Internet Technology

Student’s Name

Institutional Affiliation

Course Name& Code

Instructor

Date

Internet Technology

**1. Based off of the facts we know, should the attack be considered a crime, espionage or act of war? What should the US response be? How can the US best defend itself from future attacks such as the one that just occurred?**

The attack should be considered a crime, given that the crime was done through the use of a virus and the fact that the virus targeted a US government firm and that the attack itself did not include any critical infrastructure. The US does not have criminal intent to attack another country, but it does have the cyber assets to do so if it were so inclined. The US would view attacks on itself or its allies’ critical infrastructure as an act of war and would be able to use its own cyber capabilities to make those responsible regret their actions. Despite the attack being a crime, acts of espionage and an act of war can occur because of this attack. In the case of an act of war, the cyber attack can undermine the US economy and the proper functioning of vital US infrastructure.

The United States should respond to this incident by filing criminal charges against the attackers of the botnet. The act of retaliating against the cyber attack would not likely be the first time the US has taken such an action but it could be the first to take such an action in response to a cyber attack. This action, however, would be taken against individuals who are believed to be responsible for the cyber attack, International law would not prohibit the US from taking this action, which would be considered as an act of self-defense and would be legal under international law.

US can best defend itself from future attacks such as the one that just occurred by detecting and blocking any potentially malicious code before it executes for the US/ corp networks. The US also should increase its anticrime measures, so that the days of cyber criminals not being prosecuted for their actions are over. The US needs to also defend the private networks of US and/or US allied businesses as well as US government interest in order to effectively defend itself from future attacks. The US should also expand on its current laws along with national cyber policy so that it can better respond to future cyber attacks. Also, the US needs to expand its defensive capabilities and make all of its systems more resistant to the attack in order to stop these types of attacks from occurring in the future. The US also needs to work closely with all nations of the world to ensure these types of attacks are not used again in times of war or as an act of espionage. Finally, the US government needs to update its relationship with the private sector, specifically the banking industry, and make it so that data can be shared between them in order to make it harder for the other country to penetrate.

**2. Should the United States assign US Cyber Command with the responsibility of protecting certain private companies and if so, what should the general standard be for determining what companies the government should be responsible for defending?**

Yes, the government should assign US Cyber Command the responsibility of protecting certain private companies. The government should take an active role in defending private companies and not leave the defense of private entities to private entities. It is precarious that private companies do not have the resources available to protect their data, equipment and networks properly. It is for this reason that the government should assume a strong leadership role in defending private entities and assisting those companies that ask for its assistance.

I propose that the National Security Advisor, National Security Council and National Security Cyber Board establish a Cyber Board of Advisors that would be responsible for assisting the government in the establishment of policies to protect the private sector in the United States. The Cyber Board would provide advice on best practices in cyber defense, educate government agencies on how to protect their systems and systems with information they holds and assist in the creation and dismantling of attack and espionage networks when they are discovered. A Cyber Board of Advisors would be instrumental in determining the threat to affected private enterprise and assisting the government in balancing cost against risk. Bringing in an outside independent group provides another layer of information without the potential of personal bias. A Cyber Board of Advisors would also be able to monitor legal, ethical and financial matters that come with being able to accept or reject these larger risks.

However, in analyzing which private entities the government should be responsible for protecting, it is necessary that the government use a fair, objective standard and take into account the resources of the firm and the likelihood of a future attack. A fair, objective standard to use would be to add all the resources the firm owns to its payroll. If the firm has a relatively large number of employees on their payroll and/or owns a very large amount of data, that would be a good reason to protect the firm. It is also important to take into account the likelihood of a future attack. If a private entity has been attacked three times already, they are clearly a potential target of attack in the future. Therefore they should be considered a high priority and receive the full protection of the government. On the other hand, if the government decides to add a private entity or entities to a list of those it is responsible protecting, the government must then investigate if each of those listed entities has the necessary resources to adequately defend itself from attack. The government should continue with the investigation until the list is complete and independently verifiable. This list would then become the basis for determining what companies the government is responsible protecting. Therefore, this fair and objective standard is the best way to ensure that the government protects those firms that are most vulnerable. It is also the basis for good policy from the government because it addresses all firms in an objective and equitable manner.

