COUNCIL on FOREIGN RELATIONS | CFR Education Global Matters

Simulation from Technology and Conflict & Warfare

Cyber Clash With China (NSC)

Tensions escalate between the United States and China as the Nasdaq faces a devastating cyberattack.

Case Overview

Fictional, set in the present day. Cyberspace is a new domain of conflict that has few accepted standards of behavior. Basic questions about it—including how countries should respond to cyberattacks—are still unresolved. In recent years, China has exerted authority over areas of the South China Sea also claimed by other Asian countries, leading to tension with the United States. Last week, following several near misses in the South China Sea between U.S. and Chinese military vessels and aircraft, as well as the theft of documents from U.S. military networks, the U.S. Air Force conducted a flight near a shoal claimed by China. Three days later, the Nasdaq stock market was hacked, which significantly harmed the U.S. economy. U.S. intelligence agencies believe some in the Chinese government knew about the attack, for which a Chinese hacker collective claimed credit. National Security Council members need to advise the president on the merits of a cyber response, economic sanctions, or military measures.

Guide

Global Literacy

Global literacy is the ability to understand and engage effectively in today's interconnected world. Today's interdependent global economy and geopolitical landscape connect America's interests more than ever to the actions and interests of other countries and their citizens. To ensure students understand this interconnected world, they need to be globally literate. Learn more about global literacy.

The United States plays a critical role in establishing and maintaining international order. This is particularly true in an increasingly globalized world. The range of foreign policy issues that require its attention is vast. The United States must consider foreign policy issues from conflicts in Afghanistan, Nigeria, and Syria to tensions with Iran and North Korea; from long-standing alliances to complex, evolving relationships with Brazil, China, India, Russia, and South Africa. Issues on the agenda range from the stability of global finance to the promotion of economic opportunity in low-income countries; and from climate to health to nuclear proliferation to terrorism. The United States has a vested interest in myriad world affairs. Further, issues such as immigration, trade, cybersecurity, climate change, and global health underscore the fading distinction between domestic and international matters.

U.S. leaders use a range of tools to pursue a foreign policy to safeguard national security and achieve U.S. goals:

- diplomatic: consultations and negotiations, treaties, defense and security agreements, resolutions at global and regional bodies such as the United Nations, and public diplomacy to promote U.S. views and culture
- economic: trade and investment agreements, tariffs, sanctions, embargoes, development assistance, loans for the purchase of U.S.-manufactured products, and sales of arms, equipment, and technology
- military: missile strikes, nuclear deterrence, ground force deployments, ship and submarine patrols, blockades, unilateral or partnered military exercises, foreign military training, and special operations forces
- unconventional actions: undertaken by the U.S. government and its proxies, such as training and assisting foreign intelligence services, supporting armed nonstate actors, private security contracting, and cyberwarfare

Effective policymaking requires a deft combination of these tools. To accomplish this, policymakers must clearly define U.S. interests. Policymakers then gauge the interests, resources, and motivations of foreign governments and nonstate actors. The U.S. intelligence community supports policymakers by collecting and analyzing a vast range of information, including satellite images, communications records,, and other data.
Foreign policy successes and failures are often associated with presidential decisions. Less explored is the decision-making system that helps the president make those critical choices and coordinate their implementation. This guide will help you understand the system through which the United States creates and implements its foreign policy.

To learn more about the NSC, check out these readings:

- "What is the National Security Council?," YouTube video, 2:28, posted by CFR Education, August 28, 2023.
- "National Security Council," The White House.
- David J. Rothkopf, "Presidents and the National Security Council," Interview by Bernard Gwertzman, Council on Foreign Relations, November 12, 2008.

Regardless of the scale of the problem, a successful foreign policy–making process starts by defining interests and goals. Policymakers and their advisors then formulate policy options to meet those goals and consider each option's strengths and weaknesses. This process is challenging. In the best of times information can be unreliable or incomplete or an adversary's intentions can be unclear. Often a decision's consequences can be unknowable. Leaders frequently have to choose from a list on which every option is imperfect. Adding to this uncertainty is the complexity of the U.S. government's foreign policy machinery. Numerous agencies—each with its own interests and biases—seek to influence how policy is decided and carried out. It takes considerable effort to run a process capable of producing sound policy decisions.

The National Security Council (NSC) plays a critical role in this effort. Its mission is to help the president effectively use a variety of instruments—military, diplomatic, or otherwise—to forge policies that advance U.S. national security goals.

The NSC was created by the National Security Act of 1947. This act defined the NSC as an interagency body intended to "advise the president with respect to the integration of domestic, foreign, and military policies relating to the national security." The period after World War II was an age of expanded American interests and responsibilities. The NSC was expected to provide a place where the heads of federal departments and agencies could cooperate to develop recommendations for policies that would advance U.S. aims. The NSC and its staff were also meant to manage the policymaking process. This ensured that the president would receive a full range of advice and opinion from the departments and agencies involved in national security.

The NSC has evolved significantly over the years. The NSC has adapted to the preferences of successive presidents and the challenges they faced. Variables such as the attendees, the frequency of meetings, the manner in which information is passed to the president, the importance of consensus, and the relative dominance of the NSC over other government institutions have changed over the decades.

The NSC has evolved to comprise various interagency committees and a large staff to prepare analysis and coordinate policymaking and implementation. The NSC is at the center of the interagency process. This process is one through which relevant government agencies address foreign policy issues and help the president make and execute policy choices.

I. National Security Advisor

The national security advisor (formally assistant to the president for national security affairs) is at the heart of the NSC structure. The national security advisor's role is twofold: to offer advice to the president and to coordinate and manage policymaking. Because they have direct access to the president and do not represent a cabinet department, national security advisors are in a unique position. From this neutral perch they drive foreign policy decisions, manage the actors involved, and mitigate conflict throughout the decision-making process.

II. National Security Council Staff

The NSC staff consists of individuals from a collection of agencies that support the president, the vice president, and the administration. NSC staff members are generally organized into directorates that focus on regions or issues. The size and organization of the staff vary with each administration.

The NSC staff provides expertise for the variety of national security policy matters under consideration. It manages numerous responsibilities, including preparing speeches, memos, and discussion papers and handling inquiries from Congress on foreign policy issues. Staff members analyze both immediate and long-standing issues and help prioritize the agenda.

III. Committee Structure

Committees are at the core of policy deliberation and policymaking in the NSC. They fall into four categories:

- The highest level is the National Security Council itself. Formal NSC meetings are chaired by the president and include individuals named by the National Security Act of 1947 as well as other senior aides the president invites.
- The Principals Committee (PC) comprises cabinet-level officials who head major government departments concerned with national security, such as the secretaries of state and defense. The national security advisor traditionally chairs the Principals Committee.
- The Deputies Committee (DC) includes the deputy leaders of the government departments represented on the principals committee and is chaired by the deputy national security advisor.
- Interagency Policy Committees (IPCs) cover a range of regional areas and issues. Each committee includes officials who specialize in the relevant area or issue at one of the departments or agencies in the interagency system. IPCs are generally chaired by senior directors on the NSC staff. Much of the day-to-day work needed to formulate and implement foreign policy across the U.S. government happens at the IPC level.

This committee structure tackles both immediate crises such as an outbreak of conflict and enduring issues such as climate change. IPCs conduct analysis on an issue, gather views on it and its importance from various departments, formulate and evaluate policy options, and determine what resources and steps would be required to carry out those options. The Deputies Committee manages the interagency process up and down. It decides what IPCs to establish. and gives them specific assignments. It also considers information submitted by the IPCs before relaying it to the Principals Committee or the full NSC.

The Principals Committee is the highest-level setting, aside from the NSC itself, for debating national security issues. It consists of the heads of the NSC's component agencies. The Principals Committee is essentially all the members of the NSC except the president and vice president. Formal NSC meetings, which the president chairs, occur whenever the president sees fit. They consider issues that require the president's personal attention and a direct presidential decision.

The goal of this committee structure is to foster consensus on policy options or highlight where and why consensus cannot be reached. If officials at one level agree on an issue, it does not need to go to senior officials for a decision. This practice reserves the president's time and that of members of the Principals Committee for the most complicated and sensitive debates.

When a crisis erupts issues sometimes do not follow the usual path up from the IPCs. In these cases, NSC staff members and officials in government departments and agencies generally draft papers drawing on their expertise, available intelligence, and any existing contingency plans. Policy options are then debated and decided at the appropriate level. The policymaking process can also deviate from this model based on the preferences of each president.

For the purposes of this NSC simulation, you will role-play the NSC meeting with the assumption that the committees described have already done their jobs. Any critical information has already been passed to the highest-level decision-makers.

Presidential Decisions

When the president makes a policy decision, it can take the form of a verbal instruction recorded and shared with relevant departments and agencies. The president can also issue formal decisions in documents that lay out the administration's policy and explain its rationale and goals. These documents have gone by different names under different presidents. President Joe Biden issues national security memoranda and national security study memoranda. President Donald Trump issued national security presidential memoranda.

The president can also issue an executive order (EO). EOs are a more formal and public declaration of policy. In contrast, national security directives are generally directed internally to federal departments and are often classified. In the past, presidents have issued EOs for such purposes as facilitating sanctions against foreign individuals and establishing new offices in government departments to carry out foreign policy aims. For federal agencies, both national security directives and executive orders carry the full force of law.

Although many executive branch departments and agencies are involved in foreign policy, the Department of State, the Department of Defense, and the intelligence community form the core of the foreign policy bureaucracy. The Department of the Treasury, the Department of Homeland Security, and the Department of Justice often play crucial roles as well.

Department of State

The Department of State conducts the United States' relations with other countries and international organizations. It maintains U.S. diplomatic presence abroad. The Department of State also issues visas for foreigners to enter the country, aids U.S. citizens overseas, and manages other programs to promote American interests. The secretary of state is the president's principal foreign affairs advisor and has a keen understanding of the United States' international relations. They are also well informed on the relationships between foreign countries, and the behavior and interests of their governments.

