CSCI 1800: Cybersecurity and International Relations

Midterm Project -- The South China Sea & Critical Infrastructure

Due: 11:59pm, April 13, 2017
Submit On Canvas, Partner Project

Introduction:
The National Security Agency (NSA) is investigating a sophisticated cyberattack on Vietnam and EVETS PLC, a U.S.-owned oil and natural gas corporation. The attack began on September 15, 2017 with a distributed denial of service (DDoS) attack on Vietnamese Air Force networks, followed by exploitation of EVETS PLC’s networks.

The attacks follow what China perceived as infringement on its sovereign territory by a US-flagged gas exploration and drilling ship escorted by the Vietnamese Navy in the South China Sea. The attack is currently affecting Vietnamese military networks and the energy sector, with a risk of escalating to other sectors. The nature of the attacks, as well as nation-state dependencies and industry vulnerabilities, means that the U.S. government must act swiftly to allay concerns from the private sector and international partners.

These attacks pose a significant threat to Vietnam, the U.S.-Vietnam relationship, and U.S. relations in the region. On the U.S. side, the President will need to take swift action in order to appear strong on defense and capable of supporting industry during the fragile recovery of the US economy. Given our insight into the range of cyber capabilities that can be delivered by China on any one of its neighbors (or the U.S. homeland), the potential involvement of non-state actors such as hacktivists, for-hire hackers, or commercial “hackbacks,” and the unclear but significant precedent set by any response, a concerted effort to understand all potential downstream impacts of a response is critical.

Background:
- Preliminary Report on Dual Cyberattacks
- Joint Security Awareness Report

Assignment:
Assume the timing is September 28, 2017, and you are the Assistant Secretary of Defense for Asian and Pacific Security Affairs. Write an analytical policy memo to the Secretary of State, discussing the implications of the cyberattack. The policy memo should show informed judgement on the severity of cyber operations, the possibility of further cyber exchanges and hidden threats, and the fact that swift diplomatic response has little time for in-depth cyber
forensic investigation. All policy recommendations must be backed up by available technical intelligence. The policy memo should also demonstrate adequate understanding of key international relations concepts, including but not limited to geopolitical, economic, historical and legal aspects.

The memo should be organized using the following format:

Summary: A short summary of what you are proposing, how you will go about it, and what allies and obstacles you foresee (5 lines max)

Background: Define the problem as clearly as possible. Identify the key players and examine their motives. Describe history, economic and legal factors, public pressures and political issues that have bearing on the decision. Be sure to discuss technical elements (~2-4 pages)

Strategy: Think about your capabilities and your paths to influence. Describe how to overcome obstacles, what incentives or threats you can offer to others (potential allies), and a timeline for response and follow-through (~1-2 pages)

Policy Options: Describe succinctly 3~4 courses of action you might take and how they might differ in terms of requirements and execution. Include pros and cons for each (both technical and policy-based)-- explain the consequences of failure of each option, potential downsides of success, and mitigating steps you might take. (~3-4 pages)

Next Steps/Recommendation: After weighing the various policy options, tell the Secretary which course of action they should pursue and what you (and others) will do to get the ball rolling. (~2 pages)

Citations: at the end of the document (MLA, APA, or Chicago)

Length: 10-12 double-spaced pages, 12pt font, 1 inch margins.

Tips:
• Don’t fight the scenario. Assume all scenario information presented is true, and use your energy to explore the implications of that information, not the plausibility.
• Think multi-dimensionally. When analyzing the scenario, remember to consider implications for other organizations (E.g., private sector, military, Department of State, regional institutions) and incorporating insights from different disciplines (E.g., law, public policy, cybersecurity).
• Be creative. Cyber policy is an evolving discourse, and there is no single correct policy response alternative to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
• Analyze the issues. The goal of the midterm paper is for students to grapple with complex issues and weigh the strengths and weaknesses of sometimes conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.
• Be mindful of conflicting interests. Government response vs. private sector response; diplomatic response vs. military response; implicit deterrence vs. explicit deterrence; short-term goal vs. long-term goal.

**Grading:**
You will be graded based on the metrics described in the midterm rubric. Your grade will be shared with your partner, so we expect equal amounts of effort and completeness on both policy and technical aspects in order to maximize points. Please see the above table of guidelines to see the criteria on which you will be graded.

<table>
<thead>
<tr>
<th>Paper Guidelines (100 Points)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirements</strong></td>
<td><strong>Points</strong></td>
</tr>
<tr>
<td>Proposed response to crisis</td>
<td>10</td>
</tr>
<tr>
<td>Discussion of the extent to which this course of response is important and relevant. What’s at stake?</td>
<td>10</td>
</tr>
<tr>
<td>Process of implementation from a technical standpoint (challenges and justification of choices)</td>
<td>20</td>
</tr>
<tr>
<td>Process of implementation from a policy standpoint (challenges and justification of choices)</td>
<td>20</td>
</tr>
<tr>
<td>Tradeoff of impact vs. cost and effort of the proposed response (with cost interpreted broadly)</td>
<td>20</td>
</tr>
<tr>
<td>Style - Grammar, 10-12 pages double spaced (including both papers), follows standard formatting guidelines for papers</td>
<td>20</td>
</tr>
</tbody>
</table>

**Great Resources To Get Started:**
1. Asia Maritime Transparency Initiative
3. US, Vietnam Deepen Defense Ties
4. Rodrigo Duterte’s Pivot to Asia is a Rational Move
5. The Chinese Cyber Threat in the South China Sea
6. China's Secret Weapon in the South China Sea: Cyber Attacks
7. Hacking Attack At Vietnam Airports Another Chapter In South China Sea Dispute
8. Cybersecurity: Challenges in Securing the Electricity Grid
9. Cybersecurity: An Overview Of Risks To Critical Infrastructure