AUGUST 31, 2018

FROM	JOLTT (Coach: Robert Chesney, Team Members: Alex Shahrestani, Mohamed Al-Hendy, Zeyi Lin, Craig Gertsch)
MEMORANDUM FOR	The Hon. Wendy Fallon, Special Assistant to the President and White House Cybersecurity Coordinator
SUBJECT	Response to JPMC Cyberattack and Chinese Aggression

Recent tensions with China have become entangled with a significant DDoS attack targeting JPMC (we assess, with low confidence, that the Chinese government is behind that operation). The situation implicates important national interests, including avoiding an escalation spiral with China that might result in economic damage or military conflict, ending the immediate threats to our critical infrastructure, and deterring future attacks. We outline four policy packages below, and recommend Option 1 ("the Diplomatic Defense Package") as the best way to balance the competing interests at stake.

Option 1: The Diplomatic Defense Package

The highest priorities should be protection of our economy and avoiding an escalation spiral. To these ends, President Trump should signal our intent to preserve diplomatic and economic relations by publicly responding to President Xi with a message recognizing China's sovereignty and status as a valuable economic partner, while also denying any role in the AgBank attack. Meanwhile, in accordance with the National Cyber Incident Response Plan, immediate coordinated measures should be taken to protect our financial sector, including but not limited to close coordination among NCCIC, US CERT, the National Cyber Investigative Joint Task Force, the FS-ISAC, and the Justice Department. Among other things, FBI and DOJ should move quickly to sinkhole the DDoS attack, while NSA moves aggressively to collect intelligence to inform these efforts. This multi-pronged approach leverages agency expertise and avoids potential diplomatic fallout.

Option 2: The Cyber-Deterrence Package

If the balance of equities favors deterrence of future attacks over avoidance of an escalation spiral, we could take this opportunity to demonstrate our capacity and will to punish China. Most aggressively, we could exploit weaknesses in the Chinese "Great Firewall" to disrupt censorship. Less aggressively, we could also greenlight JPMC's request to proceed with using Bakatax under authorization of the Cyber Marque and Reprisal Act, accompanied by a public statement by

President Trump (made only after trading hours on Friday, August 31, 2018). Both steps run the risk of escalating tensions, and interference with the Great Firewall seems likely to precipitate a strong Chinese response.

Option 3: The Cyber-Agreement Package

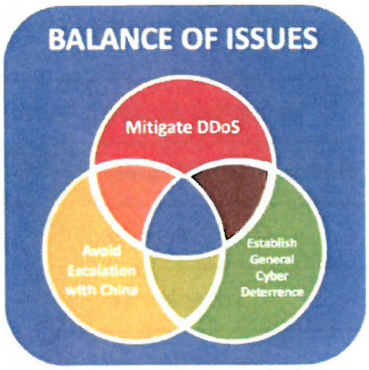
Another approach that prioritizes the avoidance of an escalation spiral involves seeking a grand bargain. Specifically, President Trump could propose an agreement under which both countries collaborate to identify the attackers on *both* AgBank and JPMC. This approach would require that the United States reveal significant portions of its cyber capabilities. Additionally, a cyber-intelligence relationship with China is unprecedented, untested, and fraught with political uncertainty. However, the proposal would undermine China's diplomatic posture, reduce China's concerns regarding our technology's presence in their banking structure, and encourage China to reintegrate itself in the US economy.

Option 4: The Economic Sanctions Package

Finally, with an emphasis on stopping the current attack and deterring future attacks, we can employ a cross-domain response that plays to our strengths. Specifically, President Trump could invoke the International Emergency Economic Powers Act to sanction key Chinese entities or individuals linked to the JPMC attack. Using a scaled approach, President Trump can warn the Chinese in private that targeted sanctions will occur and intensify if aggression does not cease. We could also announce sales of new weapons systems to Taiwan, Vietnam, or the Philippines. However, Chinese reciprocation against our economic actions could prove damaging long-term to our own economy; this is a risky strategy.

EXECUTIVE SUMMARY

An effective response to the JPMC DDoS attack requires balancing a complex set of **three interrelated issues**: (1) **avoiding an escalation spiral** that can turn into a trade war or military conflict with China, (2) **mitigating a serious cyber attack** on critical financial infrastructure, and (3) **maintaining a general cyber-deterrence interest**. In addition to deploying immediate, necessary cross-agency digital "hygiene" measures, there are four additional policy response packages to consider. At this point in time, we recommend choosing the "Diplomatic Defense Package."