Department of Defense

The Department of Defense carries out U.S. defense policy and maintains U.S. military forces. It includes the U.S. Army, Navy, Marine Corps, and Air Force, as well as an array of agencies related to defense. The department employs more than two million military and civilian personnel and operates military bases around the world. The secretary of defense is the head of the department and the president's principal defense policy advisor. They also stay up-to-date on the security situation in foreign countries and the possibilities and implications of U.S. military involvement. The chairman of the joint chiefs of staff is the highest-ranking member of the U.S. armed forces and the president's top military advisor.

Intelligence Community

The U.S. intelligence community consists of eighteen agencies and organizations, including the Central Intelligence Agency (CIA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI), which gather and analyze intelligence. Each of these agencies has its own mission; for example, the NSA focuses on signals intelligence (information gathered from communications and other electronic signals) and the Defense Intelligence Agency on military information. The director of national intelligence is the president's principal advisor on intelligence issues. They oversee this network of agencies with the aim of ensuring that they work together and deliver the best possible information to U.S. policymakers.

Department of the Treasury

The Department of the Treasury carries out policy on issues related to the U.S. and global economies and financial systems. The secretary of the treasury serves as one of the president's chief economic advisors and is responsible for addressing a range of economic concerns. The Treasury's ten bureaus, which include the U.S. Mint and the Internal Revenue Service, do much of the department's work, which ranges from collecting tax to printing currency and executing economic sanctions.

Department of Homeland Security

Created soon after the terrorist attacks of September 11, 2001, the Department of Homeland Security works to counter and respond to risks to American security. It focuses on issues such as terrorism prevention, border security and immigration, disaster response, and cybersecurity. Familiar agencies within the department include U.S. Customs and Border Protection, the U.S. Secret Service, and the Transportation Security Administration. The secretary of homeland security oversees the department and advises the president on relevant issues.

Department of Justice

The Department of Justice investigates and prosecutes possible violations of federal law. The Department of Justice represents the U.S. government in legal matters and works more broadly to prevent and respond to crime. Agencies such as the FBI and the Drug Enforcement Administration are part of the department, as are divisions focusing on particular areas of law, such as national security and civil rights. Leading the department is the attorney general, who offers legal advice to the president and the heads of other departments.

Case Notes

Fuel a lively classroom discussion with simulations that put your students in the shoes of either the National Security Council or the UN Security Council.

CFR Education simulations can be run for several days or weeks and include background readings, videos, and assignments to help students understand the situation and their roles.

Instructions

How to Run a CFR Simulation Role-Play

The Issue

Cyberspace is a new domain of conflict, one guided by few accepted rules or standards of behavior. Policymakers find offensive cyber operations attractive because they are relatively inexpensive, can be designed to be less destructive than attacks against physical targets and can provide a high degree of anonymity to the attacker. Most of these operations include cyber espionage (theft of military and political secrets or intellectual property) and political disruptions (website defacement or distributed denial-of-service [DDoS] attacks, which flood a website with so much data that it can no longer respond).

The White House's 2023 National Cyber Strategy states that the United States "will use all instruments of national power to disrupt and dismantle threat actors whose actions threaten our interests." Experts generally assume that a cyberattack that causes death or physical destruction would be considered an armed attack. However, the threshold for a military response to

other forms of cyberattack remains uncertain. Defending against cyber threats is extremely difficult. Would-be defenders need to worry about millions of lines of computer code, hundreds of devices, and scores of networks. An attacker, on the other hand, only needs to find one vulnerability.

Determining who is responsible for cyberattacks is a difficult and slow process. Unlike other kinds of attacks, cyber attackers can hide their tracks more easily. The attacks can happen in minutes, if not seconds. Many countries also rely on proxies such as criminal groups, or patriotic hackers to conduct operations for them. Even if the hackers can be located, anyone anywhere could have authorized the attack. This conundrum greatly complicates efforts to retaliate and prevent attacks.

Successful attacks could also risk military escalation. If military leaders fear that their networks or weapons systems could be subjected to cyberattacks—which would limit their ability to order forces in the field or to launch weapons—they would have an incentive to use their weapons systems preemptively. Such a move would escalate and further destabilize a conflict.

Hypothetical Decision Point

China, Brunei, Malaysia, the Philippines, Taiwan, and Vietnam have competing territorial claims in the South China Sea. In recent years, China has exerted authority over the area by increasing the size of existing islands or creating new ones. China has also constructed ports, military installations, and airstrips. The United States has promoted the right of military vessels to operate in China's claimed two-hundred-mile exclusive economic zone. Furthermore, the United States has rejected China's claim to a twelve-mile territorial zone around the artificial islands it has built. Since 2015, the United States has signaled its opposition by flying military aircraft and sending U.S. Navy ships near certain islands.

Last week, the U.S. Air Force conducted a flight near a shoal claimed by China in the South China Sea. Three days later, the Nasdaq Stock Market suffered a hack that damaged computers and forced the suspension of trading for two days. This imposed significant costs on various U.S. companies and dented confidence in the U.S. financial system. An underground hacker collective based in China known as the Zheng He Squadron has claimed responsibility for the hack. The group has known ties to the People's Liberation Army, China's military. U.S. intelligence agencies assess with 90 percent certainty that the hack occurred with the knowledge or support of parts of the Chinese government. Beijing claims no knowledge of the attack. The president has convened the National Security Council to discuss how the United States should respond.

Background

The Challenge of Cyberspace

The rapid diffusion of information technology has remade economics, politics, and international affairs. It has transformed commerce, making global supply chains possible and generating enormous wealth. It has created social and cultural networks that span the globe. It has enabled people to overcome distance and share knowledge and ideas. It has provided powerful tools for political organization and protest.

The digital revolution has also created new sources of vulnerability. Countries, terrorists, and criminals can shut down power, communication, transportation, and financial networks with the click of a mouse. These attacks inflict not just massive economic losses but also death and physical destruction.

In recent years, cyberattacks have grown in frequency and sophistication. The 2016 U.S. presidential election was marked by repeated hacking incidents linked to Russian intelligence. Attacks have also targeted U.S. critical infrastructure. One of the most extensive cyberattacks on the United States to date began in late 2019 or early 2020. This cyberattack began when a group of hackers hid a piece of malware in a widely used network management software made by the company Solar Winds. The hacking campaign ran undetected until December 2020. This span of time allowed the group to gain access to the networks of some eighteen thousand companies and government agencies that installed the software. The group was able to steal data from at least one hundred companies and nine U.S. government agencies. In May 2021, a ransomware attack on Colonial Pipeline forced the U.S. company to shut down operations. This resulted in fuel shortages along the eastern seaboard of the United States. The escalating scale and scope of those attacks have underscored the need to bolster U.S. cyber defenses.

Countries have yet to figure out how to limit competition in cyberspace. Malicious software (malware) is impossible to count or control. Agreements like those that limit nuclear competition do not exist for digital weapons. Although acceptance of international law in cyberspace is growing, great uncertainty remains about how it should be applied. Major powers, including the United States and China, have been willing to discuss threats in cyberspace but slow to develop a policy framework.

The evolution of U.S. Cyber Policy

Throughout the early 2000s, the United States was hesitant to openly acknowledge its operations in cyberspace. Experts widely believe that the United States and Israel were behind Stuxnet, one of the world's first cyber weapons. The malware was designed to slow Iran's nuclear program by damaging centrifuges at the Natanz nuclear facility in 2009. Still, both countries denied any involvement.

After years of silence, the U.S. government has gradually become more transparent about developing and using cyberattacks. The 2015 Defense Department Cyber Strategy explicitly recognized offensive missions. Furthermore, the Pentagon began to develop cyber capabilities that can support military operations. The first public acknowledgment of the United States using cyberweapons came in February 2016. It was here when Pentagon officials announced that U.S. Cyber Command had launched attacks against the self-proclaimed Islamic State. Since then, Cyber Command has grown from approximately nine hundred personnel to more than six thousand.

The United States and China have a history of clashes in cyberspace. According to a 2013 *Washington Post* report, Chinese hackers have stolen information relating to more than two dozen U.S. weapons programs. This stolen information includes the Patriot missile system, the F-35 Joint Strike Fighter, and the U.S. Navy's new littoral combat ship. The White House, the State Department, the Office of Personnel Management, and NASA have been breached. Attacks on U.S. companies including Adobe, Disney, General Electric, Google, Johnson & Johnson, and Yahoo have also been publicly reported. In addition, Chinese hackers have reportedly targeted the negotiation strategies and financial information in energy, banking, law, and other sectors.

In response to U.S. claims of Chinese hacking, China has noted that it is also a victim of cybercrime. China claims that the majority of attacks against it originate from internet protocol (IP) addresses in the United States, Japan, and South Korea. Chinese media were quick to echo claims by former National Security Agency contractor Edward Snowden that the United States hacks targets on the Chinese mainland and in Hong Kong.

Washington has steadily increased pressure on Beijing over cyber espionage. In April 2015, President Barack Obama signed an executive order that declared a national emergency to deal with the threat of "significant malicious cyber-enabled activities." This move allowed for economic sanctions against companies or individuals that profited from cyber theft. The order threatened to block financial transactions routed through the United States, prevent exports to the United States, and prevent executives of the companies that benefit from the hacks from traveling to the United States.

In August 2015, the *Washington Post* reported that the Obama administration planned to levy these sanctions against Chinese companies in the lead-up to a summit the following month between Presidents Barack Obama and Xi Jinping. Perhaps because of the threat, the summit produced a breakthrough agreement. Both sides agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." Washington and Beijing also agreed to identify and endorse norms of behavior in cyberspace. They agreed to establish two high-level working groups and a hotline between them. After departing the United States, Xi signed similar agreements with the United Kingdom and at a Group of Twenty meeting in Turkey.

