Tabletop Scenario: DPRK as Aggressor

Scenario Title: Operation Golden Sun

Overview: DPRK launches Operation Golden Sun, a covert cyber campaign aimed at infiltrating and exfiltrating funds from international financial institutions and cryptocurrency exchanges. This operation is designed to circumvent the impact of international sanctions and support the state's economic needs.

Targets: High-profile financial institutions and rapidly growing cryptocurrency exchanges globally, especially those with perceived vulnerabilities in their cyber defenses.

Attack Sequence:

- Reconnaissance: DPRK's elite cyber units conduct extensive research to identify potential vulnerabilities in the cyber defenses of targeted institutions.

- Spear-Phishing and Exploitation: Utilizing sophisticated spear-phishing techniques, the operatives gain initial access to the networks of these institutions.

- Lateral Movement and Persistence: Once inside, they move laterally across the network to gain deeper access and establish persistence, ensuring continued access for future operations.

- Financial Exfiltration: The operatives deploy custom malware designed to siphon funds undetected, transferring them to DPRK-controlled accounts. Simultaneously, ransomware is deployed in non-essential systems as a distraction and potential additional revenue source.

Tactical Objectives:
Secure financial resources to support DPRK's economy and circumvent international sanctions.

Demonstrate DPRK's cyber capabilities and resilience in the face of global opposition.

Tabletop Scenario: DPRK as Victim

Scenario Title: Operation Silent Guardian

Overview: A coalition of Western intelligence agencies launches Operation Silent Guardian, a sophisticated cyber espionage campaign aimed at infiltrating DPRK's tightly controlled digital infrastructure. The primary goal is to gather intelligence on DPRK's military capabilities and potential cyber offensive strategies.

Attack Vector: The operation employs a multi-pronged approach, including the use of advanced persistent threats (APTs) and zero-day exploits, targeting known vulnerabilities within DPRK's digital environment.

Detection and Response:
Enhanced Monitoring and Detection: DPRK's cyber defense units, utilizing advanced threat detection systems, identify unusual network activities indicating a potential breach.

Isolation and Containment: Immediate steps are taken to isolate affected systems, preventing further penetration and limiting the spread of the espionage tools.

Counter-Intelligence Operations: DPRK activates its counter-intelligence mechanisms, aiming to trace the source of the attack and gather evidence on the operatives and their objectives.

Retaliatory Cyber Operations: In line with its doctrine of tactical adversarial countermeasures, DPRK prepares a series of targeted cyber counter-attacks against the infrastructure used by the coalition, aiming to disrupt their capabilities and serve as a deterrent against future operations.

Strategic Objectives:

- Protect sensitive military and strategic information from foreign espionage efforts.
- Assert DPRK's capability to defend its digital sovereignty and retaliate against cyber intrusions, maintaining a posture of strength and deterrence in the cyber domain.

Conclusion: These scenarios illustrate DPRK's strategic use of cyber operations to advance its interests, both in terms of offensive financial and political gains and in defensive postures against external threats. Operation Golden Sun highlights DPRK's proactive approach to overcoming economic challenges through cyber means, while Operation Silent Guardian underscores the regime's vigilance and readiness to counter sophisticated espionage efforts, safeguarding its sovereignty and strategic assets in the cyber landscape.