# 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 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.

The president needs to decide, after receiving advice from, how the United States will react to 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. After years of official silence, the U.S. government has gradually become more transparent about its development and use of cyberattacks. The 2015 Defense Department cyber strategy, for example, explicitly recognizes offensive missions, directing the Pentagon to develop cyber capabilities that can support military operations. Although it is widely believed that the United States and Israel were behind Stuxnet, the malicious software (malware) designed to slow Iran's nuclear program by damaging centrifuges at the Natanz nuclear facility in 2009, the United States did not admit any role. Instead, the first public acknowledgment of the United States' use of cyber weapons came in February 2016 when Pentagon officials announced that U.S. Cyber Command had launched attacks against the self-proclaimed Islamic State, also known as ISIS. U.S. Cyber Command has grown from approximately nine hundred personnel to more than six thousand, and total requests for cyber operations in the 2017 defense budget were $6.7 billion, an increase of more than 15 percent from 2016.

Offensive cyber operations are an attractive tool for policymakers because they are relatively inexpensive, may be less destructive than kinetic strikes (i.e., those against physical targets), and may provide a high degree of anonymity to the attacker. The vast majority of attacks are cyber espionage (theft of military and political secrets or intellectual property) and political disruptions (website defacement or distributed denial of service [DDoS] attacks that flood a website with so much data that it can no longer respond). The White House's 2011 International Strategy for Cyberspace warns that the "United States will respond to hostile acts in cyberspace as we would to any other threat to our country." However, although it is widely assumed that a cyberattack that caused death or physical destruction would be considered an armed attack, the threshold for a military response to other forms of cyberattacks remains uncertain.

Indeed, cyberspace is an environment of high strategic instability. 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, but an attacker needs to find only one vulnerability. Attribution of cyberattacks is difficult and slow, which makes them vastly different from other weapons. Attackers can hide their tracks, routing attacks through multiple computers in numerous countries, and the attacks can happen in minutes, if not seconds. Many countries rely on proxies, criminal groups, or patriotic hackers to conduct operations. Thus, even if hackers are located within a state, it may remain unclear who authorized an attack. This can greatly complicate efforts to retaliate and prevent further attacks.

Yet uncertainty about the efficacy and advisability of cyberattacks is considerable. Attacks may spread from the target networks to those of uninvolved third parties. Determining the effects of an attack requires analysis and interpretation of an event at multiple targets. Defenders can respond quickly to successful attacks, patching software and changing network configurations, so cyber weapons are likely to be "one and done."

Moreover, successful attacks are likely to risk escalation. To weaken the enemy's ability to fight, attackers will take out the computers that control opposing forces. Such attacks impair enemy leaders, limiting their ability to order forces in the field to pull back or cease combat. If commanders believe they will lose the use of important weapon systems early on in a conflict, they have an incentive to use them preemptively, further destabilizing the situation.

**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.

# More To Watch

## Study: China Flirts With War in South China Sea

Right now, we've got about three billion people online, and they are using anywhere from five to fifteen million devices. And all of these devices are connected and all those connections represent doors … Most of these devices have vulnerabilities in them, and so that creates backdoors, and somebody's going to find them.

— Dorothy E. Denning, distinguished professor at the Naval Postgraduate School, October 9, 2015

# Additional Reading

## These 5 Facts Explain the Threat of Cyber Warfare

**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, eventually known as Stuxnet, which was allegedly developed and launched by the United States and Israel to slow down Iran's nuclear program. The Natanz plant seriously concerned these two countries because its centrifuges were producing enriched uranium, which can, if properly processed, be used in a nuclear weapon. Sometime in the summer of 2010, Stuxnet escaped into the wild, eventually spreading to more than 115 countries, though it did no damage to other systems. The United States also reportedly developed a cyberattack plan, code-named Nitro Zeus, to be used if negotiations failed to limit Tehran's nuclear program and military conflict erupted. U.S. Cyber Command reportedly planned attacks on air defenses, communications, and parts of the power grid. The United States, Iran, and other powers reached a deal over Iran's nuclear program in 2015, and the apparent cyberattack plan has never been used.

After Stuxnet was discovered, Iran retaliated with its own cyberattacks. Between September 2012 and June 2013, an activist group called Izz ad-Din al-Qassam Cyber Fighters took credit for roughly two hundred distributed denial of service (DDoS) attacks on almost fifty Western financial institutions, including SunTrust, JPMorgan Chase, CitiGroup, Wells Fargo, U.S. Bancorp, Capital One, PNC, and HSBC. These attacks made websites unavailable for a few hours but did not threaten the integrity of the financial system.