POLICY RESPONSES

CROSS-AGENCY DEFENSIVE TASKS

In accordance to the **National Cyber Incident Response Plan**, immediate cross-agency measures should be taken to protect the financial sector and prevent demonstrable harm to national security interests:

- **DOJ: CCIPS, National Security Division**, and **FBI Cyber Division (CyD)** should **work with JPMC** to combat the immediate effects of the DDoS attack
- **Department of Homeland Security: NCCIC** can address the DDoS from an operational level; **US-CERT** can analyze the DDoS incident and disseminate reports on the threat
- **NSA** can gather data on DDoS threats from an international level
- **National Cyber Investigative Joint Task Force (NCIJTF)** can gather and share intelligence
- **FS-ISAC** can preventatively offer member financial institutions with the details of the JPMC attack

OPTION 1: THE DIPLOMATIC DEFENSE PACKAGE

To avoid an escalation spiral with China, **President Trump can publicly signal** our intent to preserve diplomatic and economic relations with China. Furthermore, President Trump can **retract Cyber Marque and Reprisal Act** authorization from Bakatax and put JPMC's request on hold, with **NSA** gathering intelligence instead. These steps allow us to gather more information while reducing the potential for further conflict.

OPTION 2: THE CYBER-DETERRENCE PACKAGE

The U.S. could **exploit weaknesses in the Chinese "Great Firewall"** to disrupt censorship. Further, we could also **greenlight JPMC's request** to proceed with Bakatax under authorization of the Cyber Marque and Reprisal Act, accompanied by a **public statement** by President Trump after trading hours on Friday, August 31, 2018. Both steps risk escalating tensions, and Great Firewall interference is likely to precipitate a strong Chinese response.

OPTION 3: THE ECONOMIC SANCTIONS PACKAGE

Employ a two-pronged **cross-domain response**. President Trump could **invoke the International Emergency Economic Powers Act (IEEPA)** to sanction key Chinese entities or individuals linked to the JPMC attack. Using a scaled approach, the U.S can **initially warn** the Chinese privately that targeted sanctions will occur if aggression does not cease; if aggressions continue, **publicly authorize the sanctions**. We could also **announce sales of new weapons** systems to Taiwan, Vietnam, or the Philippines.

OPTION 4: THE CYBER-AGREEMENT PACKAGE

Chinese President Xi and U.S. President Trump would **draft an agreement** under which both countries work together to identify the attackers on JPMC and AgBank in the recent cyber incident. This would require the U.S. to show its cyber capabilities to our Chinese counterparts, but encourage China to reintegrate itself into the U.S. economy. However, such agreements have **historically proven unworkable** due to lack of transparency on behalf of China.

EVALUATING STRENGTHS AND WEAKNESSES

Potential Action	Avoid Escalation	Mitigation	Deterrence	Package
Diplomatic Statement				*1*
DDoS Reroute				*1*
Attacker ID				*1*
Attack firewall				*2*
Bakatax Response				*2*
Attack Disclosure				*2*
IEEPA				*3*
Weapons Sales				*3*
Agreement				*4*
Disclose Capabilities				*4*

RECOMMENDATIONS

RECOMMENDATION: Coordinate cross-agency defensive response to stop attack on critical financial Infrastructure (JPMC)

*Respond **in accordance to** National Cyber Incident Response Plan **in coordination with** NCCIC (public-private response), US CERT (examine threats), NCIJTF (information sharing), FS-ISAC (support financial services), DOJ (defend and investigate)*

RECOMMENDATION: "Diplomatic Defense Package"
Public statement to preserve diplomatic and economic relations with China; deny involvement in AgBank attack

OPTION: "Cyber-Deterrence Package"
Aggressive response: exploit weaknesses in "Great Firewall""; greenlight JPMC request to use Bakatax

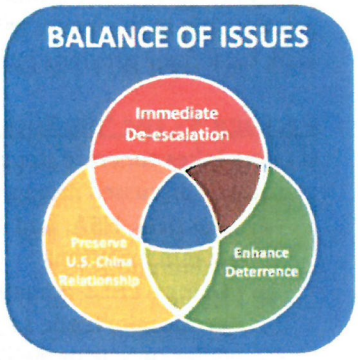
OPTION: "Economic Sanctions Package"
Invoke International Emergency Economic Powers Act to sanction China/Chinese entities in connection with attack; announce sales of weapons to Chinese neighbors

OPTION: "Cyber-Agreement Package"
Propose agreement to identify attackers on AgBank and JPMC; establish cyber-intelligence relationship with China, reveal U.S. capabilities

TEAM JOLTT **DECISION DOCUMENT** **SEPTEMBER 3, 2018**

GOALS

1. **Immediate de-escalation** of tension with China
2. **Preserve** the long-term U.S.-China relationship
3. **Enhance deterrence** capabilities more generally



BACKGROUND

We assess with high confidence that CyMRA-authorized Bakatax countermeasures significantly reduced or stopped the DDoS attack on JPMC. However, we also believe that these countermeasures resulted in limited casualties within Chinese government circles. We re-affirm our assessment with low confidence that China was behind last week's JPMC DDoS attack; in addition, new intelligence indicates the possibility of North Korean involvement.

