SY403
Fall 2018
Exercise WESPAC EXPRESS – All Moves (One through Four)

3 – 5 December 2019

Move One:

- In a speech on US foreign policy aims, the US President declares a "bright red line" across the East and South China Sea, beyond which the US will assist any and all allies who "intend to exercise freedom of navigation or commercial pursuits attendant to operations in international waters"
- While the President does not cite the limits or means the US is prepared to employ in the defense of allied use of disputed waters, the President has previously cited an increasing willingness by the US to employ cyber as an instrument of national power "if and when the times require it." Most observers consider the President's statement to be a "coming of age" declaration for United States Cyber Command, now in its ninth year of operation.
- Soon after the President's declaration, China sends several light surface combatants to chase Japanese fishing vessels out of waters near islands claimed by China in the East China Sea.
- Two days later, the Japanese fishing boats return, this time with three Japanese frigates. This time there is no Chinese interference.
- The Chinese government reacts cautiously. There are some mildly antagonistic comments from "senior PLA officers." However, official Defense and Foreign Ministry spokesmen, in virtually identical statements, stress China's commitment to the peaceful settlement of disputes and call upon Japan to show greater restraint.
- At the same time, anti-Japan rhetoric heats up in a number of news sources (not state-run) and Sina Weibo, the Chinese version of Twitter. There are demonstrations against Japanese "militarism" in several cities. And popular social networking and blogging sites hum with Chinese patriotic themes, including appeals not to forget Japanese historical crimes. There is an undertone of criticism of the Chinese government for not defending Chinese sovereign territory in the face of Japanese "aggression."
- U.S. intelligence picks up that China's leaders are surprised by the intensity of the popular outcry but want to proceed cautiously lest a crisis occur, possibly with U.S. involvement.
- Within days, Chinese "patriotic hackers" penetrate and corrupt Japanese non-governmental web sites. They even hijack one site to warn Japanese that the Chinese people will not tolerate infringement on China's sovereignty (by implication, even if their government will).
- Several days later, Chinese frigates show up in the contested waters and steam perilously close to Japanese fishing vessels. There are no incidents between the warships of the two countries.
- In the days that follow, both Japanese and Chinese media, publics, and blogospheres are focused on little else.
- The Japanese ambassador to Washington calls on the Secretary of States to ask what the United States would do if asked by Japan to join a show of force to resist Chinese attempts to back their

claims by threat of force. In parallel, the Japanese Self-Defense Force asks U.S. Pacific Command about the possibility of joint operations in the East China Sea as a signal to China.

- In both channels, the United States says only that it will meet its treaty commitments.
- As a precaution, both Japanese and U.S. governments call for government users to exercise vigilance against Chinese hackers. Chinese officials respond to complaints about hacking from China-based servers by claiming difficulty in finding much less stopping such activity.

Questions:

- What might U.S. maritime forces be called upon to do in the developing situation?

- What are the sources, motivations, and potential effects of apparent cyber threats?

- What network precautions should the U.S. military (especially the Navy) take as a whole take?

- What preparations or operations should US Cyber Command undertake?

- What measures should be taken by personnel of individual vessels (should the command issue rules of engagement, ROE?), or should naval units await specific instructions?

- How does the broader worldwide political situation affect your responses?

- Any other matters you deem important at this

SY403
Fall 2019
Exercise WESPAC EXPRESS
As of 3 December 2019

Move Two:

- The United States agrees to send naval forces for Japanese-American operations in the East China Sea, though not in contested waters (lest it be seen as endorsing Japan's claims).
    - INDOPACOM-JDF contacts are instructed to design non-provocative joint maneuvers, intended only to remind China that the Japan-U.S. bilateral defense treaty could be invoked if Chinese vessels attacked Japanese fishing or naval vessels.
- The Chinese government remains restrained.
    - While reiterating Chinese territorial claims and insisting that Japan is acting belligerently, Beijing is calling for the two parties to hold high-level talks to avoid mistakes.
    - Consistent with its position that this is a bilateral matter, the Chinese in public and private call upon the United States not to inflame the situation by encouraging Japan to use force or by sending forces.
- Chinese hackers continue to corrupt popular Japanese social-networks through a combination of service denial attacks and insertion of phony content, and appear to interrupt traffic on the Japanese maritime authority's network.
    - These attacks are not very sophisticated or coordinated, and patches are quickly put in place.
    - Similar penetrations by Japanese hackers are reported by China
    - Internet-based communications among U.S. naval and other military units experience minor irregularities and disruptions well above the "usual and customary baseline". The Japanese report similar problems.

- Chinese civilian officials responsible for cyber-security make contact with their American counterparts through a channel established by the two governments to prevent cyber-war and cooperate against third-party hacking.
    - While explaining that incensed Chinese citizens and pressure groups appear to be active, China declines U.S. involvement in attributing, tracking, and neutralizing these groups.
- Despite Chinese warnings, U.S. and Japanese surface units rendezvous in the East China Sea, but not in contested waters.

Questions for Move 2:

- Beyond the operations already ordered, what might U.S. maritime forces be called on to do?

- What are the sources, motivations, and potential effects of apparent cyber threats?

- Should INDOPACOM and the U.S. Navy take steps to minimize either unclassified and/or classified communications that use the internet?

- What role should the INDOPACOM-CYBERCOM combat mission teams be expected to play?

- Is there sufficient cause to place US intelligence and investigative agencies on higher alert?

- What if any defensive or offensive steps should be taken by individual naval units?