Following the presidents' September summit, the cybersecurity firm FireEye reported a sharp decline in the number of Chinese cyberattacks. However, the firm also suggested that actors could simply have become stealthier and more difficult to detect. Former U.S. Assistant Attorney General John P. Carlin confirmed the company's findings that attacks were "less voluminous but more focused, calculated, and still successful."

The U.S.-China working group on security issues met only once before the end of the Obama administration, but the cybercrime group reported some progress. The two sides established a point of contact and a designated email address. They

also successfully cooperated on taking down websites with false information. After Donald Trump met Xi Jinping in April 2017, Washington and Beijing agreed to a U.S.-China Comprehensive Dialogue that would have four pillars, including one on law enforcement and cybersecurity. The negotiations broke down before the two countries could come to an agreement.

In 2018, the Trump administration implemented a series of sweeping tariffs on Chinese goods. The administration cited unfavorable trade practices and Chinese theft of American intellectual property. The resulting trade war stalled cooperation on cybersecurity. According to cybersecurity firms, cyberattacks on American businesses and government agencies have increased since the trade war began.

In September 2018, the Trump administration announced a more aggressive cybersecurity strategy. It authorized using offensive cyber operations as a deterrent against foreign cyberattacks. This strategy, known as defend forward, focused on observing, countering, and disrupting adversary operations before they affect U.S. networks. The Trump administration further oversaw the creation of the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security. The goal of CISA is to coordinate and improve government defenses against cyberattacks. Despite this increase in offensive operations, officials have continued to warn that critical U.S. government agencies remain dangerously unprepared to defend against cyberattacks. For example, in June 2023, a group of Russian cybercriminals led a global cyberattack targeting personnel data from several U.S. government agencies.

The Joe Biden administration has reaffirmed the importance of cyber issues to U.S. national security and taken steps to improve U.S. cyber defenses. The administration also increased efforts to deter cyberattacks by imposing costs on perpetrators, and invigorate diplomatic efforts toward cyber norms. Soon after the May 2021 Colonial Pipeline attack, the Biden administration released an executive order designed to improve U.S. cybersecurity. This included a significant increase in funding. Requests for cyber operations in the 2023 defense budget totaled $13.5 billion, an increase of more than 30 percent from 2021. In addition to increasing the financial resources going towards cyber security, U.S. Cyber Command has also changed its approach in responding to cybersecurity threats. In a Cyber Strategy Report published in September 2023, the department called for expanding beyond its previous mandate of just protecting U.S. military networks. Instead, it suggested "opening up communications with other federal agencies and the private sector,...and increasing assistance to foreign allies."

Meanwhile, tensions between the United States and China have remained high. The first round of high-level talks between Washington and Beijing since Biden's inauguration were marked by tense rhetoric and yielded little progress toward addressing ongoing issues including cyber concerns. Although high-level meetings have continued to occur between the two leaders, concerns over Chinese activity in cyberspace have remained high. The Office of the Director of National Intelligence's 2023 Annual Threat Assessment underscored that China still represents "the broadest, most active, and persistent cyber espionage threat to the U.S. Government and private-sector networks." This sustained tension, coupled with continued U.S. vulnerabilities in cyberspace, highlights the continued need for increased cyber preparedness.

Role of the United States

The United States has an interest in ensuring that China does not assert its sovereignty claims over the South China Sea by using force or intimidation. Washington has sought to secure this interest through freedom of navigation operations—sending ships or aircraft into areas that China claims but that the United States considers open to all—as well as increased military exercises with its allies in the region. The United States also has an interest in defining the rules of behavior for cyberspace. It has tried to strengthen deterrence by building up offensive capabilities. It has demonstrated its ability to attribute attacks, indicting foreign hackers, and levying sanctions. It has also promoted norms of behavior through bilateral agreements and multilateral forums.

The principal policy options available in this case are discussed below. These responses are available individually, in combination, or all together.

Preparation and Role-Play

Fuel a lively classroom discussion with simulations that put your students in the shoes of either the National Security Council or the UN Security Council.

CFR Education simulations can be run for several days or weeks and include background readings, videos, and assignments to help students understand the situation and their roles.

Instructions

Video: How to Run a CFR Simulation Role-Play

Roles Overview

Print these custom placards for use during your simulation. If you need to edit them, make a copy to your Google Drive.

Roles

President

The president is the head of state and commander in chief of the U.S. Armed Forces. They preside over National Security Council (NSC) meetings and listens to the advice and information presented by others. The president is not expected to be an expert on any single subject, but instead draws on the expertise of the NSC to analyze options and choose what they feel is the best policy to advance U.S. interests.

The president's goals are to

- select one or more policy options after considering the opinions and recommendations of NSC members; and
- balance and promote U.S. interests, with an eye toward both immediate goals and long-term foreign policy strategy.

Issues for Consideration

- How does the cyberattack on Nasdaq, along with the other incidents that have recently occurred in this case, threaten U.S. national security?
- What are the principal dynamics of the U.S.-China bilateral relationship? What factors account for the competition and cooperation between the two countries? What does the current state of the relationship suggest about the potential effect of various U.S. actions in this case?
- What U.S. interests are at stake in this crisis—in the U.S. relationship with China, the disputes in the South China Sea, and the evolution of behavior in cyberspace?
- Where does cybersecurity fit into the broader context of U.S. national security concerns?
- What are the positions and interests of other countries and organizations that have a stake in both the evolving norms in cyberspace and the competing territorial claims in the South China Sea? How might they help resolve, exacerbate, or otherwise shape the current situation?
- What is the status of international norms for state behavior in cyberspace? How might the policy options in this case adhere to or defy these norms, to the extent that they exist?
- What are the costs, benefits, and risks that accompany each policy option open to the United States?
- What are the trade-offs raised by the potential policy options in this case?

Vice President

The vice president must be ready at a moment's notice to assume the presidency if the commander in chief is unable to perform their duties. Vice presidents can play a relatively active role on the National Security Council (NSC), serving as a general advisor and freely advocating their own positions during meetings. In particular, the president may ask the vice president to serve as an independent voice, untethered to any of the agencies represented by other NSC participants. The president may also ask about the interaction between the issue at hand and the domestic political situation, including in Congress.

The vice president's goals are to

- provide advice to the president on any topic, including those overlooked by other NSC participants; and
- understand the range of views in Congress and work to build congressional and public support for the president's chosen approach.

Issues for Consideration

- How does the cyberattack on Nasdaq, along with the other incidents that have recently occurred in this case, threaten U.S. national security?
- What are the principal dynamics of the U.S.-China bilateral relationship? What factors account for the competition and cooperation between the two countries? What does the current state of the relationship suggest about the potential effect of various U.S. actions in this case?
- What U.S. interests are at stake in this crisis—in the U.S. relationship with China, the disputes in the South China Sea, and the evolution of behavior in cyberspace?
- Where does cybersecurity fit into the broader context of U.S. national security concerns?
- What is the range of attitudes in Congress on cybersecurity and internet governance, particularly in the context of U.S.-China relations?
- How do the media and public opinion affect U.S. policy toward China, especially regarding cybersecurity and internet governance?
- What are the costs, benefits, and risks that accompany each policy option open to the United States?
- What are the trade-offs raised by the potential policy options in this case?

Chief of Staff

The chief of staff oversees the Executive Office of the President, which provides the president with support to govern effectively. This post has traditionally been home to many of the president's closest advisors. In National Security Council (NSC) meetings, the chief of staff ensures that the president has the necessary analysis on the full range of factors relevant to the case, including the U.S. political situation. They also guide the process of implementing and communicating presidential decisions.

The chief of staff's goals are to

- highlight the domestic implications of U.S. foreign policy choices; and
- develop strategies to carry out the president's policy and communicate it to U.S. and international audiences.

Issues for Consideration

- How does the cyberattack on Nasdaq, along with the other incidents that have recently occurred in this case, threaten U.S. national security?
- What are the principal dynamics of the U.S.-China bilateral relationship? What factors account for the competition and cooperation between the two countries? What does the current state of the relationship suggest about the potential effect of various U.S. actions in this case?
- What U.S. interests are at stake in this crisis—in the U.S. relationship with China, the disputes in the South China Sea, and the evolution of behavior in cyberspace?
- Where does cybersecurity fit into the broader context of U.S. national security concerns?
- What is the range of attitudes in Congress on cybersecurity and internet governance, particularly in the context of U.S.-China relations?
- How do the media and public opinion affect U.S. policy toward China, especially regarding cybersecurity and internet governance?
- What are the costs, benefits, and risks that accompany each policy option open to the United States?
- What are the trade-offs raised by the potential policy options in this case?

National Security Advisor

The national security advisor (NSA) has a special role in crisis management, serving as the "honest broker" for the national security policy process. Although the president makes final decisions, the NSA is responsible for ensuring that they have all the necessary information, that a full range of viable policy options has been articulated, that the prospects for success and failure have been identified, that any legal issues have been addressed, and that all members of the National Security Council (NSC) have had the opportunity to contribute.

The national security advisor's goals are to

- facilitate the president's consideration of issues by keeping the NSC discussion on track and guiding it toward concrete policy options; and
- build trust as an honest broker among the other NSC participants.

Issues for Consideration

- How does the cyberattack on Nasdaq, along with the other incidents that have recently occurred in this case, threaten U.S. national security?
- What are the principal dynamics of the U.S.-China bilateral relationship? What factors account for the competition and cooperation between the two countries? What does the current state of the relationship suggest about the potential effect of various U.S. actions in this case?
- What U.S. interests are at stake in this crisis—in the U.S. relationship with China, the disputes in the South China Sea, and the evolution of behavior in cyberspace?
- Where does cybersecurity fit into the broader context of U.S. national security concerns?
- What are the most important factors for the president to balance when making a decision?
- What are the costs, benefits, and risks that accompany each policy option open to the United States?
- What are the trade-offs raised by the potential policy options in this case?

