**TO:** The Honorable Wendy Fallon
**FROM:** Garrett Hinck, Jordan Cohen, Natalie Brown, and Sebastian Mada
(Georgetown STIA Cyber, Coach Samuel Visner)
**SUBJECT:** JP Morgan Chase Cyber Attack

**Judgements:**

The recent cyber attack on JP Morgan Chase (JPMC) threatens our nation's critical infrastructure, but it is not yet possible to definitively attribute this attack to the organization behind it. While preserving the U.S. cyber deterrent demands immediate action, determining a proportionate response requires further consideration and intelligence. Furthermore, allowing JPMC to respond under the Cyber Marque and Reprisal Act jeopardizes U.S. government control of the situation and risks escalating the conflict with China.

**Background on Cyber Attack on JPMC:**

JPMC is considering employing cyber privateering to respond to the ongoing distributed denial of service attack (DDoS) from a botnet that compromised the Agricultural Bank of China earlier this week. According to JPMC, this attack is affecting their business-business transactions. In response, JPMC will be taking individual action under the Cyber Marque and Reprisal Act. President Xi Jinping of China has accused the U.S. government of perpetrating the attacks against China's banking networks by leveraging vulnerabilities in Linksys router software.

**Substantiation:**

The attack of JPMC is a threat to vital critical infrastructure that demands immediate action. Disruption of U.S. financial services could cripple the U.S. economy and, pursuant to Presidential Policy Directive 21, the financial sector is part of U.S. critical infrastructure. Under the US-CERT's Cyber Incident Severity Schema, this attack is a severe incident, constituting a significant impact to national economic security, as JPMC's ability to provide business-business credit is under attack.

A definitive attribution of the attack on JPMC cannot be made at this time. Despite the fact that elements of AgBank China's infrastructure are participating in the attack, it is not clear that the Chinese government directed the attack. Reports indicate that this malware exploits a common vulnerability, Shellshock, and links Internet of Things (IoT) devices including Linksys routers to form a botnet. This botnet attacked AgBank China and converted its machines. Because this vulnerability is common, and because large DDoS attacks involving IoT devices have originated from private actors, the attack could be coming from an unknown source.

Allowing JPMC to respond via the Cyber Marque and Reprisal Act would most likely lead to an escalation of the conflict. Privateering, the practice allowed by the Cyber Marque and Reprisal Act, is illegal under customary international law, and cybercrime is outlawed by the Budapest Convention. China would most likely accuse the U.S. of illegally directing a corporation to attack its national infrastructure. Furthermore, JPMC has an incentive to act aggressively to cripple a financial competitor, and therefore escalate the political crisis.

Preserving U.S. cyber deterrence requires immediate action, but delaying may be necessary to determine the time, form, and scale of a response. An immediate condemnation of the Chinese government for tolerating this DDoS botnet risks further escalation, while covert operations risk the appearance of doing nothing. Determining a 'proportionate' response that may include diplomatic repercussions, sanctions, or cyber reprisals in kind takes time, but postponing a response compromises U.S. credibility by the hour.

**Decision Document, Cyber 9/12 Incident, Georgtown STIA Cyber**

**Issue:** Ongoing DDoS attacks against JP Morgan Chase from an unknown source leveraging compromised elements of the Agricultural Bank of China.

***Policy Recommendation:*** Flexible policy involving public reassurances and cooperation with China, with recourse that provides calibrated response in case of non-cooperation

---

**Policy Alternatives & Analysis:**

**1. Transparency and Public Outreach**

- Publicize nature of attack, Shellshock vulnerability, Chinese involvement
- Pressure China to cooperate and update its compromised infrastructure
- Significant risks of consumer panic, public pressure to create conflict
- Public approach may not adequately protect security of U.S. financial system

**2. Public Diplomacy with Covert Action**

- Public outreach to China asking for cooperation, using One China policy as leverage
- ODNI & NSA operations to gather intelligence on Ag Bank China's networks
- Potential for valuable information for attribution, but serious risk of discovery
- Appearance of inaction if covert action fails to generate significant results

**3. Public reassurance and Flexible Diplomacy**

- Reassure the financial sector through public statements and FBI, NCCIC support
- Negotiate with China to share information and respond jointly, foster norms
- Act flexibility and utilize ISP geo-blocking if China does not cooperate
- Mitigates damage, emphasizes information sharing
- Provides flexibility in diplomacy that allows for future calibration

