Cyber and Information Operations

Some of the most common means and methods behind cyber and information operations used by malicious actors to target elections.

CYBER OPERATIONS

Social engineering is a category of attack in which malicious actors manipulate their target into performing a given action or divulging certain information (often a login or password).

Spear-phishing is a social engineering attack in which malicious actors send an email attachment or link that is designed to infect a device or obtain sensitive information. Malicious actors often review a target's social media accounts and work environment to tailor an email to appear enticing and convincing.

Hacking refers to attacks that exploit or manipulate a target system in order to disrupt or gain unauthorized access.

SQL injection is a way for attackers to read and/or alter the contents of a user's database by manipulating forms that are publicly available or exposed. Properly validating any incoming information from users can help prevent this method of attack.

Port scans are similar to checking whether doors are locked and walking through those that are open. Attackers often use it to profile potential targets and conduct surveillance on the systems they are running. A skilled attacker can use this method to gain access to unprotected servers or networks.

Man in the middle (MITM) attacks occur when attackers insert themselves between two or more parties and gain access to any information in transit between those parties.

Distributed Denial of service (DDoS) attacks seek to prevent legitimate users from accessing information (e.g., databases, websites) or services by disrupting access. Attackers disrupt service by using multiple computers and Internet connections to flood a target with excessive traffic, causing the service to crash.

Insider threat is a category of attack in which a current or former employee or authorized individual with access to a network, system, or data deliberately uses their access for malicious purposes.

INFORMATION OPERATIONS

Information Operations (IO) include propaganda, disinformation, and other tools used to manipulate public perception. Digital technologies have enabled adversaries to conduct IO at an unprecedented scale and to an unprecedented effect. In the context of elections, adversaries might use IO to undermine trust in an election result, exacerbate political divisions, or sow confusion and dissent.

Leaking stolen information: Attackers penetrate networks to obtain and leak sensitive information. Leaking information about budgets, election system vulnerabilities, or sensitive processes can reduce public trust.

Spreading false or misleading information: Attackers may hijack official accounts, or use social media or paid ads to distribute false information (e.g., polling times/places, election results), discredit a candidate, election officials, or voting system integrity.

Amplifying divisive content: Malicious actors often use existing social or political tensions to stoke divisions, distract, and disrupt a target to divert their resources.

Interrupting service to public-facing online resources: Attackers may use this tactic to accomplish a broader strategic objective. A DoS attack can serve to undermine trust in electoral systems or government services.