POLICY RESPONSES

Digital "Hygiene" Tasks

There are three tasks that must be done before acting upon any additional policy package:

A. Interagency communication and cooperation building on the framework of the **National Cyber Incident Response Plan** (national approach involving multiple agencies and partners including **DOJ--CCIPS, FBI, CyD; DHS--DCCIC; US-CERT; NCIJTF; FS-ISAC)**
B. **FDA and DHS ICS-CERT** should direct manufacturers **(Hospira and GE)** to patch vulnerabilities and continue to encourage healthcare facilities to follow delineated recommendations
C. **NSA** should continue to collect intelligence for ascertaining attribution

Package 1 - Proportional Response

There are **two threats** from China that immediately require a necessary and proportional response: the potential sale of $1.3T in Treasury notes and the use of military and cyber capabilities. Thus, we recommend inviting Chinese Foreign Minister Wang Yi to the White House and discussing the following with him:

A. With regards to the Treasury bill threat, we first privately **warn China of significant monetary loss**; recommend the Treasury Department **buy up notes** to minimize damage
B. With regards to the military threat, we privately **warn China of the unnecessary casualties** in the case of military escalation and **pre-emptively reinforce PACOM AOR capabilities**

By utilizing these options, we maintain a firm initial response while retaining flexibility for other options moving forward.

Package 2 - The "Olive Branch" Option

If China takes concrete steps to de-escalate following our initial response, we can focus on preserving the long-term U.S.-China relationship in the following ways:

A. Offer to help **mitigate technical vulnerabilities** in known affected devices located in China
B. Make a **public "statement of sorrow"** regarding injuries caused by Bakatax countermeasures without admitting responsibility, similar to the 2001 Hainan island incident statement.
C. Offer **private compensation measures** for affected Chinese casualties in exchange for a commitment to cooperate with the U.S. to determine JPMC and AgBank DDoS attribution

This package rewards China for de-escalating tensions, and works to strengthen the US - China relationship in the future without placing either country's leader in the awkward position of having to walk back their previous public statements.

Package 3 - The "Big Stick" Option

If China takes concrete steps to escalate following our initial response, we suggest, in addition to the previously discussed measures Package 1:

A. Put **DHS, NSA, and U.S. CYBERCOM on high alert** for all Chinese and North Korean communications
B. Using a cross-domain approach, we recommend **warning and following with the threat of economic/trade sanctions under IEEPA**
C. Offer new arms deals to **Taiwan, Vietnam, or the Philippines**

Purposely, none of these measures initiate active armed conflict with China, and instead aim at sending a more forceful deterrence message to China that we are willing to use military force if necessary.

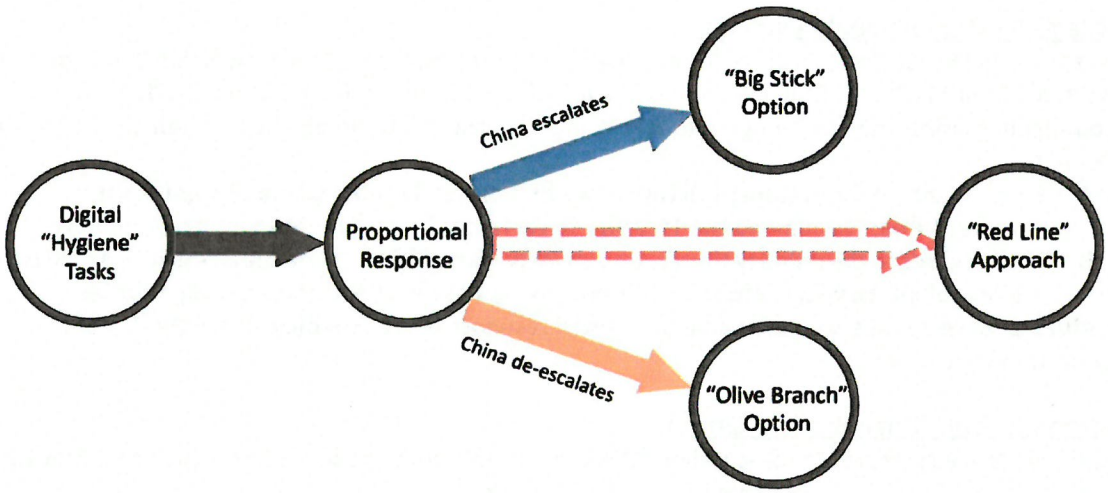
Package 4 - The "Red Line" Option

Alternatively, instead of taking action based on Chinese responses, President Trump can privately convey a "red line" message to China that any significant level of military/cyber escalation will be reciprocated with:

A. The full force of the U.S. **military action**
B. A **potential attack** against the Chinese Great Firewall

This approach sends a strong deterrence signal to China to cease aggression; however, it is hard to walk back from a red line, as shown by President Obama in Syria in 2012.

DECISION PROCESS



RECOMMENDATIONS

Following implementation of digital hygiene tasks, we are recommending the implementation of package one, followed by package two or three depending on China's response to package one. We believe this series of actions represents the best plan of action to encourage China to back down on its military and diplomatic aggression, and sends a strong deterrence message to other hostile military and cyber actors.