

Cognitive Warfare Threats & Mitigation Checklist

Phone / SMS Spoofing & Robocalls

- Verify unexpected calls through official channels.
- Deploy STIR/SHAKEN where supported.
- Use caller-ID reputation services.
- Educate staff on phone-based scams.

Email Impersonation & Spoofing (BEC)

- Enable SPF, DKIM, DMARC with reject/quarantine.
- Mandate MFA for email access.
- Train staff on BEC red flags.
- Use sandboxing for suspicious links/attachments.

Deepfakes & Synthetic Media

- Adopt watermarking and provenance standards.
- Validate media via independent channels.
- Educate public to question extraordinary media claims.
- Deploy AI-assisted detection tools (advisory only).

Image Manipulation & Narrative Framing

- Preserve metadata for critical images.
- Use forensic tools for image authenticity.
- Require source traceability for published images.

Voice Cloning & Synthetic Audio

- Require out-of-band verification for verbal requests.
- Ban sensitive actions from voice-only instructions.
- Adopt provenance and watermarking for audio.

Social-Media Botnets

- Deploy anomaly detection on accounts.
- Label automated accounts clearly.
- Rate-limit suspicious activity.
- Encourage platform transparency reports.

Targeted Advertising & Micro-Targeting

- Restrict micro-targeting in political ads.
- Audit ad libraries and archives.
- Limit sensitive attribute use in targeting.
- Increase transparency of sponsors.

Data Exfiltration / Hacking

- Apply zero-trust access controls.
- Regular patching and EDR deployment.
- Conduct vendor risk audits.
- Establish rapid breach response protocols.

Automated Disinformation (LLMs)

- Rate-limit mass content generation.
- Deploy spam/malicious-content filters.
- Fund fact-checking networks.
- Mandate AI output watermarking.

Psychological Operations & Memory Altering

- Invest in civic/media literacy programs.
- Support plural local journalism.
- Monitor for repeated manipulative narratives.

Identity Fraud & Deep Identity Spoofing

- Adopt MFA and phishing-resistant authentication.
- Use risk-based authentication checks.
- Restrict retention of sensitive PII.
- Deploy identity-verification protocols in high-risk contexts.