Figure 1. **Analytical Framework for Election Interference**

TYPES OF INTERFERENCE

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)

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 2 3
Social media platforms
Conventional news organizations
Election management bodies
Election infrastructure
(e.g., voter registration databases, voter management systems)

1 2
Party databases
Campaign databases
Candidates' and candidates' families' personal accounts

3
E-pollbooks
Transmission channels for voting results
Election workers (intimidation and bribery)

PROTECTIVE ACTIONS

Legal

Technical

Policy

Operational

Educational/awareness raising

COUNTRY A

ACTORS

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

ACTORS

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