Pop-Up Case: Election Security

Intelligence shows that foreign actors are already interfering in the 2020 U.S. election. How should the United States respond?

Use the following case to spark discussion and help students to think through what they would do if they were decision makers. See the back of the page for some inspiration for how to structure your conversation.

The Situation:

Free and fair elections are essential to a functioning democracy. However, ensuring the integrity of U.S. elections is a growing national security challenge. As cyber capabilities become more advanced, foreign actors are increasingly targeting elections around the world through cyberattacks and disinformation campaigns in order to influence results, aggravate social and political tensions, and undermine confidence in democratic processes. Election interference not only threatens U.S. sovereignty but can also sow instability that hinders the government's ability to operate effectively. The U.S. intelligence community has concluded that Russia interfered in both the 2016 U.S. presidential election and the 2018 midterm elections by accessing state election systems and voter data, hacking and leaking Democratic National Committee emails, and spreading disinformation on social media. It does not appear that hackers directly manipulated any voter data, and it is difficult to know how successful the disinformation campaign was. But Russian interference struck a blow at confidence in U.S. elections. Analysts fear that if policymakers cannot ensure public trust in future elections, even the threat of interference could erode democratic systems and aggravate domestic divisions, weakening national security.

Intelligence agencies and security experts warn that the 2020 U.S. elections are already being targeted by Russia and are at risk of being targeted by China and Iran as well. Election interference is expected on multiple fronts. Most directly, foreign actors could launch cyberattacks on U.S. election infrastructure by hacking voting systems to manipulate votes. They could also attack voter registration systems in order to remove certain voters from the rolls, target them for disinformation, or impede their access to the polls. Cyberattacks could target specific campaigns or parties as well in search of damaging information to leak. Furthermore, disinformation campaigns on social media threaten to influence the outcome of an election and exacerbate partisan divisions. Even a small-scale or failed attack on an election would create mistrust in the democratic process. With elections fast approaching, policymakers face a renewed challenge to safeguard U.S. elections against foreign threats and to determine how to respond to actors seeking to interfere in the United States' democracy.

Learn more:

- The Trouble With Election Security (CFR.org)
- CSIS Election Cybersecurity Scorecard (CSIS.org)
- 'Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020 (*New York Times*)

Reuters/Ryan M. Kelly

Decision Point:

The U.S. intelligence community has reported that foreign actors, including Russia, have mounted campaigns to interfere in the upcoming U.S. 2020 election process. These are likely multipronged efforts involving disinformation campaigns and cyberattacks on election infrastructure or candidates. If not addressed, these efforts could undermine U.S. election integrity and damage public trust in democratic systems, potentially for years to come. The National Security Council (NSC) is meeting to advise the president on how the government should safeguard U.S. national elections. Members will need to address current insecurity in the country's election systems and determine if and how the United States should counter foreign interference.

NSC members should consider any combination of the following options:

- Prepare to employ cyber counterattacks and sanctions against perpetrators. Offensive measures could safeguard future elections, but they risk diplomatic fallout and do not secure current election systems.
- Provide federal funding to bolster election infrastructure and establish a task force to create election day contingency plans, oversee preelection testing on ballot machines, and provide cybersecurity training and support. This option enhances security but requires significant funds.
- Take executive action to regulate disinformation on social media and create a public awareness and media literacy campaign to educate voters. This option would address disinformation but not election infrastructure. In addition, regulations on social media could face criticism for limiting freedom of expression.
- Maintain current election practices while continuing to monitor and disclose threats and warn foreign actors of severe consequences if interference continues. This option would require the least commitment of resources but would not improve the security of upcoming elections.

Like Model Diplomacy? Try a full case at modeldiplomacy.cfr.org.

Pop-Up Case Guidelines

Pop-up cases from Model Diplomacy are short case studies on current events that put students in the shoes of policymakers facing the most pressing issues in international relations. There are lots of ways to organize a discussion using a pop-up case. It is always helpful to think about your goals for the discussion and then to consider any time or participation constraints you could have. If you are looking for some inspiration, here are a few ideas:

Gauge reaction:

If you want to show what students are thinking before diving into the discussion, here are two easy ways to do it. In one, often called "four corners," assign each policy option to a corner of the room, and then ask students to stand in the corner associated with the policy option they support. In the other, if you want your students to think along a spectrum instead (e.g., interventionist-isolationist, unilateral-multilateral, more urgent–less urgent), put the ends of your spectrum at either end of your blackboard and have students stand along the board to indicate where along the spectrum they fall. With both approaches, everyone will sit down again with a sense of where they stand regarding the case. Use this knowledge to shape discussion—eliciting less popular opinions, challenging more popular ones, encouraging like-minded students to further develop their ideas, or having students who disagree discuss in small groups.

Think-Pair-Share:

This exercise is particularly useful for groups where some students are hesitant. Ask everyone to spend a few minutes quietly gathering their thoughts and articulating them in a notebook ("think"), then have them turn to the person sitting next to them to compare notes ("pair"), and then have students report out to the whole group ("share"), knowing that everyone will have had time to think through something to say.

Whiparound:

Ask students to briefly share their position one after the other without responding to each other. Typically, everyone speaks in the order they are sitting. This can be a way to see where everyone stands before launching into a discussion. If you expect a topic to be particularly contentious, you could have students listen to each other and then reflect in writing.


Don Pollard

Simple NSC simulation:

If you would like to simulate a simplified version of a more realistic policy debate, you can appoint yourself (or a randomly chosen student) president. Ask students to debate the policy options (or come up with new ones) and try to reach consensus on a recommendation to the president.

NSC simulation with assigned opinions:

While assigning individual roles for a brief case study is complicated, you could assign opinions. For example, assign one-third of the class to be isolationist, one-third to favor a military response, and one-third to favor a diplomatic response. Let the groups caucus for a few minutes, then present their policy options and debate them, leaving the final decision up to you (or a student) as president.

Note: In our experience, simulations are often most productive if students imagine they are advising a generic president rather than a specific one.

Like Model Diplomacy? Try a full case at modeldiplomacy.cfr.org.