopolitical maneuvering.

**Attack Vector:** The adversary employs a multi-stage ransomware attack targeting the control systems of key power plants across China, intending to cause widespread disruption and undermine public confidence in the government's ability to protect critical infrastructure.

### Detection and Response:

**Immediate Response:** Upon detection of the intrusion, China's cybersecurity response teams are mobilized to isolate affected systems, preventing the spread of ransomware.

**Damage Assessment:** Concurrently, a comprehensive assessment is launched to determine the extent of the intrusion and the impact on critical infrastructure operations.

**Tactical Countermeasures:** Utilizing advanced threat intelligence and forensic capabilities, China identifies the source of the attack and prepares a series of calibrated retaliatory cyber operations aimed at the infrastructure of the aggressor nation, designed to signal capability and resolve without escalating into open conflict.

### Strategic Objectives:

- Demonstrate China's cyber defensive capabilities and resilience in the face of targeted attacks.
- Employ strategic retaliatory measures to deter future aggression, establishing a clear stance against cyber provocations while maintaining plausible deniability.

### Conclusion:

In both scenarios, China's actions as an aggressor and victim are deeply intertwined with its broader geopolitical strategies and objectives. Operation Dragon's Claw highlights China's proactive stance in advancing its technological capabilities and global position through cyber operations. Conversely, Operation Firewall Breach showcases China's robust defensive

mechanisms and strategic retaliatory capabilities, underlining its commitment to safeguarding national security and interests in the cyber domain.