Secretary of State

The Department of State maintains the U.S. diplomatic presence around the world, conducting foreign relations and using an on-the-ground perspective to generate country-specific knowledge. As head of the department, the secretary draws on this

knowledge to present an authoritative view of the United States' bilateral relationships, the relationships between foreign countries, and the behavior and interests of foreign governments.

The secretary of state's goals are to

- serve as the president's principal foreign policy advisor; and
- analyze how policy options will affect the interests, reputation, and relationships of the United States.

Issues for Consideration

- How does the cyberattack on Nasdaq, along with the other incidents that have recently occurred in this case, threaten U.S. national security?
- What are the principal dynamics of the U.S.-China bilateral relationship? What factors account for the competition and cooperation between the two countries? What does the current state of the relationship suggest about the potential effect of various U.S. actions in this case?
- What U.S. interests are at stake in this crisis—in the U.S. relationship with China, the disputes in the South China Sea, and the evolution of behavior in cyberspace?
- What are the positions and interests of other countries and organizations that have a stake in both the evolving norms in cyberspace and the competing territorial claims in the South China Sea? How might they help resolve, exacerbate, or otherwise shape the current situation?
- What is the state of U.S. relations with the countries competing with China for territorial and jurisdictional control over islands in the South China Sea?
- What is the status of international norms for state behavior in cyberspace? How might the policy options in this case adhere to or defy these norms, to the extent that they exist?
- In what way do the competing territorial claims in the South China Sea affect U.S. national security?
- What interest does the United States have in the sovereignty of the islands there and in the stability of the South China Sea?
- What are the costs, benefits, and risks that accompany each policy option open to the United States?

Secretary of Defense

The secretary of defense is the principal defense policy advisor to the president, under whose direction they exercise authority over the Department of Defense. In National Security Council (NSC) meetings, the secretary analyzes the security situation in the relevant region and explains the likely implications of U.S. military involvement, both for the immediate crisis and for the United States' overall strategic position.

The secretary of defense's goals are to

- understand the options for and feasibility of any military action, as well as its possible outcomes; and
- identify ways to prevent the deterioration of a crisis to the point where it mandates U.S. military intervention.

Issues for Consideration

- How does the cyberattack on Nasdaq, along with the other incidents that have recently occurred in this case, threaten U.S. national security?
- What are the immediate security risks of the policy options being considered in this case? For example, what might be the implications or consequences of sending more U.S. military forces near Chinese forces in the South China Sea? What might be the implications of any Chinese retaliation for a U.S. cyberattack on Chinese networks?

- Does the current situation as presented in this case mandate consideration of military action by the United States? If so, what kind? If not, what conditions would necessitate such consideration?
- If the United States were to respond militarily in this case, what should its goals be? How should it determine when the military mission has been completed?
- What are China's general military capabilities? How have they evolved in recent years, especially in the western Pacific Ocean? What do these circumstances suggest about the U.S. policy response in this case, particularly about situations that might bring U.S. forces into contact with Chinese ones?
- What are the military capabilities of countries with competing claims in the South China Sea?
- What are the similarities and differences between cyber weapons and kinetic (physical) weapons? How might the use of each type of weapon by the United States be perceived in this case?
- What are the costs, benefits, and risks of using a military response in this case?

Secretary of the Treasury

The Department of the Treasury carries out policy on issues related to the U.S. and global economies and financial systems. The secretary of the treasury, as head of this department, serves as one of the president's chief economic advisors. In National Security Council (NSC) meetings, they analyze the economic dimensions of foreign policy issues and weigh the potential impact of policy options on U.S. economic concerns, including growth, trade and investment, and the position of the U.S. dollar.

The secretary of the treasury's goals are to

- serve as a senior presidential advisor on economic policy; and
- determine how foreign policy options might affect the U.S. economy and financial system, the global economy, and economic relations between the United States and others.

Issues for Consideration

- How does the cyberattack on Nasdaq, along with the other incidents that have recently occurred in this case, threaten U.S. national security?
- How does the situation as presented in this case affect the U.S. economy? How might the economic effects evolve should the crisis endure, intensify, or abate?
- What is the nature and scope of the U.S. economic relationship (including trade and investment) with China? What are the possible effects of a continued crisis on the U.S. and Chinese economies?
- What is the role of sanctions in responding to cyberattacks and in past and present U.S.-China relations? What are the potential implications of using sanctions in response to the current crisis?
- What are the economic costs, benefits, and risks that accompany each policy option open to the United States?
- What are the costs, benefits, and risks of imposing sanctions in this case?
- What are the trade-offs raised by the potential policy options in this case?

Chairman of the Joint Chiefs of Staff

The chairman of the Joint Chiefs of Staff (CJCS) is the highest-ranking member of the U.S. military and the principal military advisor to the president, the secretary of defense, the National Security Council (NSC), and the Homeland Security Council. The CJCS does not exercise command authority over U.S. troops. Instead, they work with the heads of the U.S. military services to provide advice to the president and other senior leaders.

The CJCS's goals are to

- serve as the president's military advisor on the NSC; and
- advise the president on specific military options and the corresponding risks, benefits, and implications.

Issues for Consideration

- How does the cyberattack on Nasdaq, along with the other incidents that have recently occurred in this case, threaten U.S. national security?
- What are the immediate security risks of the policy options being considered in this case? For example, what might be the implications or consequences of sending more U.S. military forces near Chinese forces in the South China Sea? What might be the implications of any Chinese retaliation for a U.S. cyberattack on Chinese networks?
- Does the current situation as presented in this case mandate consideration of U.S. military action? If so, what kind? If not, what conditions would necessitate such consideration?
- If the United States were to respond militarily in this case, what should its goals be? How should it determine when the military mission has been completed?
- What are China's general military capabilities? How have they evolved in recent years, especially in the western Pacific Ocean? What do these circumstances suggest about the U.S. policy response in this case, particularly about situations that might bring U.S. forces into contact with Chinese ones?
- What are the military capabilities of countries with competing claims in the South China Sea?
- What are the similarities and differences between cyber weapons and kinetic (physical) weapons? How might the use of each type of weapon by the United States be perceived in this case?
- What are the costs, benefits, and risks of using a military response in this case?

Attorney General

The attorney general is the head of the Department of Justice and the chief lawyer of the U.S. government. The department represents the United States in legal matters, including by prosecuting violations of federal law. In National Security Council (NSC) meetings, the attorney general gives the president advice and opinions on the legal aspects of policies under consideration.

The Attorney General's goals are to

- consider the legal elements and implications of U.S. foreign policy options; and
- ensure that any policies decided by the NSC are in compliance with domestic and international law.

Issues for Consideration

- How does the cyberattack on Nasdaq, along with the other incidents that have recently occurred in this case, threaten U.S. national security?
- Why is it difficult to attribute responsibility for cyberattacks? What are the implications of this difficulty for developing norms of behavior in cyberspace and for a U.S. response to the Nasdaq hack in this case?
- What issues of U.S. and international law does this case raise? How should these legal issues shape consideration of a U.S. policy response?
- What has been the evolution of official U.S. policy on internet governance and cyber strategy?
- What are the costs, benefits, and risks that accompany each policy option open to the United States?
- What are the trade-offs raised by the potential policy options in this case?

Director of National Intelligence

The U.S. intelligence community consists of seventeen agencies and organizations that gather and analyze intelligence to help policymakers formulate and implement U.S. foreign policy. The director of national intelligence oversees this network of agencies. They focus on providing the latest relevant information to National Security Council (NSC) members and articulating the capabilities and interests of the intelligence community.

The director of national intelligence's goals are to

- provide complete, accurate, and up-to-date information to the NSC on the situation under discussion; and
- serve as the principal advisor to the president and the NSC on intelligence matters.

Issues for Consideration

- How does the cyberattack on Nasdaq, along with the other incidents that have recently occurred in this case, threaten U.S. national security?
- Where does cybersecurity fit into the broader context of U.S. national security concerns? How should this analysis shape your consideration of policy options in this case?
- What are the positions and interests of other countries and organizations that have a stake in both the evolving norms in cyberspace and the competing territorial claims in the South China Sea? How might they help resolve, exacerbate, or otherwise shape the current situation?
- What are the immediate security risks of the policy options being considered in this case? For example, what might be the implications or consequences of sending more U.S. military forces near Chinese forces in the South China Sea? What might be the implications of any Chinese retaliation for a U.S. cyberattack on Chinese networks?
- What are the primary interests, motivations, and goals of the major actors in this crisis? What factors drive potential responses to it?
- Why is it difficult to attribute responsibility for cyberattacks? What are the implications of this difficulty for developing norms of behavior in cyberspace and for a U.S. response to the Nasdaq hack in this case?
- In what way do the competing territorial claims in the South China Sea affect U.S. national security? What interest does the United States have in the sovereignty of the islands there and in the stability of the South China Sea?
- What are the trade-offs raised by the potential policy options in this case?

U.S. Permanent Representative to the United Nations

The role of the U.S. permanent representative to the United Nations (UN) is to advance U.S. foreign policy interests in the bodies and forums of the UN system.?Reporting to the secretary of state, the permanent representative helps formulate and articulate the U.S. position on all political and security matters under discussion at the UN. At National Security Council (NSC) meetings, they outline policy steps available to the United States at the UN and advises NSC participants on the positions and actions of other UN member states.

The U.S. permanent representative to the UN's goals are to

- advise the president and secretary of state on the diplomatic actions the United States can or should take at the UN; and
- promote the United States' interests and values at the UN.

Issues for Consideration

- How does the cyberattack on Nasdaq, along with the other incidents that have recently occurred in this case, threaten U.S. national security?

