**1.0 Pre-Operational Planning and Intelligence Gathering**: Involves gathering intelligence through OSINT, HUMINT, phishing, and network scanning to identify vulnerabilities in the target.

1.1 OSINT Collection: Gathering publicly available information on targets through social media, public records, and online research.

1.2 Phishing and Spear-Phishing Campaigns: Targeted email campaigns aimed at obtaining credentials or planting malware.

1.3 Network Scanning: Identifying vulnerabilities in target networks using scanning tools to map attack vectors.

1.4 Account Takeover: Exploiting credentials obtained through phishing, brute force, or social engineering to impersonate a target and gain unauthorized access.

1.5 Advanced Persistent Threat (APT): State-sponsored or criminal organizations using covert techniques to compromise systems for long-term espionage or data exfiltration.

1.6 Cloud Access Management: Exploiting poor cloud configuration or mismanagement to gain unauthorized access to sensitive data stored in cloud systems.

1.7 Business Email Compromise (BEC): Impersonating executives or trusted individuals via email to manipulate financial transactions or gain sensitive information.

1.8 Watering Hole Attack: Compromising websites frequently visited by a target group to deploy malware.

**2.0 Weapon and Tool Preparation**: Focuses on assembling physical and digital tools, including IEDs, CBRNE devices, and custom malware for operations.

2.1 Weapon Assembly and Modifications: Assembling and modifying weapons to meet operational needs.

2.2 IED Design and Assembly: Designing Improvised Explosive Devices with customized triggers and payloads.

2.3 CBRNE Weapon Development: Developing and configuring Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) devices.

2.4 Exploitation Frameworks: Utilizing advanced cyber exploitation frameworks like Metasploit and Cobalt Strike to automate the exploitation of vulnerabilities.

2.5 Brute Force Attack: Using automated tools to repeatedly guess usernames and passwords to gain access to accounts.

2.6 Credential Dumping: Extracting credentials from memory or files to gain further access or escalate privileges.

2.7 Password Spraying: Attempting common passwords across multiple accounts to avoid triggering account lockouts.

**3.0 Operational Security (OPSEC)**: Implements security measures like encryption, anonymization, and persistence mechanisms to maintain secrecy and evade detection.

3.1 Use of Encrypted Messaging Apps: Using secure communication tools to avoid interception.

3.2 Use of TOR and VPNs for Anonymity: Protecting digital communications and masking online presence.

3.3 Use of Command and Control (C2) Infrastructure: Setting up C2 servers to maintain control over compromised machines and networks.

3.4 DNS Tunneling: Using DNS queries to exfiltrate data or bypass security controls.

3.5 Web Shell Installation: Installing web shells on compromised servers to maintain persistent access.

3.6 Living Off the Land (LotL): Using legitimate system tools like PowerShell to conduct attacks and evade detection.

**4.0 Financing and Funding Operations**: Uses methods like cryptocurrency laundering and crowdfunding to raise and obscure operational funds.

4.1 Exploitation of Crowdfunding Platforms: Raising funds under false pretenses using online platforms.

4.2 Use of Cryptocurrency for Fundraising: Leveraging digital currencies to finance operations while evading controls.

4.3 Cryptocurrency Laundering through Mixers and Tumblers: Obfuscating the source of funds to bypass financial tracking.

4.4 Cryptojacking Attack: Using compromised systems or cloud environments to mine cryptocurrency without the owner's knowledge.

4.5 Cloud Cryptomining: Using cloud infrastructure to mine cryptocurrencies without authorization.

**5.0 Reconnaissance and Targeting**: Involves mapping networks, selecting critical infrastructure, and exploiting third-party vulnerabilities for operational advantage.

5.1 Network Enumeration: Mapping target networks to identify weaknesses.

5.2 Vulnerability Exploitation: Identifying and exploiting vulnerabilities in target systems.

5.3 Target Selection of Critical Infrastructure Sectors: Identifying high-value infrastructure targets.

5.4 Cloud and IoT Exploitation: Targeting misconfigurations and vulnerabilities in cloud infrastructures and Internet of Things (IoT) devices.

