The Road to Crisis

During a press conference in mid-December 2021, President Biden announced plans to provide Taiwan with additional Patriot air defense systems, two-dozen new F-16 fighter jets, eight surplus P-3 maritime patrol aircraft, and five naval destroyers equipped with Aegis Combat Systems. Biden explained that the arms deal—one of the largest in Taiwan's history—was intended to bolster Taiwan's ability to defend itself and its democratic way of life. In response to questions from reporters, President Biden also reiterated a pledge that he had made in October: "If China attacks Taiwan, the United States will take steps to defend Taiwan."

That evening, China's Foreign Minister Wang Yi issued an official statement criticizing the arms deal and accused the United States of "meddling in regional affairs" and "dangerously and unnecessarily escalating tensions."

In the days following Biden's press conference, the People's Liberation Army (PLA) significantly increased military flights through Taiwan's Air Defense Identification Zone. In a 72-hour period from December 20-December 23, the PLA Air Force (PLAAF) and PLA Navy (PLAN) flew more than 180 aircraft in the airspace surrounding Taiwan. Taiwan's government responded by scrambling fighter jets to intercept many of these PLAAF and PLAN aircraft.

On December 24, a PLAAF Su-27 fighter jet collided with a Taiwan Air Force F-16 fighter jet, leading to the deaths of both pilots. The domestic public in China takes to the streets demanding harsh action against Taiwan to avenge the death of the PLAAF pilot.

President Biden and Secretary of State Blinken urge calm, but also warn China—both privately and publicly—to not attempt to forcefully change the status of Taiwan.

On December 25, Christmas celebrations in the Taiwanese cities of Taipei and Kaoshiung are interrupted by extensive blackouts. More than a million people are left without power, and 279 Taiwanese citizens die as a result of the power outages (e.g., life support failures, etc.).

Recorded Futures, the Somerville, Massachusetts-based company that identified the Chinese malware behind power outages that plagued Indian cities during the Sino-Indian conflict of 2020, make a similar discovery in this case: the Taiwan backouts are almost certainly triggered by Chinese malware. The discovery was made possible by advances in machine learning that allowed Recorded Futures to find common patterns between the timings of sequential cyber-intrusion attacks in India and Taiwan. Recorded Futures identified a record of attempts to connect to the same infrastructure registered to Tsinghua University that was implicated in the Indian outages. In the China-India incident, analysts believed China was signaling its ability to cause significant damage if India escalated the border conflict. The U.S. intelligence community has yet to confirm that the blackout is the result of a Chinese cyberattack, and some AI/ML scholars have raised doubts about the accuracy of the Recorded Futures machine learning algorithms.

President Biden schedules an emergency National Security Council Principals Committee meeting for this afternoon. You've been called into the office to help your organization prepare for this meeting. You open your email to find President Biden's <u>strategic objectives for dealing with the crisis:</u>

1. Maintain status quo (i.e., no change to the status of Taiwan).
2. Protect U.S. citizens and interests in the People's Republic of China (PRC) and Taiwan.
3. Prevent further escalation between the PRC and Taiwan.
4. Should the PRC and Taiwan escalate, minimize direct U.S. combat involvement in conflict.

Move 1:
December 26, 2021
(30 minutes followed by 15 minute "report back")

As the death toll in Taipei and Kaoshiung continues to climb, your teams begin formulating the initial U.S. response. The FBI and NSA also reports increased evidence of Chinese intelligence collection in the United States. Specifically, Chinese "consular" officials have been started taking photos of U.S. military and port facilities in Hawaii, Alaska, California, and Washington, and there have been increased phishing attempts against senior U.S. military officers.

The list below includes tasks for each team.

Department of State:

- What actions, if any, should the United States take to protect American citizens and interests in China/Taiwan?
- What coordination, if any, should the United States take with allies and partners within the Asia-Pacific region and beyond?
- Prepare talking points for the Secretary of State that he can use to offer brief comments on the situation if asked by reporters. Ensure these are aligned with the whole of government position.

