🗳️ Esempi di *information operations* e di *cyber operations* nell'*electoral cycle*

Fase	*Information Operations*	*Cyber Operations*
🔧 **1. Fase Preparatoria / campagna Elettorale**	Fake news, deepfake, bot, dark advertising, SLAPP, intimidazioni digitali, doxing, flooding informativo, amplificazione selettiva, manipolazione di account dormienti, disinformazione strategica mirata/generalizzata, delegittimazione di individui e gruppi, minacce di azioni legali, sponsorizzazioni occulte finanziamenti a media e *social*	Malware, ransomware, wiperware, trojan phishing / spear phishing, SIM swapping, spoofing, MITM, SQL injection, brute-force, credential stuffing, keylogging, APT, remote access trojan, supply chain attack, identity theft, IP sharing, criptovalute, crowdfunding fittizi
🗳️ **2. Fase di Voto**	Fake news su sedi/orari, disinformazione su validità del voto, call center falsi,tTag "vota domani", manipolazione su affluenza e dati elettorali	DDoS/DoS su siti e sistemi, manomissione software/algoritmi/device di voto, fake app elettorali, MITM nei seggi, GPS spoofing, malware in sistemi di autenticazione, blackout
🧮 **3. Fase di Conteggio / verifica**	Pubblicazione risultati falsi, exit poll manipolati, narrative delegittimanti, contestazioni social, flooding social, teorie di brogli, falsi reclami online	SQL injection, ransomware su server, zero-day, MITM trasmissione dati, manipolazione log, firmware attack, audit trail tampering, attacchi a sistemi di pubblicazione
🏛️ **4. Post-Elezione**	Teorie complottiste e delegittimanti, campagne social di destabilizzazione, attivazione di troll e amplificatori, flooding informativo, destabilizzazione socio-politica, incitamento a proteste e sommosse	DDoS a infrastrutture critiche, DNS hijacking, botnet, attacchi a reti civili, cyber-attacchi a sistemi energetici/logistici, cognitive breach hacking