- What are the principal dynamics of the U.S.-China bilateral relationship? What factors account for the competition and cooperation between the two countries? What does the current state of the relationship suggest about the potential effect of various U.S. actions in this case?
- What are the positions and interests of other countries and organizations that have a stake in both the evolving norms in cyberspace and the competing territorial claims in the South China Sea? How might they help resolve, exacerbate, or otherwise shape the current situation?
- What position do UN member states, particularly those on the Security Council, take on cyberattacks and on competing claims in the South China Sea? How are these governments likely to react to various policy responses by the United States? How should the United States take these views into account when deliberating its policy options?
- What has been the role of the United Nations and its component parts in developing norms for state behavior in cyberspace and responding to cyberattacks? What role could or should the United Nations play in addressing the current crisis?
- What is the status of international norms for state behavior in cyberspace? How might the policy options in this case adhere to or defy these norms, to the extent that they exist?
- What are the costs, benefits, and risks that accompany each U.S. policy option?
- What are the trade-offs raised by the potential policy options in this case?

Special Assistant to the President and Cybersecurity Coordinator

The Special Assistant to the President and Cybersecurity Coordinator works through the interagency process to manage the development and implementation of the country's strategy and policies on cybersecurity. Rather than offering specific technical solutions, the special assistant is charged with coordinating policy responses among components of the U.S. government. The special assistant also oversees the relationship between the federal government and foreign governments, state and local governments, businesses, and other organizations on cybersecurity issues.

The goals of the Special Assistant to the President and Cybersecurity Coordinator are to

-advise the president on matters relating to cybersecurity, including the political, economic, and military dimensions of the issue; and
-provide guidance on devising and implementing policy responses to cyberattacks or other harmful cyber activity aimed at the United States.

Issues for Consideration

- How does the cyberattack on Nasdaq, along with the other incidents that have recently occurred in this case, threaten U.S. national security?
- Where does cybersecurity fit into the broader context of national security concerns facing the United States? How should this analysis shape your consideration of policy options in this case?
- Why is it difficult to attribute responsibility for cyberattacks? What are the implications of this difficulty for developing norms of behavior in cyberspace, and for a U.S. response to the hack on the NASDAQ in this case?
- What has been the evolution of official U.S. policy on internet governance and cyber strategy?
- What are some past examples of cyberattacks believed to have been carried out by the United States and other countries or entities? What were the results of these attacks, and what do the results suggest about using a cyber response in this case?
- What are the similarities and differences between cyber weapons and kinetic (physical) weapons? How might the use of each type of weapon by the United States be perceived in this case?
- What are the costs, benefits, and risks of using a cyber response in this case?
- What are the trade-offs raised by the potential policy options in this case?

General Advisor to the President

The general advisor offers analysis and recommendations that are unconstrained by the interests of any department or agency. They are tasked with providing a comprehensive assessment of the situation at hand and ideas for policy options that serve U.S. interests.

The general advisor's goals are to

- understand the breadth of the issue and outline its stakes for the United States; and
- advise the president on the range of policy options proposed by all NSC members.

Issues for Consideration

- How does the cyberattack on Nasdaq, along with the other incidents that have recently occurred in this case, threaten U.S. national security?
- What are the principal dynamics of the U.S.-China bilateral relationship? What factors account for the competition and cooperation between the two countries? What does the current state of the relationship suggest about the potential effect of various U.S. actions in this case?
- What U.S. interests are at stake in this crisis—in the U.S. relationship with China, the disputes in the South China Sea, and the evolution of behavior in cyberspace? How should these various interests influence a U.S. response? How should they be prioritized?
- What are the positions and interests of other countries and organizations that have a stake in both the evolving norms in cyberspace and the competing territorial claims in the South China Sea? How might they help resolve, exacerbate, or otherwise shape the current situation?
- What is the range of attitudes in Congress on cybersecurity and internet governance, particularly in the context of U.S.-China relations? How might these attitudes influence the U.S. response to the crisis?
- What is the status of international norms for state behavior in cyberspace? How might the policy options in this case adhere to or defy these norms, to the extent that they exist?
- What are the costs, benefits, and risks that accompany each policy option open to the United States?
- What are the trade-offs raised by the potential policy options in this case?

Guide to the Memorandum

All National Security Council (NSC) members except the president will write a position memo before the role-play. You can find more details about writing position memos under Student Resources. The president will write a presidential directive after the role-play. More details about that are also under Student Resources.

What is a memorandum?

- A memo is a formal, succinct written message from one person, department, or organization to another. It is an important form of formal, written communication in the workplace. A memo is generally short, to the point, and free of flowery language and extraneous information. A memo is typically informative or decision-oriented and is formatted in a way that helps readers quickly grasp the main points.
- In the NSC, memos consider, coordinate, and articulate policy options. They help analyze, evaluate, advocate, and channel those policy options and decisions within the bureaucracy.

- Memos also function as historical record. Many memos related to NSC discussions and presidential decisions are filed in government archives. Some are later declassified and released to help people understand how policy was devised at a given time in U.S. history.

Guide to the Role-Play

- There is no right or wrong way to participate in a role-play, but the better prepared you are, the more likely you will be able to advance a position effectively, and the more you and your peers will get out of the experience.
- Be patient during the role-play. Do not hold back from sharing your perspective, but be sure to give others a chance to do the same.
- Where there are competing interests, make the judgment calls that you would make if you were a government official, as informed by your earlier consideration of potential trade-offs. Ensure that the consequences of various decisions are carefully weighed.

Round	Timing	Objectives	Procedural Notes
One:	2 to 3 minutes per participant	1. Present initial positions to the president. 2. Investigate the nuances of the positions through questioning. 3. Clarify the central questions to be debated.	Each participant presents their position statement. If time permits, the president may ask questions to understand each NSC member's position and bring out the essential questions they wish to debate.
Two	30 to 60 minutes	1. Clarify the obstacles, risks, opportunities, and threats. 2. Evaluate the various positions on their merits.	This is the debate portion of the role-play, when participants can defend their recommendations against others' and identify potential areas of compromise agreement.
Three	30 to 60 minutes	1. Narrow the options to a few comprehensive and well- focused strategies that the president prefers. 2. Provide the president with clear recommendations (from NSC members), perhaps as a consensus or through a vote. 3. Arrive at a final presidential decision.	This round should start with the president's stating one to three preferred options to be fleshed out.

Wrap-up

Fuel a lively classroom discussion with simulations that put your students in the shoes of either the National Security Council or the UN Security Council.

CFR Education simulations can be run for several days or weeks and include background readings, videos, and assignments to help students understand the situation and their roles.

Instructions

Role-Play How-To Video

The Debrief

After the debate and deliberation close, the president will announce his or her decision, to be later finalized in the form of a written presidential directive. If time permits, you will participate in a debrief following the president's announcement.

Be active in this debrief. The role-play might seem to be the most challenging part of the experience, but the debrief is equally important. It will reinforce what you learned during the role-play exercise and refine your analytical skills. It will also force you to step out of your role and to view the case from a personal perspective. You will have the opportunity to discuss any

challenges you encountered as you worked through the discussion with your peers and how you felt about the final presidential decision.

The debrief will close with a reflection on the complexities and challenges of crafting foreign policy. This should help clarify your understanding of what you learned and answer any lingering questions. This exercise will also assist you in completing your final assignment, a written reflection.

Reflecting on the Experience

The following questions are proposed to guide the discussion in the in-class debrief. This is not an exhaustive list and may vary depending on how your role-play exercise unfolded. If your class or group does not hold a debrief, these questions will nonetheless help you reflect on the role-play and write your policy review memo:

- Which issues received adequate attention during the role-play? Which, if any, received excessive attention or were left unresolved?
- Did the group consider long-term strategic concerns, or was it able to focus only on the immediate issue and the short-term implications of policy options?
- Which U.S. interests did the group or the president prioritize in the presidential directive and why? Were you comfortable with this prioritization?
- What techniques did you use to convince others that your policy position was the best option? What were successful strategies employed by others?
- What were the most significant challenges to your position? Did any make you rethink or adjust your position?
- Did your points cause anyone else to change their arguments or position?
- What political, economic, and other issues arose that you had not previously considered?
- If you could go back, what would you have done differently in presenting and advocating your point of view?

Written Reflection

The written reflection is your final assignment in the simulation. In the debrief discussion after the role-play, you and your peers went beyond the role you played and thought about the issue from a variety of perspectives. Now that the National Security Council discussion and debrief are behind you, you can consider whether you personally support your recommended policy given the full spectrum of arguments and considerations that arose. Shedding your institutional role and writing from a personal point of view, you will craft a policy review memo that outlines and reflects on the policy options discussed, incorporating and critiquing the president’s decision where appropriate.

If you played the role of president in the simulation, your memo should still reflect your personal opinion. You can comment on the course of action you ordered as president, further justify it, write more extensively on the options you dismissed, or suggest and support alternate options.

No matter which role you played originally, take into account all you have learned. Your instructor or facilitator will want to see whether and how your understanding of the issue and of the policymaking process has evolved from that expressed in your position memo.

More details about the written reflection are available under Student Resources.

Student Resources

Fuel a lively classroom discussion with simulations that put your students in the shoes of either the National Security Council or the UN Security Council.

CFR Education simulations can be run for several days or weeks and include background readings, videos, and assignments to help students understand the situation and their roles.

