CERIAS

The Center for Education and Research in Information Assurance and Security

Cyber 9/12 Student Challenge: Team Purdue Cyber Forensics

Rachel Sitarz, Eric Katz, Nick Sturgeon & Jake Kambic

Challenge Overview: We were asked to take on the role of the Cyber Security Directorate of the National Security Staff. We had to create 4 policy response alternatives to a fictional major cyber incident, that affected US National Security. We were given the task to create the 4 policies, in 5 pages or less, and submit to the Atlantic Council. The policies were aimed to test an understanding of Cyber Security, Law, Foreign Policy, and Security Theory. February 7-8, 2014, we traveled to Washington D.C., to present our policies to Cyber Security experts, who judged our responses based on 5 predetermined criteria.

Scenario: The distributed denial of service (DDoS) attack, along with the spread of the malware "Moonrok" has effectively shut down all the stock markets in the United States. Within five days of the initial DDoS attack, "Moonrok" hit every major financial institution, causing irregularities with their computer systems. At first glance the attack seems to be in response to joint military operations being conducted by the United States and the Republic of South Korea (ROK). One day after the report from the major financial institutions, North Korea claimed responsibility for the cyber-attacks on the United States. The initial indications can only confirm that the attacks appeared to originate in Asia.

Policy Alternative 1

This response is focused on resolving the technical issues with the current attack, mitigating damage and establishing recovery of United States critical infrastructure. PA-1 specifically avoids placing blame on various potential actors, until further intelligence can be gathered and founded in fact.

Decision Process: The United States Government has the responsibility to maintain stable and resilient financial institutions and critical infrastructures. In reacting to this event, the US Government must take into account the current Cyber Laws and react in a way that upholds the laws, and maintains international relationships.

Police Alternative 2

This response incorporates the objectives of PA-1, but identifies a non-state sponsored actor as an enemy combatant. The response utilizes diplomatic methods designed to cease and desist the current attack and strengthen international cyber-crime laws and responses. It asserts that a state is responsible for the use of its infrastructure during a cyber-attack, and aims to strengthen international cooperation and actively disrupt and deter criminal activity in cyber space.

Decision Process: The United States Government must work to mitigate the current and potential future impacts of the event. In doing so, the originating parties must be held accountable for their actions, so that future attacks do not recur.

Policy Alternative 3

This response incorporates the objectives of PA-1, as well as identifying a state actor as being accountable for the attack. PA-3 takes the stances that diplomacy is the best method of diminishing the current attack, while increasing international laws and standards to prevent future cyber-attacks.

Decision Process: The United States Government has a responsibility to protect the United States populous by enlisting their allies with US diplomatic powers, to mitigate the impact and deter future attacks.

Policy Alternative 4

This response incorporates the objectives of PA-1, as well as PA-3, but it establishes that a military response is necessary to end the current conflict. It is the most aggressive policy, out of the 4 Policy Alternatives, but continues to follow international rules and norms.

Decision Process: Cyber-attacks on the US Financial system can be considered synonymous with acts of war, thus the use of US hard power is a necessary option to protect the US interests.

Lessons Learned: This challenge tested our knowledge of the topic of Cyber Security. The judges were very critical of the policies. There was a large focus on military response, versus diplomatic. As well, there was an emphasis on foreign response, versus domestic. It appeared that those who focused on military foreign response, did better than those who focused on domestic response.

- Set actionable goals
- Clearly state what you want to accomplish
- Be upfront with the main primary policy alternative
- Clearly identify how goals will be met
- Explain how you will leverage foreign cooperation
- Utilize "BLUF" or Bottom-Line Up Front
- A weakness of our team was that we did not utilize a coach. Future competitions we will enlist the help of a coach

PURDUE UNIVERSITY