Cyber Clash with China

https://modeldiplomacy.cfr.org/#/simulations/20181/

Exercise to practice:

1. Collaboration
2. Critical thinking - disciplined thinking that is clear, rational, open-minded, skeptical, and unbiased analysis or evaluation of factual evidence (Dictionary.com Unabridged).
3. Writing
4. Oral Communication

GENERAL ADVISOR TO THE PRESIDENT

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

the attack. You will consider three types of responses, alone or together:

1, cyber responses, such as disrupting Chinese networks in a manner proportionate to the hack against the Nasdaq;

2. economic sanctions on Chinese government entities and state-owned enterprises connected to the recent hacks; and military responses, such as increased freedom of navigation operations and

3. a larger U.S. military presence more broadly in the South China Sea.

Tasks:

1. Develop a position memorandum of your recommendations to the President on what he should do in this situation.

2. Prepare and deliver an oral briefing to the President on the contents of your position memorandum.

The Issue

Cyberspace is a new domain of conflict, one with few accepted rules or standards of behavior.

example, explicitly recognizes offensive missions, directing the Pentagon to develop cyber capabilities that can support military operations. Although it is

Decision Point

China, Taiwan, Vietnam, Malaysia, Brunei, and the Philippines have competing territorial and jurisdictional 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 islands, as well as by constructing 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 and has rejected China's claim to a twelve-mile territorial zone around the artificial islands China has built. Since 2015, the United States has signaled its opposition by flying military aircraft and sending U.S. naval ships near some islands.

Over the past several weeks, there have been several near misses in the South China Sea involving U.S. and Chinese military vessels and aircraft. So-called patriotic hackers—individuals who act out of nationalist pride or anger—in China and the United States have defaced websites in both countries. The Pentagon recently announced that its website had been breached, and in the last two months China-based hackers have stolen a trove of electronic documents from U.S. military networks, including information about an upcoming joint exercise with the Philippine Navy.

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, imposing significant costs on various U.S. companies and denting confidence in the U.S. economy. The Zheng He Squadron, an underground hacker collective based in China, has taken credit for the hack. The group has known ties to the People's Liberation Army (PLA), 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, however, claims that it has no knowledge of the attack and warns Washington that "irresponsible, unscientific" attempts at attribution are a distraction from the United States' own hacking and will heighten mistrust between the two countries.

Fact Sheet: The Department of Defense (DOD) Cyber Strategy

Why Is the South China Sea Contentious?

The Context

The United States and China have significant disagreements over cyber espionage, cyberattacks, and internet governance. These differences have intensified in recent years as cyber issues have become more significant on the bilateral and global agenda.

In late 2009 or early 2010, Iran replaced about one thousand of the nine thousand centrifuges deployed at its fuel enrichment plant at Natanz. The centrifuges had been damaged by sophisticated malware, eventu ID i (l)-2 .0 Tc 0 2 72 693.TfCID 10 >>BDC /TT2 1 Tf 12 -n

damaged two-thirds of the company’s servers and computers. On December 19, 2014, the FBI

responsible for and should act against cyberattacks that originate within their territories. In 2015, the same group agreed to a set of peacetime norms promoted by the United States. These norms include the idea that states should not attack each other's critical infrastructure or target each other's computer emergency response teams—national agencies that defend against and help recover from cyberattacks. The norms also hold that countries should assist other nations investigating cyberattacks and cybercrime. However, the 2017 round of negotiations ended with the participants unable to identify new norms or agree whether international law applied to cyberspace.

Additional Reading

The Inside Story of the Biggest Hack in History

U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict

Iran Learns From U.S. Cyberattacks

Recent History

Chinese cyberattacks in particular are often driven by the desire to collect political and military intelligence. According to a Washington Post report, Chinese hackers have stolen information relating to over two dozen U.S. weapons programs, including the Patriot missile system, the F-35 Joint Strike Fighter, and the U.S. Navy's new littoral combat ship. The State Department, the

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 and establish two high-level working groups and a hotline between the two sides.

Following the September summit between the two presidents, the cybersecurity firm FireEye reported a sharp decline in the number of Chinese cyberattacks, though it also suggested that actors might have become stealthier and more difficult to detect. U.S. Assistant Attorney General John Carlin confirmed the company's findings that attacks were less voluminous but more focused and calculated.

The US-China group on security issues only met once before the end of the Obama administration, but the cyber crime group reported some small progress. The two sides established a point of contact and a designated email address, and successfully cooperated on taking down fake websites. After President Trump met President Xi at Mar-a-Lago in April 2017, the Washington and Beijing agreed to a United States-China Comprehensive Dialogue that will have four pillars, including one on law enforcement and cybersecurity.

We know that foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity, and water plants, and those that guide transportation throughout this country.

