Information operations based on the dissemination of information (e.g., social media campaigns that are legal in most countries)

Cyber operations based on unauthorized access to systems (i.e., hacking that is illegal in the country where effect occurs)

Mixed operations (e.g., the dissemination of illegally obtained information)

**TYPES OF INTERFERENCE**

**ELECTORAL DIMENSION**

1. **Voter Preference**
   - Months and weeks leading up to the election (depending on the country, potentially including primaries)

2. **Voter Turnout**
   - Official voting period

3. **Voting Process**
   - Close to, during, and after election day (including potential efforts to delegitimize the election outcome afterward)

**POTENTIAL TARGETS**

1. Social media platforms
2. Party databases
3. E-pollbooks

1. Conventional news organizations
2. Campaign databases
3. Transmission channels for voting results

1. Election management bodies
2. Candidates’ and candidates’ families’ personal accounts
3. Election workers (intimidation and bribery)

1. Election infrastructure (e.g., voter registration databases, voter management systems)

**PROTECTIVE ACTIONS**

**COUNTRY A**

- Federal government/executive agency
- State/local government
- Legislative body
- Political party/campaign
- Election software companies and other relevant companies
- Conventional media company
- Social media company

**COUNTRY B**

- Federal government/executive agency
- State/local government
- Legislative body
- Political party/campaign
- Election software companies and other relevant companies
- Conventional media company
- Social media company

**LEARNING PROCESS**

Over time, between actors and across countries

© 2018 Carnegie Endowment for International Peace