Instructions How-To Video

Reading List

Essential Resources

- "Cyber Clash with China Case Study," YouTube, 3:41, posted by CFR Education, November 16, 2016.
- Ian Bremmer, "These 5 Facts Explain the Threat of Cyber Warfare," *Time*, June 19, 2015.
- "Cyberspace and Cybersecurity Explained," YouTube video, 7:16, posted by CFR Education, June 18, 2019.
- "Stuxnet Worm: One of the World's First Cyber Attacks," YouTube video, 4:24, posted by CFR Education.
- "China's Maritime Disputes" Council on Foreign Relations.
- "Military Confrontation in the South China Sea," Council on Foreign Relations. May 21, 2020.
- "Destined for War: Can the U.S. and China Escape the Thucydides Trap?," YouTube video, 1:45, posted by The Belfer Center, September 23, 2015.
- "The Colonial Pipeline Incident Shows the Need for Broader Thinking about Cyber Resilience," Council on Foreign Relations, May 20, 2021.
- David E. Sanger, Nicole Perlroth, and Julian E. Barnes, "Biden Plans an Order to Strengthen Cyberdefenses. Will It Be Enough?" *New York Times*, May 9, 2021.
- "Executive Order on Improving the Nation's Cybersecurity," White House. May 12, 2021.
- YOUTUBE PLAYLIST

Additional Resources

- Bruce Schneier, "The Story Behind the Stuxnet Virus," Forbes, October 7, 2010.
- Kathrin Hille, "Chinese Tech Companies Have Army-Linked 'Cybermilitias,'" CNN, October 12, 2011.
- Bonnie S. Glaser, "Armed Clash in the South China Sea," Council on Foreign Relations, April 2012.
- Barack Obama, "Taking the Cyberattack Threat Seriously," *Wall Street Journal*, July 19, 2012.
- Graham Allison, "The Thucydides Trap: Are the U.S. and China Headed for War?" *Atlantic*, September 24, 2015.
- Derek Watkins, "What China Has Been Building in the South China Sea," *New York Times*, last updated February 29, 2016.
- Adrian Chen, "The Agency," *New York Times Magazine*, June 7, 2015.
- Andy Greenberg, "China Tests the Limits of its U.S. Hacking Truce," *Wired*, October 31, 2017.

How to Conduct Research and Use Sources

Research and Preparation

- Draw on the case notes, additional case materials, and your own research to familiarize yourself with
  - the goals of the NSC in general and of this NSC meeting in particular;
  - the U.S. interests at stake in the case and their importance to national security;
  - your role and your department or agency, including its purpose and objectives in the government and on the NSC;

    - the aspects of the case most relevant to your role;
    - the elements that a comprehensive policy proposal on the case should contain; and
    - the major debates or conflicts likely to occur during the role-play. You need not resolve these yourself, of course, but you will want to anticipate them in order to articulate and defend your position in the NSC deliberation.
- Set goals for your research. Know which questions you seek to answer and refer back to the case notes, additional readings, and research leads as needed.
- Make a list of questions that you feel are not fully answered by the given materials. What do you need to research in greater depth? Can your peers help you understand these subjects?
- Using the case materials, additional readings, and discussions with your peers, weigh the relative importance of the U.S. interests at stake in the case. Determine where trade-offs might be required and think through the potential consequences of several different policy options.
- Conduct your research from the perspective of your assigned role, rather than the particular perspective of the person who currently inhabits that office. Make sure to consider the full range of U.S. interests at stake in the case, whether diplomatic, military, economic, environmental, moral, or otherwise. This will help you strengthen your policy position and anticipate and prepare for debates in the role-play.
- Consider what questions or challenges the president or other NSC members might raise regarding the options you propose and have responses ready.

Sources

- Consult a wide range of sources to gain a full perspective on the issues raised in the case and on policy options. Seek out sources that you may not normally use, such as publications from the region(s) under discussion, unclassified and declassified government documents, and specialized policy reports and journals.
- Remember: Wikipedia is not a reliable source, but it can be a reasonable starting point. The citations at the bottom of each entry often contain useful resources.
- Just as policymakers tackle issues that are controversial and subject to multiple interpretations, so will you in your preparation for the writing assignments and role-play. For this reason, evaluate your sources carefully. Always ask yourself:
    - When was the information produced? Is it still relevant and accurate?
    - Who is writing or speaking and why? Does the author or speaker have a particular motivation or affiliation that you should take into account?
    - Where is the information published? Determine the political leanings of journals, magazines, and newspapers by reading several articles published by each one.
    - Who is the intended audience?
    - Does the author provide sufficient evidence for their analysis or opinion? Does the author cite reliable and impartial sources?
    - Does the information appear one-sided? Does it consider multiple points of view?
    - Is the language measured or inflammatory? Do any of the points appear exaggerated?
- Take note of and cite your sources correctly. This is important not just for reasons of academic integrity, but so that you can revisit them as needed.
- Ask your teacher which style they prefer you use when citing sources, such as Modern Language Association (MLA), Chicago Manual of Style, or Associated Press (AP).

How to Write a Position Memo

- The first memo everyone (except the president) writes is called a position memo. It is written from the perspective of your assigned role. It presents a set of policy options for consideration by the NSC and recommends one of them to the president. The recommendation, or position, outlined in this memo is the one you will present during the role-play. (Keep in mind you may change your position as a result of the role-play discussion.)

- The position memo will help your fellow NSC members consider the issue efficiently and facilitate decision-making by the president. Equally important, it will help you clarify your understanding of the case by forcing you to identify the essential facts and viable policy options.
- If you have been assigned a specific role, remember that you are writing from the point of view of the department, agency, or office you represent, and not directly mimicking the policies or opinions of the person currently in that office (unless your instructor says otherwise). If needed, return to your case role description to understand the interests and position of your institution as well as goals of your role. Using the perspective of your institutional position, you will outline a set of options to address the crisis. Make sure you take into account the pros, cons, and ramifications of each policy option as it pertains to your role, institution, and as it is informed by your reading of the case materials and further research. Also, anticipate critiques of your proposed policy and incorporate your response into the memo. Doing so will help you prepare for the role-play.

Note: If you are assigned the role of president, you will not write a position memo. Instead, you will write a two-page presidential directive (PD) at the conclusion of the role-play. You will address the PD, which will follow a memo format, to the NSC members and inform them of your final decision regarding the policy option or options to be implemented (see below).

If your teacher has chosen to assign you the role of general advisor to the president, you will not need to write the position memo from a particular institutional position. Instead, you will have the flexibility to approach the issue from your own perspective, incorporating a comprehensive assessment of the crisis into your argument.

Click here to see a sample of a position memo.

How to Write a Presidential Directive

The format of the presidential directive is simpler than that of a position memo. A directive contains a record of the policy option or options that the president has chosen as well as the accompanying orders to various parts of the government with details on how to carry out these decisions.

- Start with a short paragraph describing the purpose of the memo. Everyone you are writing to was in the NSC meeting, so only brief context is needed.
- Explain in numbered paragraphs the decisions you have made, why you have made them, and any details regarding how you want the decisions carried out.
- Explain the communications strategy for the decision, considering both relevant foreign governments and the public. Also, consider that you may wish to keep certain elements of the decision secret from the public.
- Include any additional details before you sign.
- Be sure to include all the information necessary for NSC members to understand and carry out your intentions.

Click here to see a sample presidential directive.

During the simulated NSC meeting, you will meet to debate and discuss U.S. policy options in response to the issues outlined in the case. Consistent with the NSC's mission to advise the president, you should raise the issues that are most important for the president to consider. This will enable them to make the most informed decision on policy options. Though you may or may not agree with this decision, your responsibility as an NSC member is to provide the best possible analysis and advice

from the perspective of your role.

Role-play Guidelines

1. Stay in your role at all times. (Keep in mind that your role refers to the perspective and duties of the agency or department you represent, and not the specific person currently holding office of the role.)
2. Follow the general protocol for speaking.
    1. Signaling to Speak
        1. The National Security Advisor (NSA) will administer the meeting and should decide on a speaking order. Wait to be called on by the NSA.
        2. If you would like to speak out of turn, signal to the NSA, perhaps by raising a hand or a placard, and wait until the NSA calls on you.
    2. Form of Speech
        1. All NSC members (like the president in the following example) can be addressed as Mr./Madam/Mx. President or simply President [last name]. Before you begin the role-play, share which title you would like to use, and make sure to respect the title your fellow NSC members choose to use as well.
        2. Do not exceed predetermined time limits. If you exceed these limits, the NSA will cut you off.
        3. Frame your comments with a purpose and stay on topic. Remember that you must advise the president so that they can reach a decision on a precise policy question.
    3. Listening
        1. Take notes while others are speaking.
        2. Refrain from whispering or conducting side conversations.
        3. Applause and booing are not appropriate. Your words will be the most effective tool to indicate agreement or disagreement.

How to Write a Written Reflection

Guidelines

- **Subject (one short paragraph):** Offer a brief statement about the significance of the issue as it relates to U.S. foreign policy and national security. Provide just enough information about the crisis so that the reader can understand the purpose and importance of your memo. Be sure to include an initial statement of whether you agree or disagree with the president's decision.
- **Options and analysis (one paragraph per option):** Present and analyze the options discussed during the debate, deliberation, or debrief. Discuss their drawbacks, benefits, and resource needs. Be sure to acknowledge any weaknesses or disadvantages of the proposed options.
- **Recommendation and justification (several paragraphs):** Identify and explain your preferred policy option or options in more detail. Here, you can explain why you personally favor one or more of the recommendations that you initially presented or the president chose, or different options entirely. If you choose to support the options you presented in your position memo, make sure to justify why you feel yours is still the best position.
- **Reflection (one to two paragraphs):** Discuss how your position and the presidential directive are similar; if they are not, discuss how they are different. Use this section to give your thoughts on what the president should have included in their directive, or what you would have done differently. Remember, this is from your point of view; you are no longer advocating on behalf of a department or agency.

Click here to see a full example of a written reflection.

Cyber Clash With China (NSC)

Educator Simulation Guide

Global Literacy

Global literacy is the ability to understand and engage effectively in today's interconnected world. Today's interdependent global economy and geopolitical landscape connect America's interests more than ever to the actions and interests of other countries and their citizens. To ensure students understand this interconnected world, they need to be globally literate. Learn more about global literacy.