5.5 Supply Chain Vulnerability Exploitation: Targeting third-party vendors, software supply chains, or hardware manufacturers to insert backdoors or malicious code into critical systems.

5.6 Credential Stuffing: Using previously breached credentials across various services to gain unauthorized access.

5.7 Cross-Site Scripting (XSS): Injecting malicious scripts into websites to steal session cookies or redirect users to malicious sites.

5.8 DNS Hijacking: Redirecting DNS queries to malicious sites.

**6.0 Tactical Planning and Coordination**: Develops attack strategies, assigns roles, and conducts rehearsals to ensure coordinated and effective execution.

6.1 Developing Attack Strategies: Creating operational plans based on intelligence and identified vulnerabilities.

6.2 Assigning Roles and Responsibilities: Organizing team roles to ensure cohesive execution.

6.3 Contingency Planning: Developing backup plans to address potential failures.

6.4 Conducting Dry Runs and Rehearsals: Testing strategies and refining operational details.

6.5 Synchronizing Cyber and Physical Attacks: Coordinating timing and execution of cyber and physical elements.

6.6 Real-Time Communication and Coordination: Ensuring continuous communication during operations.

6.7 DDoS Attack: Overloading a system or service with traffic to render it inaccessible.

6.8 SQL Injection (SQLi): Manipulating web application inputs to gain unauthorized access to backend databases.

**7.0 Execution of Cyber and Physical Attacks**: Executes attacks on targets, including disabling security systems and targeting critical infrastructure or deploying WMDs.

7.1 Disabling Security Systems: Neutralizing security measures to facilitate attacks.

7.2 Targeting Critical Infrastructure: Attacking key infrastructure to disrupt services, with an emphasis on hybrid cloud, IoT, and traditional critical systems.

7.3 Deploying WMD (Chemical, Biological, Radiological, Nuclear): Executing attacks using unconventional weapons.

7.4 Data Exfiltration: Exfiltrating sensitive data from compromised networks using encryption, steganography, or tunneling techniques.

7.5 Ransomware Deployment: Deploying ransomware to lock or encrypt systems, demanding payment for restoration.

7.6 Targeted Malware: Deploying malware specifically designed for high-value targets or critical infrastructure.

**8.0 Post-Attack Activities and Evasion**: Focuses on covering tracks, deleting evidence, and using new identities or safe locations to evade capture.

8.1 Deleting Digital Evidence: Removing traces of activity from networks and devices.

8.2 Rotating Digital Identities: Switching digital identities to avoid detection.

8.3 Advanced Obfuscation Techniques: Employing data encoding, fileless malware, and polymorphic malware to evade detection and prevent forensic analysis.

8.4 Evading Detection through Mobility and Safe Houses: Using secure locations and strategies to avoid capture.

8.5 Fileless Malware: Deploying malware that operates entirely in memory without leaving traces on disk.

**9.0 Major Crimes**: Engages in violent crimes like robbery, arson, and murder to fund operations or spread fear.

9.1 Murder and Nonnegligent Manslaughter: Elimination of threats or intimidation.

9.2 Forcible Rape: Employed as a tool of terror, coercion, and control.

9.3 Robbery: Armed theft targeting valuable assets to fund operations.

9.4 Aggravated Assault: Violent attacks used to intimidate or eliminate opposition forces.

9.5 Burglary: Breaking into secure locations to steal valuable items.

9.6 Larceny-Theft: Theft of property without direct confrontation.

9.7 Motor Vehicle Theft: Stealing vehicles for use in operations.

9.8 Arson: Setting fires to destroy property and create chaos.

**10.0 Interaction with Law Enforcement and Exploitation**: Unintended or manipulative law enforcement encounters that may include, intelligence gathering, or evasive tactics, bribery or extortion.

10.1 Bribery and Corruption of Police and Officials: Leveraging corrupt practices to avoid prosecution.

10.2 Evasion Techniques During Arrest or Interrogation: Employing deception and legal manipulation.

10.3 Exploiting Law Enforcement Encounters: Manipulating interactions to gain intelligence.

10.4 Anti-Forensics Techniques: Using tools to corrupt logs, manipulate timestamps, and encrypt file systems to prevent forensic recovery.