In August 2012, the Shamoon malware struck Saudi Aramco, Saudi Arabia's state-owned oil company, which supplies about a tenth of the world's oil. Shamoon corrupted tens of thousands of hard drives and shut down the employee email service. The company had to replace thirty thousand computers but the malware did not affect systems involved with technical oil operations. A subsequent attack damaged RasGas, a joint venture between Qatar Petroleum and ExxonMobil. Data was destroyed but production continued. A group calling itself the Cutting Sword of Justice claimed responsibility, but in this case, as in the earlier financial attacks, U.S. officials speaking off the record blamed the Iranian government. Saudi Arabia, predominantly Sunni, and Iran, predominantly Shiite, often compete for influence and leadership in the Middle East.

During Thanksgiving week in 2014, employees of Sony Pictures lost access to the company's computer networks and their email accounts due to a massive hack. The hackers, operating under the name Guardians of Peace, not only stole one hundred terabytes of internal data but also damaged two-thirds of the company's servers and computers. On December 19, 2014, the FBI announced that the Guardians of Peace were North Korean government hackers. Pyongyang had previously expressed outrage over the Sony film The Interview, which depicts the assassination of its supreme leader, Kim Jong-un. This was the first time the U.S. government had explicitly and directly named another government as responsible for hacking.

On January 2, 2015, the United States levied economic sanctions on the Reconnaissance General Bureau, a North Korean intelligence agency; the Korea Tangun Trading Corporation, which acquires military-related materials and technology for North Korea; and the Korea Mining Development Trading Corporation, the country's main exporter of ballistic missiles and conventional weapons. The United States also reportedly asked the Chinese government for help with identifying and controlling North Korean hackers, some of whom were reportedly based in a hotel in northeastern China, but public statements from Beijing were noncommittal. Around this time, North Korea (formally the Democratic People's Republic of Korea, or DPRK) disappeared from the internet. The few DPRK websites available to the outside world were knocked offline by a DDoS attack. Despite some suspicion that the U.S. government was responsible, the attack was more likely conducted by individual hackers or a group of activists.

In March 2016, the United States indicted seven Iranians working for entities affiliated with the Islamic Revolutionary Guard Corps for conducting cyberattacks in 2012 and 2013 against the U.S. financial sector, and also charged one of them with unauthorized access to the control systems of a New York dam. The United States also announced that Cyber Command was engaged in offensive operations against the Islamic State. According to the *New York Times*, U.S. military hackers first placed "implants" in the militants' networks to learn about commanders, then began to alter messages to make fighters more vulnerable to attack by U.S. drones. In other cases, Cyber Command disrupted the Islamic State's financial transactions.

The 2016 U.S. presidential election was marked by repeated hacking incidents. In July, thousands of emails from the Democratic National Committee (DNC) were leaked and subsequently published by Wikileaks. The fallout was significant, leading to the resignations of DNC chairwoman Debbie Wasserman Schultz, representative from Florida, and many top party aides. In the fall of 2016, thousands of emails from the personal Gmail account of John Podesta, the chairman of Hillary Clinton's presidential campaign, were also released. Researchers concluded that hackers linked to Russian intelligence were behind both the DNC and the Podesta hacks. The U.S. government also denounced the incidents as Russian-directed hacking, accusing Russia of attempting to interfere in U.S. elections. In December 2016, the White House announced that it was expelling thirty-five Russian spies from the United States and sanctioning nine individuals and organizations linked to the hacking: the FSB and GRU, four intelligence officers, and three companies that provided material support to the hackers.

Since 2005, a small group of governmental experts has gathered at the United Nations (UN) to discuss cyber threats. The group, which includes government representatives from China, Russia, and the United States, signed a nonbinding report in 2013 agreeing that international law applies in cyberspace. This means, among other things, that cyberattacks can be considered a use of force, that a state can exercise the right to self-defense if it is the victim of a cyberattack, and that the laws of armed conflict apply to cyberwar. The 2013 report also asserted that states are 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 White House, the Office of Personnel Management, and NASA have been breached. China's cyber espionage, however, has not been limited to U.S. targets. Embassies, foreign ministries, and the government offices of India, South Korea, Indonesia, Romania, Taiwan, and Germany, among others, have also been breached.

Cyberattacks are also motivated by the need to move Chinese industries out of labor-intensive, energy-inefficient, highly polluting manufacturing sectors to cleaner, more technology-intensive ones. The Chinese fear being caught in a technology trap, dependent on U.S., Japanese, and European firms for core technologies. Cyberattacks are intended to acquire information that could help Chinese firms develop such technologies themselves. Attacks on Google, Yahoo, Adobe, Symantec, Juniper Networks, Disney, Sony, Johnson & Johnson, General Electric, General Dynamics, and DuPont have been publicly reported. Chinese hackers have also reportedly targeted the negotiation strategies and financial information of 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, with the majority of attacks originating from IP (Internet Protocol) addresses in Japan, the United States, and South Korea (formally the Republic of Korea). The Chinese press was quick to echo claims by the National Security Agency (NSA) contractor Edward Snowden that the United States hacks targets on the Chinese mainland and in Hong Kong.