Case Overview

Fictional, set in the present day. Cyberspace is a new domain of conflict that has few accepted standards of behavior. Basic questions about it—including how countries should respond to cyberattacks—are still unresolved. In recent years, China has exerted authority over areas of the South China Sea also claimed by other Asian countries, leading to tension with the United States. Last week, following several near misses in the South China Sea between U.S. and Chinese military vessels and aircraft, as well as the theft of documents from U.S. military networks, the U.S. Air Force conducted a flight near a shoal claimed by China. Three days later, the Nasdaq stock market was hacked, which significantly harmed the U.S. economy. U.S. intelligence agencies believe some in the Chinese government knew about the attack, for which a Chinese hacker collective claimed credit. National Security Council members need to advise the president on the merits of a cyber response, economic sanctions, or military measures.

Decision Point

China, Brunei, Malaysia, the Philippines, Taiwan, and Vietnam have competing territorial claims in the South China Sea. In recent years, China has exerted authority over the area by increasing the size of existing islands or creating new ones. China has also constructed ports, military installations, and airstrips. The United States has promoted the right of military vessels to operate in China's claimed two-hundred-mile exclusive economic zone. Furthermore, the United States has rejected China's claim to a twelve-mile territorial zone around the artificial islands it has built. Since 2015, the United States has signaled its opposition by flying military aircraft and sending U.S. Navy ships near certain islands.

Last week, the U.S. Air Force conducted a flight near a shoal claimed by China in the South China Sea. Three days later, the Nasdaq Stock Market suffered a hack that damaged computers and forced the suspension of trading for two days. This imposed significant costs on various U.S. companies and dented confidence in the U.S. financial system. An underground hacker collective based in China known as the Zheng He Squadron has claimed responsibility for the hack. The group has known ties to the People's Liberation Army, China's military. U.S. intelligence agencies assess with 90 percent certainty that the hack occurred with the knowledge or support of parts of the Chinese government. Beijing claims no knowledge of the attack. The president has convened the National Security Council to discuss how the United States should respond.

Learning Goals

CFR Education extended simulations use a variety of pedagogical tools to create an effective, meaningful, and memorable learning experience for students that builds their global literacy. Students will develop crucial skills such as critical thinking, communication, collaboration, and creativity. Students will complete authentic assessments that feel relevant: instead of five-paragraph essays and book reports, students will write policy memos and participate in a role-play of a meeting of a foreign policy–making body. There are no right or wrong answers in actual policy deliberations, and there are none here, either; students will walk away from this experience with an appreciation for the complexity of policy questions.

In this simulation, students will learn about the National Security Council, as well as meeting these learning outcomes specific to this simulation:

- Students will understand that cyberspace is a new domain of conflict with few accepted standards of behavior and continues to be difficult to find agreement around.
- Students will consider the extent to which cyberattacks pose a threat to international peace and security.
- Students will evaluate the costs and benefits associated with options the United States could take in response to a Chinese cyberattack.

Concepts and Issues

Concepts

- Cyberattacks and cybersecurity
- Sovereignty
- Great power rivalry
- Nationalism
- Sanctions

Issues

- U.S.-China relations and China’s emergence as a rising power
- Territorial disputes in the South China Sea
- Definition of standards for behavior in cyberspace
- Military, economic, and other activities in cyberspace
- Information and communications revolution

Policy Options: Educator's Guide

This section presents context, potential benefits and drawbacks, and other information about the policy options outlined in the case that you may find helpful as you guide the role-play and assess students.

The United States has an interest in ensuring that China does not assert its sovereignty claims over the South China Sea by using force or intimidation. Washington has sought to secure this interest through freedom of navigation operations—sending ships or aircraft into areas that China claims but that the United States considers open to all—as well as increased military exercises with its allies in the region. The United States also has an interest in defining the rules of behavior for cyberspace. It has tried to strengthen deterrence by building up offensive capabilities. It has demonstrated its ability to attribute attacks, indicting foreign hackers, and levying sanctions. It has also promoted norms of behavior through bilateral agreements and multilateral forums.

The principal policy options available in this case are discussed below. These responses are available individually, in combination, or all together.

Cyber Responses

The United States could pursue a proportionate response. The United States could try to disrupt critical networks within China, such as its banking system, for a limited period. The attacks could also be directed at a target that seems particularly valuable to the Chinese leadership. These attacks could be focused on the censorship technology that constitutes the so-called Great Firewall. The U.S. response should be accompanied by some level of attribution. This means that the United States would need to identify the attackers, and the attack would reveal some of the United States' technical and intelligence capabilities.

With this option, the United States would essentially be responding in kind. This would keep the U.S.-China dispute in the domain (cyberspace) it is already in rather than extending it. Even if the conflict were to escalate, Washington could claim that it was not the instigator. The United States would likely be capable of mounting a targeted cyberattack that stood a good chance of producing the desired effect.

Nonetheless, a cyber response has costs and risks. A cyberattack could fail if the defender has already patched the vulnerability. Given China's extensive connection with the global economy, malware used against China could also quickly spread to the rest of the world. This could infect U.S. allies and eventually make its way back to the United States. Although limited to one domain, cyberattacks could also escalate rapidly. If attacks damage Chinese defense networks, Beijing could fear that a conventional strike could soon follow. In this scenario, China could decide to launch conventional strikes on U.S. military assets as quickly as possible. Chinese economic retaliation—such as sanctions or tariffs—against the United States is also possible. In addition, other countries could find U.S. claims of China's guilt unconvincing. Failing to convince others that the Chinese government was behind the attacks would not only limit support for the U.S. response but also undermine Washington's efforts to develop international norms for behavior in cyberspace.

Punitive Sanctions

In April 2015, Obama issued an executive order that laid the groundwork for economic sanctions. Declaring a national emergency to deal with the threat of "significant malicious cyber-enabled activities," the order enabled the treasury secretary to sanction individuals and entities involved, directly or indirectly, in cyberattacks. Possible sanctions include freezing suspects' financial assets and barring commercial transactions with them. In the current scenario, the White House could sanction high-level Chinese authorities who it believes ordered the attack and levy economic sanctions on government entities and state-owned enterprises deemed to be connected to the hacks. It could also expel Chinese diplomats from the United States.

Another response would be to indict the individual hackers involved. Although these individuals are unlikely to ever be handed over to U.S. authorities for trial, their international travel would be limited, and the indictments could deter future Chinese hackers who wish to someday travel abroad. Punitive sanctions would involve identifying the attackers and revealing some U.S. technical and intelligence methods.

It could take a while for economic sanctions to be imposed. However, it could take even longer for them to cause enough damage to affect the target's behavior. Chinese firms could also skirt financial restrictions by trading with Russia or others, and China could retaliate against U.S. companies that heavily export to China. The U.S. response could appear weak, undermine deterrence, and embolden other cyberattackers. The United States would need to convince others that the Chinese government was behind the attacks. Otherwise, support for U.S. sanctions would be limited, possibly reducing their effectiveness.

Military Responses

Washington could increase freedom of navigation operations and the U.S. military presence more broadly in the South China Sea. It could help small countries build maritime law enforcement and security capacity and in particular improve the Philippines' long-term maritime capabilities. The United States could also expand military exercises with countries in the region.

Such a response is clear and well within the capability of the U.S. military and would also convey the United States' resolve. Washington could announce that its military initiatives were in response to the Chinese cyberattacks. It could also refrain from doing so. Connecting the response to the attack publicly could be more escalatory. However, it would have the advantage of marking a clear response to the Chinese behavior, ideally leading Beijing to reduce or end this activity. Not making the connection public would be less provocative but could signal to potential attackers that cyberattacks such as the one against Nasdaq fall below the threshold for a forthright response. Regardless of whether the United States announces the connection, military steps could escalate Chinese reclamation behavior in the South China Sea. It could also lead to an incident that escalates into military conflict. Moreover, U.S. support could also embolden the smaller countries to push China harder than they would dare to alone.

Running the Simulation

CFR Education extended simulations are project-based learning activities. Project-based learning (PBL) leads to better learning outcomes and improves skills, and is more fun than traditional instructional methods. The website that students will navigate throughout the simulation is divided into several parts:

In the **NSC Guide**, students will learn about the National Security Council, the body they will be simulating. Included are details on its history, how it works, who its major players are, and more. There is also a video interview with experts who have served on the body.

In the **Case Notes**, students dive into the actual situation they will be trying to solve in their simulation. At the beginning is a clear decision point: the question that students will debate during the role-play. This is followed by detailed background material and a discussion of the role that the United States plays.

Preparation and Role-Play includes details on the various roles students could take on, guidelines for the memorandum they will write (the student playing the role of president has a slightly different task), as well as an outline of how the discussion will flow during the role-play.

The **Wrap-Up** is an important part of the project and includes reflection questions and guidelines for reflecting in a class discussion and in a second memorandum. For historical cases, this section also includes a short description of how the decision point was addressed by policymakers in real life.

The simulation also includes **Student Resources**, which include a reading list to support research, additional directions and exemplars for writing assignments, and other tips students may find helpful.

Once students have read the simulation and prepared their position memos, here is how we recommend structuring the role-play:

Round	Timing	Objectives	Procedural Notes
One	2 to 3 minutes per participant	1. Present initial positions to the president. 2. Investigate the nuances of the positions through questioning. 3. Clarify the central questions to be debated.	Each participant presents their position statement. If time permits, the president may ask questions to understand each NSC member's position and bring out the essential questions they wish to debate.
Two	30 to 60 minutes	1. Clarify the obstacles, risks, opportunities, and threats. 2. Evaluate the various positions on their merits.	This is the debate portion of the role-play, when participants can defend their recommendations against others' and identify potential areas of compromise agreement.
Three	30 to 60 minutes	1. Narrow the options to a few comprehensive and well-focused strategies that the president prefers. 2. Provide the president with clear recommendations (from NSC members), perhaps as a consensus or through a vote. 3. Arrive at a final presidential decision.	This round should start with the president's stating one to three preferred options to be fleshed out.