**4. Forceful Response**

- Demand Chinese cooperation in U.S. investigation and in disabling attacking systems
- Upon refusal, immediate action by intelligence services to collect information and disable attacking systems.
- Significant risks of escalation, given likelihood China will refuse to cooperate
- Develops a doctrine of responsibility for cyber attacks originating from nation's territory

---

**Justification of Recommend Policy Response:**

***Response #3: Public Reassurance and Flexible Diplomacy***
*Cost of Inaction:* JPMC Response, leading to unnecessary, uncontrolled escalation
*Stability:* Preserves confidence while more information is gathered
*Diplomatic Cooperation:* Creates norm that allows peaceful cooperation in future
*Information Gathering:* Cultivates international information sharing

**Decision Document II, Cyber 9/12 Incident, Georgetown STIA Cyber**

**Issue:** Escalation of Chinese diplomatic crisis due to current cybersecurity incident

**General Recommendations:** Release presidential statement of condolences to China, US-CERT alert advising immediate patching of known vulnerabilities in affected routers, Halt issue of Letters of Marque until the implications of this act are explored further

***Policy Recommendation:*** **Option #3: Negotiate with China to resolve the crisis, based on a U.S. apology, cyber confidence building measures, and proposed agreement**

**Policy Alternatives & Analysis:**
1. OBJECTIVE: Stress int. norms while focusing on defensive measures and domestic security.
ACTION: Secretary of Homeland Security Lead - Approach China on the International Stage, strongly condemn any reprisals, and convince them that peaceful resolution is best, while thoroughly investigating the effects of the Cyber Marque and Reprisal Act and the role the intelligence community has played in this crisis.
RISK: China has no reason to proactively approach us in diplomatic channels, is likely to see hypocrisy in U.S. reliance on norms, and distrust that the U.S. is sufficiently addressing why escalation occurred.
BENEFIT: Take the time to fully investigate what occurred and how U.S. government and private sector actions have played a role in the escalation.

2. OBJECTIVE: Raise military readiness in response to Chinese threats.
ACTION: Secretary of Defense Lead - Put U.S. Pacific Command on High Alert, Instruct U.S. Cyber Command to collaborate with Pacific Command and prepare to defend U.S. networks. Issue a presidential statement decrying Chinese threats against the United States.
RISK: China would perceive this action as highly aggressive. It risks escalating the situation and does not solve the underlying diplomatic crisis.
BENEFIT: Signals to U.S. allies that China will not intimidate U.S. in Pacific region, Ensures U.S. credibility and deterrent against any Chinese or non-state actor attack

3. OBJECTIVE: Resolution of crisis through diplomacy, creating a durable cyber framework.
ACTION: Secretary of State Lead - Share threat intelligence with China, and offer cooperation based on a U.S. official apology in order to negotiate comprehensive cybersecurity code of conduct agreement, and national accountability for cyber incidents.
RISK: Rejection of proposed talks by China could be likely based on mistrust.
BENEFIT: Resolution of crisis, contribution to lasting international norms, reduction of misperceptions between U.S. – China.

4. OBJECTIVE: Utilize radical transparency to call China's bluff
ACTION: National Security Advisor Lead - The US would publicize and rebuke NSA involvement in the creation of the tools that may have been involved in the attack on Chinese systems to set a precedent of transparency and cooperation. Establish a U.S. - China direct military hotline. The US would give the Chinese government intelligence regarding the capabilities that Bakatax possesses in order to demonstrate that they did not perpetrate the attack.
RISK: The US appears weak in the face of Chinese aggression. Loss of US offensive cyber capabilities.
BENEFIT: The US gains moral legitimacy in the eyes of the international community. The Chinese are unlikely to escalate once exposed to relevant US intelligence.

**Justification of Recommended Policy Response:**

- Resolves misperceptions between U.S. - China through generous promise of apology, despite evidence that Bakatax is not entirely to blame for Chinese deaths.
- Long lasting agreement not only defuses current crisis but prevents further incident escalation.
- Most effectively leverages joint U.S. - China economic interests and averts conflict.
- Emphasizes joint responsibilities - regarding current and future attacks.