Department of Defense:

- What military measures, if any, should the United States take at this point? These measures could include mobilization/deployment of forces, kinetic/non-kinetic action, etc.
- Prepare talking points for the Secretary of Defense and Chairman of the Joint Chiefs that they can use to offer brief comments on the situation if asked by reporters. Ensure these are aligned with the whole of government position.

Office of the Director of National Intelligence:

- What additional information does your team (and the other Executive Branch agencies) need?
- How will you obtain this information (i.e., which intelligence disciplines are best suited to collect this)?

Department of Homeland Security:

- What steps should the United States take to protect the U.S. homeland from kinetic and non-kinetic attacks?

Department of Justice:

- What actions should the Department of Justice take to mitigate the risk of espionage against the United States during this period of heightened tensions? Which organizations will DOJ need to coordinate with?

When formulating your recommendations, ensure you respond to the defined tasks/questions and ensure your recommendations are in line with President Biden's objections. You are encouraged to coordinate with the other Executive branch agencies when developing your response.

Move 2:
December 28, 2021
(35 minutes followed by 15 minute "report back")

On December 27th, Taiwan's President Tsai Ing-Wen declares a state of emergency in Taipei and Kaoshiung, where power still remains out. She also orders a limited mobilization of Taiwan's reserve forces (including 3000 infantry personnel) and puts 40 civilian fishing vessels and 8 civilian Boeing airliners from China Airlines under the operational control of the Ministry of Defense. Tsai publicly states these measures are to "support humanitarian relief operations," but also makes a secret call to President Biden in which she expresses fear that China may attempt to use military force to seize Taiwan in the coming weeks.

Although large numbers of PLA ground, naval, and air forces continue to flow into China's Eastern Theater Command, U.S. intelligence has no specific indication of an impending attack. China's defense minister, however, issues the warning that "outside nations should not meddle in China's internal affairs. Unnecessary meddling will risk a significant heightening of tensions."

In the early morning hours of December 28th, Guam—a U.S. territory that is home to Anderson Air Force Base and several key U.S. naval facilities—suffers a significant cyberattack that significantly degrades operations at Anderson and kills 3 Americans at Guam Medical Center in the city of Tamuning. Intelligence assessments suggest with high confidence that China's military is behind the data breach and cyberattack on Guam

At the same time, ransomware locks down systems at sea and airport facilities in Long Beach, Los Angeles, Oakland, San Francisco, and Seattle—all facilities that would be used to deploy material into the Pacific Theater. An unknown actor demands $500 million to unlock the systems. Security analysis identifies the attack as Conti ransomware deployed via a spearphishing attack that compromised employee accounts lacking multi-factor authentication. The Conti Ransomware Gang is known to perform ruthless attacks on life-critical systems, but in this case, the NSA and DHS are unable to attribute the ransomware attack's initiator.

Events also continue to unfold in Asia. The identities of U.S. diplomatic and intelligence personnel stationed at diplomatic posts throughout Asia are posted on Chinese social media sites, which urge "loyal Chinese patriots" to track down and hold these individuals accountable for "aggression against China." Intelligence analysis of Chinese operations reveals that information about these personnel were likely obtained through the SolarWinds leak in early 2020.

On top of actions in the cyber domain, China has detained four U.S. citizens working for Ford in Shanghai, accusing them of espionage.

In this move, teams do not have specific tasks. Instead, determine what actions you believe your agency is responsible for and develop a set of policy recommendations. Again, ensure the recommendations are in line with the president's objectives and are coordinated with the other agencies. President Biden, however, has tasked the NSC to address three specific points (ensure, however, that you consider all events that have transpired):

- The president seeks advice on retaliation for the cyberattack on Guam. Specifically, he asks for legal and military/intelligence guidance on 1) the legality of a retaliatory cyberattack and 2) an assessment of the risks of spillover effects that impact non-military actors in China (he is concerned about the legal, political, and ethical implications of harming civilians)
- How to address the ransomware incident?
- What actions can the United States take to deter further aggression against the U.S. homeland and Taiwan without significantly escalating tensions?