Tips for the National Security Advisor
In Round 1, call on everyone for their opening statements, keeping to a strict time limit—if students have more to say, they can say it in Round 2. The president doesn't have a specific time limit, but you should keep things moving by not letting the president get bogged down on one issue or policy option.

In Round 2, students do not need to follow a prescribed speaking order; you can call on them as they raise their placards. Work to include everyone and prevent anyone from dominating. As debate goes on, remind students they can change their minds. If it will help move things along, help students see when they are agreeing with each other without realizing it. Feel free to pose questions or propose discussion topics if you feel that certain issues are not receiving adequate consideration. Ultimately, it's up to you to judge when Round 2 has run its course and it is time to move on to Round 3. You will want to move on when all policy options have been discussed and all of the president's questions have been answered. The room does not need to come to a consensus—every option just needs to have a fair airing.

In Round 3, ask students to make a final case for their positions. If, during the course of the discussion, some students seem to have coalesced into blocs, you could ask one student to present on behalf of the bloc. If consensus seems possible, you could work toward it; if not, just make sure each option has been clearly presented to the president. Remember, the NSC is not democratic and is an advisory, not decision-making, body. There is no vote, and the president does not need to choose the most popular option.

Tips for the President
Before Round 1, review all the position memos, if you can. During Round 1, as students are presenting their opening statements, you can ask questions to clarify or help draw out the differences between one policy option and another. Try not to get too deep in the weeds, though—that is what Round 2 will be for.

In Round 2, you can take a more active role. If you have concerns about a policy option, ask questions; if some policy options seem stronger than others, say so. If an element of the issue is not being discussed, raise it.

In Round 3, once you have heard all the policy options, it is all down to you. You should choose whichever policy option you think is best, or combine the strongest elements of several different options. Remember, the NSC is not democratic and is an advisory, not decision-making, body. There is no vote, and you do not need to choose the most popular option. Your decision must be made and announced before the wrap-up discussion, although the written presidential directive can come later.

Tips for Online Classes

We suggest conducting the role-play in three rounds, and that three-round structure is a helpful way to approach chunking the role-play for online learning as well. You can conduct each round synchronously or asynchronously.

In round one, participants present their positions.

- In a synchronous meeting, you can go through opening statements using videoconferencing software, allowing for live clarifying questions.
- However, this is probably the easiest round to conduct asynchronously. You could disseminate positions in writing by having participants share their position memos or write a summary for the purpose of the role-play. You could also have participants record a video of themselves delivering their opening statement and disseminate it for all to watch.

In round two, participants debate the various policy options.

- In a synchronous setting, you can simply run a full-class discussion for round two. If you need more structure or want to prod reticent participants, consider starting by randomly assigning students to breakout rooms, assigning each breakout room one policy option. After working through pros and cons, representatives from each breakout room can share out to kick off the general discussion.
- In an asynchronous setting, consider a discussion forum, with a thread for each policy option. Coach the National Security Advisor and President to be active in the forum, raising questions and responding to points.

In round three, debate begins to coalesce around the policy options that the president favors.

- This round can be approached similarly to round two, but the president should set the topics for breakout rooms or forum threads.

Flashpoints

To add spice or challenge to the role-play, partway through the discussion throw in one of the following flashpoints—additional hypothetical developments that fit within the case's existing decision point—or create your own.

1. In an informal discussion with the U.S. ambassador in Beijing, a senior official at China's Ministry of Foreign Affairs admits believing that hackers linked to the People's Liberation Army (PLA) are indeed responsible for the Nasdaq hack, despite the Chinese government's formal denial. Acknowledging the difficulty for the United States, the official asks the ambassador to urge restraint in any U.S. response. Assertive U.S. action, the official suggests, will only give the PLA license to escalate.
2. Aircraft from the PLA Air Force fire on a Vietnamese military ship in the South China Sea off Vietnam. Several Vietnamese sailors appear to have been killed. PLA leaders claim they were merely defending unarmed Chinese fishing vessels that were being fired on by the Vietnamese ship. Vietnam's government, meanwhile, claims that its ship was trying to prevent illegal fishing in Vietnamese waters and fired only warning shots. Vietnam's foreign minister calls on "all countries concerned, in the Asia-Pacific region and beyond, to work together to contain Chinese aggression in the South China Sea."
3. Three of the largest U.S.-based banks privately inform U.S. government officials that they have detected suspicious activity in their networks. The activity appears to be directed at disrupting international transactions so that more money

than intended is transferred from the U.S. banks to banks overseas. The attacks seem to originate from IP addresses in China, though their true origin remains uncertain. So far, the attacks have not succeeded. However, bank executives tell U.S. Treasury officials that if any vulnerabilities cannot be patched in a matter of hours, they may need to cease international transactions, an action that has massive economic repercussions.

4. Claiming that the feelings of the Chinese people have been hurt by U.S. actions in the South China Sea, large protests break out outside the U.S. embassy in Beijing and U.S. consulates in Chengdu, Guangzhou, Shenyang, Shanghai, and Wuhan. Initially, the protests are orderly: students are bused in from campuses, given placards, and told what to chant. After several hours, unemployed people join the crowd, and protestors throw stones at and start fires outside the consulate in Chengdu. U.S. embassy websites and social media accounts are taken down within China, and access to all foreign websites is temporarily blocked.

After introducing a flashpoint, you might want to help students refocus their discussion by considering critical questions such as these:

1. Who is affected by this event or development, and how?
2. Is there any uncertainty about what has taken place? How credible is the report?
3. Does this event or development affect the feasibility of any policy options? If so, how?
4. Does this event or development affect the desirability of any policy options? If so, how?

Case Assessment

1. What is at stake in the conflicts among China and other Asian countries regarding the South China Sea? What interests does the United States have in the situation?
2. What are the chief characteristics of cyberspace as a domain of conflict? What advantages and disadvantages arise when governments and other entities contemplate using or defending against cyber weapons?
3. What have been the main achievements and shortcomings in the effort to develop rules and norms for how countries should behave in cyberspace?
4. What are the principal motivations underlying Chinese cyber strategy? How has China sought to implement this strategy?
5. How has the United States reacted to Chinese cyber activities? What policy steps has the United States pursued with China in the cyber realm more broadly? What does this history suggest for a policy decision in this case?

NSC Assessment

1. What are the four categories of tools available to U.S. leaders crafting foreign policy, and what is the range of specific tools in each?
2. What is the interagency process and how is it related to the NSC system?
3. What are the various committees in the NSC system and how do they interact to drive U.S. policymaking and implementation?
4. What are the responsibilities of the national security advisor (NSA)?
5. What are the major departments and agencies involved in the U.S. national security and foreign policy–making process? What are their responsibilities?

Each CFR Education extended simulation involves writing assignments that help students think through policy options and reflect on their learning experience.

In NSC cases, there are three types of writing assignments.

- Before the role-play, everyone but the president writes a position memo.
- After the role-play, the president writes a presidential directive.
- As part of the wrap-up, everyone writes a written reflection.

Simulations (on the student-facing side) have instructions for written assignments, and samples for each of these writing exercises. You can also find sample rubrics below.

Samples:

- NSC position memo
- NSC presidential directive
- NSC written reflection

Rubric

Below are sample rubrics for your use in assessing the writing students will do as part of this extended simulation.

These are single-point rubrics. Jennifer Gonzalez, who writes the blog Cult of Pedagogy, has a great explainer, but the bottom line is that single-point rubrics are relatively easy for students to digest but still have all the advantages of giving structure to instructors' feedback.

NSC Position Memo Rubric

CONCERNS	CRITERIA	ADVANCED
What needs improvement	*What is expected*	*What is excellent*
	Subject and Background paragraphs • Briefly explains the significance of the issue in the context of U.S. foreign policy • Clearly identifies the central question • Does not summarize the case	
	Objectives bullet points • Lists several objectives of the department the writer represents • Objectives are grounded in knowledge of the role of the department • Objectives help to shape the analysis of options described in the next section	
	Options and Analysis paragraphs • Lists all options mentioned in the case • Lists other potential options • Analysis considers advantages, disadvantages, and trade-offs	
	Recommendation and Justification paragraphs • Clearly identifies a preferred option or options • Supports the choice with appropriate analysis • Explains why other options are less preferable • Written with the president as the intended audience	

CONCERNS	CRITERIA	ADVANCED
What needs improvement	*What is expected*	*What is excellent*
	Purpose • Provides context for the memo • Is succinct	
	Decisions • Clearly states the decisions made • Explains the decisions convincingly • Details how to implement them	
	Communications strategy • Contains an effective strategy for relevant foreign governments • Contains an effective strategy for the public	

NSC Written Reflection Rubric

CONCERNS	CRITERIA	ADVANCED
What needs improvement	*What is expected*	*What is excellent*
	Subject paragraph • Is brief • Places the issue in the larger context of U.S. foreign policy • Clearly states whether the writer agrees or disagrees with the president's decision	
	Options and Analysis paragraph • Discusses each option that came up during the role-play in discrete paragraphs • Weighs the advantages and disadvantages of each option • If options from the position memo are discussed, those options contain additional analysis	
	Recommendation and Justification paragraph • Makes a clear recommendation based on the writer's personal position • Supports the recommendation effectively	
	Reflection paragraph or paragraphs • Reflects on and critiques the president's decision • Is written from a personal point of view, not that of the assigned role	

Downloadable rubrics are available here:

- NSC position memo
- NSC presidential directive
- NSC written reflection