Chinese cyber strategy has a military dimension as well. PLA analysts write frequently of seizing information dominance early on in a conflict by conducting cyberattacks on an enemy's command and control centers. These centers allow commanders to collect information, issue orders, and monitor operations. Follow-up attacks would target transportation, communication, and logistics networks to slow down an adversary. To prepare for this strategy in any potential conflict with the United States, Chinese actors appear to be surveilling and entering military networks as well as some critical U.S. infrastructure, such as power grids and oil and gas pipelines. U.S. military doctrine—in particular the Air-Sea Battle doctrine (now known as Joint Concept for Access and Maneuver in the Global Commons), adopted to defeat cruise missiles, submarines, and cyber capabilities—also assumes cyberattacks on an adversary's sensors, networks, launchers, and weapons in the beginning stages of a conflict.

As with economic policy and national security, Chinese President Xi Jinping has consolidated control over cybersecurity by creating a so-called small leading group, an ad hoc body that advises the Politburo and implements decisions. Moreover, on December 31, 2015, China's Central Military Commission overhauled the organizational structure of the PLA, establishing three new branches. One of them is the Strategic Support Force, whose operations remain unclear but whose responsibilities will reportedly include intelligence, technical reconnaissance, electronic warfare, cyber offense and defense, and psychological warfare.

Beginning in 2013, Washington publicly increased pressure on Beijing over cyber espionage. In March 2013, for example, National Security Advisor Tom Donilon spoke of the "serious concerns about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale." Two months later, the Defense Department went further, and, in a break from the past, directly blamed the Chinese government and military for espionage.

In May 2014, the Department of Justice charged five Chinese hackers with stealing the business plans, internal deliberations, and other intellectual property of Westinghouse Electric, United States Steel Corporation, and other companies. The department claimed the hackers were members of the PLA's General Staff, Third Department, Unit 61398, located in Shanghai. The indictment incensed the Chinese government, which quickly suspended a high-level bilateral cyber working group.

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," allowing 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 from the companies that benefit from the hacks from traveling to the United States. After departing the United States, Xi signed similar agreements with the UK and at the G20 meeting in Turkey.

In August 2015, the *Washington Post* reported that the Obama administration planned to levy these sanctions against Chinese companies in the lead up to the summit the next month between Presidents Obama and Xi. Perhaps because of the threat, the summit produced a breakthrough agreement. Both sides pledged 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 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 maritime disputes with China—Japan, Malaysia, Taiwan, Vietnam, Brunei, and the Philippines—all have an interest in how this dispute and the broader issue of cyber behavior are managed or resolved. Japan, Vietnam, Taiwan, and the Philippines have also been the targets of Chinese cyber espionage campaigns as well as DDoS attacks and website defacements.

In 2002, China and the Association of Southeast Asian Nations (ASEAN) signed a Declaration on the Conduct of Parties in the South China Sea. The agreement called on all claimants not to resort "to the threat or use of force" in pursuing their objectives in the area, and to work on a code of conduct. ASEAN ministers tried to reinvigorate the code in 2012, but little progress has been made. No code of conduct has emerged. ASEAN has struggled to find a coherent diplomatic position that supports the four members (Brunei, Malaysia, the Philippines, and Vietnam) who have disputes with China, some of which are more willing to compromise than others, given the reality that China is the largest trading partner of many ASEAN states. ASEAN has also been active in trying to develop confidence-building measures for cyberspace, holding a number of regional and bilateral (ASEAN-China and ASEAN-Japan) conferences on cyber norms. Acting individually, the Philippines in 2013 brought a claim against China over the sovereignty of the Spratly Islands to the Permanent Court of Arbitration (PCA), a tribunal in The Hague. In July 2016, the court ruled unanimously in the Philippines' favor, dismissing China's 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 developing norms of state behavior in cyberspace. In 2011, the U.S.-Australia alliance was extended to cover cyberattacks and, in the summer of 2014, NATO declared that cyber defense was part of alliance's "core task of collective defense." Depending on the severity of the attack, both treaties could create a mutual defense obligation for cyberattacks.

**U.S. Competitors**: Russia, North Korea, and Iran will take a keen interest in Washington's response to this case given that they have all reportedly launched attacks on the United States and may do so again in the future. In addition, Moscow and Beijing signed a cybersecurity pact in May 2015 in which they stated they would not conduct cyberattacks on each other but would exchange technology and information on threats.

