Tabletop Scenario: United States as Aggressor

Scenario Title: Operation Liberty Shield

Overview:
The United States initiates Operation Liberty Shield, a covert cyber operation targeting the military communication networks of a hostile nation-state. The primary objective is to disrupt the adversary's command and control capabilities and to gather critical intelligence on military deployments and strategies.

Targets:
The operation focuses on military communication infrastructures, including satellite communication systems and encrypted messaging networks used by the hostile nation's armed forces.

Attack Sequence:
Cyber Reconnaissance: Specialized cyber units conduct a comprehensive reconnaissance to identify vulnerabilities within the adversary's military communication networks.

Infiltration and Exploitation: Utilizing sophisticated cyber tools, the units exploit identified vulnerabilities to gain access to the networks without detection.

Intelligence Gathering: Once inside, they deploy custom malware to monitor communications, exfiltrate sensitive military plans, and gather actionable intelligence.

Strategic Disruption: In parallel, the operation involves the selective disruption of communication channels to sow confusion and hamper the adversary's military coordination, while avoiding collateral damage.

Tactical Objectives:

- Undermine the adversary's military operational capabilities by disrupting command and control communications.
- Gather valuable intelligence to inform U.S. military and diplomatic strategies.
- Demonstrate the United States' cyber operational capabilities as a deterrent against future aggression.

Tabletop Scenario: United States as Victim

Scenario Title: Operation Cyber Dawn

Overview:
The United States faces Operation Cyber Dawn, a sophisticated multi-vector ransomware attack orchestrated by an unknown adversary. The attack targets critical infrastructure sectors, including the energy grid and financial services, aiming to cause widespread disruption and erode public confidence in national cyber defenses.

Attack Vector:
The adversary employs a combination of phishing, zero-day exploits, and supply chain compromises to deploy ransomware across critical networks, encrypting data and demanding substantial ransoms.

Detection and Response:
Immediate Containment: Cyber response teams from the Department of Homeland Security and the FBI work in coordination with affected entities to isolate compromised systems and prevent the spread of ransomware.

Rapid Recovery: Leveraging pre-established emergency response protocols, efforts are focused on restoring affected services using backup systems and redundancy measures.

Public-Private Collaboration: The U.S. government activates its partnerships with the private sector, including major cybersecurity firms, to assist in analyzing the attack, developing decryption tools, and reinforcing cybersecurity measures.

International Diplomacy and Cooperation: The U.S. engages with international allies to share intelligence on the attack, seeking to identify the perpetrators and explore coordinated responses.

Strategic Objectives:

- Rapidly restore critical services to minimize the impact of the attack on national security and the economy.
-

- Strengthen public confidence in the government's ability to protect against and respond to cyber threats.
-
- Utilize diplomatic and intelligence resources to attribute the attack, holding the perpetrators accountable through international legal mechanisms or targeted sanctions.

Conclusion:
These scenarios illustrate the United States' dual role in the cyber domain, showcasing its strategic application of cyber capabilities to advance national interests and its comprehensive defensive measures to mitigate the impact of cyber aggression. Operation Liberty Shield highlights the U.S.'s proactive stance in leveraging cyber operations for strategic advantage, while Operation Cyber Dawn underscores its resilience and collaborative approach in responding to significant cyber threats.