- What communications should be undertaken with the Japanese? The Chinese?

- Any other matters you deem important at this stage?

<u>Move Three</u>:

- China has not reacted militarily to U.S.-Japanese exercises in the East China Sea, largely because they remain in uncontested areas.
    - Government spokespersons are consistent in emphasizing that all parties must avoid confrontation and in laying the blame with Japan.
- While passive in the East China Sea, Chinese naval forces appear near disputed islands in the South China Sea. China informs the United States that this is only a precautionary measure.
- U.S. intelligence reports disagreements between Chinese foreign ministry officials and the PLA as to how to proceed – the former urging caution and the latter urging resolve.
- INDOPACOM alerts all forces assigned to it to increase readiness for operations in both the East and South China Seas**, and requests TRANSCOM to begin the processes associated with movement of forces into the theater**. **TRANSCOM soon thereafter begins reporting noticeable disruptions and corruption of data in the deployment data bases.**
- Chinese media and social-networking step up the drum beat of anti-Japanese rhetoric.
- In addition to increased disruption of Internet-based civilian and governmental networks, a large exfiltration of data from defense-contractor computer networks is reported by U.S. intelligence. INDOPACOM and CYBERCOM also report content irregularities in certain unclassified data bases.
- **U.S. electric utilities experience isolated but more frequent power fluctuations and short outages, primarily on the West Coast.**
- **In general, cyber attacks from apparent Chinese sources are becoming more sophisticated and consequential.**
    - These attacks are confirmed to be from China's physical territory, though it is less certain they are attributable to the PRC government.
    - A group called Citizens for China's Honor, previously unheard of, announces that it is responsible for cyber-attacks, that these are directed against Japanese "militaristic revisionists," that they will increase, and that collateral inconvenience for third parties is regretted but unavoidable.
- In the relatively new cyber-security consultative channel, China reiterates that it is trying to find and stop patriotic hacking and requests U.S. technical assistance in active network surveillance to this end. China also complains to the United States about being targeted by Japanese hackers.
- Japan proposes that U.S. and Japanese forces enter disputed waters in the East China Sea.
- Vietnam and the Philippines request that U.S. forces be sent to the South China Sea.
- At the political level, China proposes direct bilateral consultations with the United States for the purpose of defusing the brewing crisis. Japan would be excluded.

Questions for Move 3:

- What are the intentions of China? Of Japan?
- What are the sources, motivations, and potential effects of apparent cyber threats?
- Should the United States agree to China's proposal for political talks to defuse the crisis?
- Should the United States agree to cooperate with China to curb private hacking?
- Should the United States agree with Japan's request to move joint forces into disputed waters?
- What posture should the United States take toward increased Chinese activity and requests for support by local states in the South China Sea?
- Should INDOPACOM combat mission forces prepare for offensive cyber actions? If so, what should they be doing? If not, why?
- Should CYBERCOM assist civilian infrastructure owners with protection measures? What access does the US military need to civilian (private sector) data and/or infrastructure to prepare for and support these operation?
- Should the U.S. Government take actions to secure government and other critical networks or to deter attacks?
- What should be the highest priorities for intelligence collection and analysis?
- Any other matters you deem important at this stage?

Move Four:

- The U.S. intelligence community reports a substantial increase in disruptions and ex-filtration in intelligence, national security, and critical network traffic.
- INDOPACOM reports intermittent but severe disruptions in networks on which it relies to surge and support naval and other forces. **Commercial shipping and air transport companies involved in the movements report interruptions of their networks and data corruption.**
- Individual units report major degradation in their ability to receive guidance and to coordinate their actions. **Satellite-based C4ISR systems, in particular, become increasingly unreliable.**
- Internal and external Chinese government communications are sharply reduced, for reasons that are unclear.
- Chinese media and social-networking content strikes a different tone: calling for national unity and sacrifice, and referring to Japanese as "running dogs" of American neo-imperialists.
- The Chinese government transmits a statement via the Internet explaining that use of the Internet should be minimized and the government will be using it to transmit guidance to Chinese citizens.
- Chinese naval forces enter disputed waters in both the South China Sea and East China Sea on a large scale. Chinese officials declare that Chinese sovereignty over key islands in both seas is a "core interest" that will be defended at all cost.
- The U.S. intelligence community reports PLA has taken note that US has not sent forces into disputed waters, have not conducted any cyber attacks, have not warned China of cyber retaliation, and have not activated mil-mil channels, all of who emboldens the PLA.
- China officially urges the United States to avoid any moves that could escalate the crisis.
- All public appearances and statements by the Chinese government are made by state officials with PLA senior officers at their side.
- **The Western portion of the US electric grid experiences significant but intermittent outages over a period of several days. Power company technicians cannot determine immediately the cause(s).**

Questions for Move 4:

- What are Chinese intentions? Has the US/Chinese political context changed?
- What might be the sources, motivations, and potential effects of cyber attacks?
- Has deterrence failed at this point? To what extent has cyber contributed to the current situation?
- What operations must U.S. maritime forces be able to undertake, and how dependent are these on network security?
- What defensive measures should the U.S. government as a whole (including DHS, FBI, NSA, etc.), INDOPACOM, CYBERCOM, and naval commanders take in regard to critical networks?
- Should the United States undertake any offensive cyber operations? Against what targets and for what purposes? What reaction can be expected? Who should authorize, direct, and execute offensive action?
- How should unit commanders react to the degradation in communications and C4ISR?
- Any other matters you deem important?