**United Nations**: The UN has also been increasingly focused on cybersecurity and international peace. In September 2011, Russia, China, Tajikistan, and Uzbekistan collectively proposed an international code of conduct for information security to be considered by the UN General Assembly, and have reintroduced it in subsequent years. It is also the basis of an agreement on cybersecurity adopted by the Shanghai Cooperation Organization, a regional organization that includes China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan (and India and Pakistan by 2016). In 2013, a group of governmental experts at the UN agreed in a report that international law, and the UN Charter in particular, applies in cyberspace. In 2015, the same group, which includes representatives of China, Russia, and the United States, agreed to a set of peacetime norms, including that states should not attack each other's critical infrastructure.

# 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 United States' strategic objectives; present and analyze several policy options; and, finally, recommend and justify a particular course of action. Although conveying complex ideas in a concise way can be challenging, it 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.
- Make sure to take into account the pros, cons, and ramifications of each option as it pertains to your role, and as 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.

- The position memo below gives you a sample template to follow as you write your own memo. When reviewing the sample memo, pay attention to how they are structured, how much information they include, and how they advance their analysis and argument.

**Position Memo Template**

- **Subject and Background (two short paragraphs):** Briefly summarize the significance of the issue for U.S. foreign policy and national security and identify the central policy question(s) to be decided. Provide just enough information about the crisis so the reader can understand your memo's purpose and importance. Do not summarize the case in depth since your readers are already well-informed.
- **Objectives (bullet points):** Succinctly state your department's objectives in the current crisis. These can be general national security objectives (such as preventing war), or more specific goals tied to your department's mission (such as protecting U.S. citizens). They should be important to U.S. national security, directly tied to the case, and feasible. These objectives should guide the policy analysis and recommendation that make up the rest of your memo. This section requires exceptional clarity of thought.
- **Options and Analysis (one paragraph for each option):** Present and analyze several options for U.S. policy. Discuss their costs, benefits, and resource needs where possible. Be sure to acknowledge the weaknesses or disadvantages of each proposed option in order to illuminate the trade-offs inherent in complex policy decisions. No option is likely to be perfect.
- **Recommendation and Justification (several paragraphs):** Identify your preferred policy option(s) and provide more details about it or them. Explain your reasoning, keeping in mind that you aim to convince the president that he or she should follow your recommendation. Addressing the weaknesses or disadvantages you identified in the Options and Analysis section can help strengthen your argument.

## SAMPLE POSITION MEMO

Office of the Secretary of Defense

Washington, DC

October 19, 1962

TOP SECRET

MEMORANDUM FOR: the President

the Vice President

the Secretary of State

the Secretary of the Treasury

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.

OBJECTIVES:

This agency has two principal objectives in this matter:

- eliminate the missiles located in Cuba
- avoid nuclear war with the Soviet Union

OPTIONS AND ANALYSIS:

In order to accomplish the aforementioned objectives, this agency proposes two options:

1. Implement a naval quarantine around Cuba.

   The United States could implement a naval quarantine on offensive military equipment bound to Cuba, thwarting the further growth and development of missile sites. A quarantine is a limited military response that takes direct action while reducing the risk of significant casualties, and it leaves room for additional U.S. action in the future. It would not, however, eliminate missiles already in Cuba, nor would it halt construction or operationalization of existing sites with equipment already delivered. It also risks escalation of the conflict due to miscommunication between ships or unpredictable Soviet behavior. To that end, if the president orders a quarantine, he should ask Chairman Khrushchev to preemptively stop Soviet ships en route to Cuba.

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 dialogue with the Soviet Union, a quarantine could effectively lead to Moscow's removal of the missiles. The United States should seek approval of the quarantine from the Organization of American States in order to lend it further diplomatic weight.

Operationally, the U.S. Navy would establish a quarantine line and signal ships approaching it to stop for boarding and inspection. As a first warning, a nonresponsive ship would receive a shot across the bow, and as a second warning, a shot fired into the rudder to stop the vessel. Any ship determined to be delivering offensive weapons to Cuba, regardless of port of origin, would be turned back.

Although this agency prefers a quarantine, it recommends simultaneously preparing for air strikes and invasion in case such measures become necessary to eliminate the missile threat. The United States should reinforce its naval base at Guantanamo Bay, raise military alert levels, and take steps to protect U.S. shipping interests in the Florida Strait. The Joint Chiefs of Staff have separately identified such preparatory measures.

As part of any response, this agency supports continuing reconnaissance missions over Cuba and strengthening air defenses in the southeastern United States. Finally, the United States should advise the Soviet Union that any attack from Cuba will be seen as an attack from the Soviet Union itself and will prompt a commensurate U.S. response.

# 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?