Move 3:
January 5, 2021
(40 minutes, followed by 20 minute brief)

In the days following the cyberattack on Guam, PLA forces continued to flow into the mainland areas near Taiwan. In response, Taiwan ordered a full mobilization of its reserve forces and heightened its military alert level on December 29th. That evening, President Biden issued a public statement again urging calm in the Taiwan Strait Crisis of 2021, and reiterated Washington's support for Taiwan's democratic system.

Efforts to remove the ransomware have been largely ineffective and the port facilities remain closed. The port closure has had several follow-on effects. First, the inability to load/un-load ships has led to a back-up of shipping vessels both off the western U.S. coast and in key chokepoints, including the Panama Canal. Shipping analysts have described the port closures as having the potential to generate a larger impact on global trade than the 2021 Ever Given incident. The U.S. Chief of Naval Operations has voiced concerns that delays at the Panama Canal could make it difficult to reposition naval vessels in the event of conflict. Closer to home, fears that the port closure will exacerbate global supply chain issues has led to Americans to begin stockpiling household goods. In Los Angeles, large scale protests erupt as port workers take to the streets criticizing the U.S. government of its inability to resolve the ransomware incidents. Other actors take advantage of the protests to loot homes and businesses around the city. Amid the chaos, protestors set the Chinese Consulate in Los Angeles ablaze, resulting in the death of two Chinese consular officials. The governor of California activates the National Guard to restore calm. Governors in several other states including Washington, Texas, Florida, and New York follow suit as a preemptive measure.

China's foreign minister condemns "the violent attack" on its Los Angeles Consulate and publicly lambasts the United States for failing to uphold its responsibilities under the Vienna Convention on Consular Relations. As protests outside of U.S. diplomatic and consular facilities in China mount, the Chinese foreign ministry announces they are no longer able to ensure the security of U.S. consulates in China and orders the immediate closure of U.S. consulates in Shanghai, Nanjing, and Guangzhou. These facilities support some of the largest populations of American citizens in China.

U.S. intelligence indicates that a U.S.- based Taiwan-activist group is taking advantage of the protests to deliberately target Chinese diplomatic facilities and may be planning to attack Chinese diplomats and consular officials in major U.S. cities. While some officials in the DHS and DOJ push for search warrants (and forced nondisclosure, to keep the search under wraps) to inspect electronic communications of protest attendees, they face pushback from internal groups that believe the warrant would grossly violate the privacy of innocent citizens exercising their protest rights.

On January 3rd, a U.S. Air Force RQ-4 unmanned reconnaissance aircraft flying 50 miles north of Taiwan crashes into the East China Sea after U.S. operators lose contact with the aircraft. Initial reports suggest that Chinese disturbance signals jammed the drone signal and disrupted communication with its operators. A frigate from Taiwan's Navy sailing to the crash site to help recover wreckage suffers an explosion, killing 17 Taiwanese sailors. Although it is too soon to assess the cause of the explosion, members of Taiwan's public are calling for military retaliation against China.

At home, American pundits and politicians are calling on President Biden to resolve the situation. Hawks are calling for action to punish China for causing the incident; some doves have demanded that Biden cut back elements of the arms deal as an olive branch to China; while others simply hope the U.S. stays out of the rapidly escalating conflict in Taiwan.

Determine how your agency can best respond to the events that have transpired in this move and develop a set of policy recommendations. What are the most important issues that your agency must wrestle with? Again, ensure your recommendations are in line with the president's objectives and are coordinated with the other agencies.

RES.TLL-008 Social and Ethical Responsibilities of Computing (SERC)
Fall 2022