— Leon Panetta, then U.S. Secretary of Defense, October 12, 2012

Other Interested Parties

Other Asian countries: The countries involved in maritimoug (m)8 (a)

claims to territorial rights over a large expanse of the South China Sea. The court also "found that China had violated the Philippines' sovereign rights" by building artificial islands and meddling in fishing and oil exploration. China had previously stated that it would "neither accept nor participate in the arbitration unilaterally initiated by the Philippines," and rejected the ruling.

U.S. Allies: The European Union has expressed support for U.S. freedom of navigation operations in the South China Sea, as well as a vision of the internet that is global, open, and secure. The United Kingdom, Germany, and the Netherlands have been particularly vocal proponents of devel

Guide to the Memorandum

A major goal is to strengthen your ability to write concise, articulate, and persuasive documents that busy colleagues can quickly absorb. You will write a position memorandum. This will improve your writing skills and give you a taste of how U.S. foreign policy is conceived, coordinated, and executed.

What is a memorandum?

- A memo is a succinct written message from one person, department, or organization to another. It is an important means of formal, written communication in the workplace. Business, government, law, and many other disciplines will prefer that you be proficient in memo-style writing. 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.
- The NSC's role is to advise the president by generating and weighing policy options and overseeing the implementation of the president's policy decisions. The proposed options and recommendations need to be considered, coordinated, and articulated through some form of written communication. Memos do exactly that: they help analyze, evaluate, advocate, and channel policy options and decisions within the government bureaucracy.
- Memos also serve as a historical record. Many memos related to NSC discussions and presidential decisions are filed in the government's archives. Some are later declassified and released for future generations to understand how policy was devised at a given time in U.S. history. You can access historical examples of memos by searching online. One such resource is maintained by the Federation of American Scientists and offers links to memoranda and directives issued by various U.S. presidents.

Position Memo

- The memo you will write is called a position memo. This memo is written from the perspective of your assigned role. In about two single-spaced pages, it presents a set of policy options for consideration by the NSC and recommends one of them to the president.
- The position memo should provide brief background on the issue at hand; outline the

the Attorney General

the National Security Advisor

the Director of Central Intelligence

the Chairman of the Joint Chiefs of Staff

SUBJECT: Options for a U.S. response to Soviet missiles in Cuba

This memo outlines options for U.S. action against Soviet missile installations in Cuba. On October 14, an American U-2 plane photographed Soviet construction of medium-range ballistic missile (MRBM) sites in Cuba, some of which contain missiles that could be launched within eighteen hours. Failure to swiftly eliminate this threat would encourage Soviet aggression and increase the risk of a nuclear attack on the United States.

BACKGROUND: U-2 reconnaissance has provided evidence of offensive Soviet military activity in Cuba, including the presence of MiG fighter jets, IL-28 bombers, and sites for SS-4 and SS-5 missiles with ranges between 1,000 and 2,200 nautical miles. These distances encompass Washington and other major U.S. cities. U.S. intelligence services estimate that the MRBMs will be ready to launch in eighteen hours and that the longer range SS-5 missile sites could be operational in December.

OBJECclS <</bq -1(l)-2 (e)le- os thre Sorsll iuss. T2</bq -1MC /P <</MC presutreep (e)a(n)1 (e)bco

2. Order air strikes against missile sites in Cuba.

   The United States could carry out air strikes against missile sites in Cuba. These could entail surgical strikes targeting only MRBM sites or broader strikes that would also target other Soviet military assets, including IL-28 bombers, MiG jets, patrol boats, tanks, and airfields. Broader air strikes would eliminate missile sites and limit Soviet capability to retaliate against U.S. forces and U.S. bases in Florida. However, no air strikes guarantee 100 percent elimination of the missiles, making several rounds necessary. Moreover, sustained military action carries a relatively high risk of Soviet retaliation and the capture or death of U.S. pilots. This could set off a chain of events that necessitates a U.S. invasion of Cuba. Such an invasion, involving as many as 250,000 U.S. troops, could begin within seven days of air strikes. Though an invasion would be the most direct means of eliminating the threat in Cuba, it would also be the most costly.

RECOMMENDATIONS AND JUSTIFICATIONS:

This agency's first priority is to eliminate the missile threat from Cuba. To do so, it recommends that the president implement a naval quarantine on offensive military equipment headed to that island. The quarantine is a measured response that will inhibit Soviet plans in Cuba with significantly lower risk of casualties and escalation than air strikes. Moreover, if accompanied by

Critical Analysis

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 some notable uses of cyber weapons by governments or other actors against either government or private targets? What has their impact been? What lessons, if any, can be drawn from this history for this case?
5. What are the principal motivations underlying Chinese cyber strategy? How has China sought to implement this strategy?
6. 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?
7. What are the root causes of the conflict presented in this case?
8. What options are available to the United States in this case? What are the potential benefits and drawbacks of each option?
9. What other parties are interested in this case? How do their interests intersect with those of the United States? What do these parties and intersecting interests suggest for a U.S. policy decision?
10. What are the goals of a U.S. policy decision in this case? How do these goals align or conflict with each other? What trade-offs might you be willing to make to pursue them?