**3. Should the United States lead the effort at an international cyber agreement? Why or why not? What challenges would the President face in trying to get an agreement? Are there any alternatives?**

The United States should lead the effort at an international cyber agreement. The United States is the foremost leader in the Internet. As a leader in the Internet it is very important to the United States that it keeps its dominant position. The United States should be involved in an international cyber agreement for many reasons. First of all it would show the rest of the world that the United States is a democratic nation that is willing to engage in free trade in a fair manner. Thus, it will set aright example showing the rest of the world that United States is willing to negotiate a treaty with other countries where there is mutual interest, rather than use its position as the most advanced country to demand international standards.

There are a number of challenges that the President would face in negotiating an international cyber agreement. The President would be looking to accomplish a lot in the next year and formulating an international agreement would take a good deal of time and effort. The first hurdle for the President would be the advanced nature of the agreement. As pointed out earlier in the paper, an agreement would have to be negotiated. The President will have to address the amount of time, effort and resources that would be necessary to do such a task. Another part of the challenge would be the different attitudes of each of these countries. The Powers behind the NSA, the Chinese and Russian governments and hackers, have different agendas and objectives. Each of these governments, as well as the hackers, would have to decide how committed they are to having a cyber agreement and to compromise and look at the positive effects that having an agreement would have. To this point the United States has not been the first to propose international agreements. The United States believes that the biggest problem with cyber warfare is the fact that we have not agreed upon a solid set of standards yet. The solution to this problem does not stand in isolation. The agreement would have to be a set of standards that would be open and compatible with the rest of the world.

There are different alternatives if the United States is unable to reach an agreement. There are many options that the President could pursue. The simplest alternative is to deter other nations from cyber attacks by building a cyber army that could destroy the Internet of any nation that threatens the United States. This may be the simplest way to resolve the cyber attack issue. Another alternative is to control information that flows into the United States. This would require planting people into companies who are able to monitor their computer systems. A third alternative would be to control who can build software. A fourth alternative would be to use our military and/or NSA to plant malware into computer systems located in nations hostile to the United States. A fifth alternative would be to develop an international committee that would decide what country can build or sell software to a company that is located in the United States. The members of this committee would be countries which are not hostile to the United States.

**4. Are there any substantive changes that should be made to the current US cyber policy?**

Yes. There are several changes that need to be made to the current US cyber policy. Currently, the US does not have a clearly defined cyber foreign policy. For this reason the current US cyber policy is outdated and can often be contradictory. For example, if there is classified information on a private entity server and the government wants access to the server to prevent an attack and the company does not comply with the governments request, what is the next step? Under Section 218, the government must temporarily pause trade talks that the U.S. is having with the country of origin. Upon the investigation of the attack, the government of the affected company is required to assist the government with the investigation. In addition, the government is allowed to contract with the affected company without any competition. In return, the government must report the findings to the company and must safeguard any data it obtains legally. This entire process creates a fertile environment for corruption and also creates a system where the company is blackmailed and/or fearful of a negative response from the United States, if it does not comply with any request.

With the current US cyber policy, it is very cumbersome for the government to take action against a company for refusing to comply with a government request. Section 218 is not an appropriate US policy to enforce the control of cyber attacks and to create a workable and productive relationship between the private sector and the government. As a result, the Section 218 is a very controversial cyber policy.

The current US cyber policy in regards to companies that are refusing to comply with requests to provide information is a very confusing process that leaves many questions unanswered. The following improvements need to be made to be able to provide a working US cyber policy in order to better defend the private sector.

First, information that is critical to the national security, whether classified or not, must always have a legitimate reason for being withheld. For example, if an energy company is ill-equipped to handle the cybersecurity aspects of their company and are in bullet train to losing power, the energy company should not be expected to provide vast amounts of information that could possibly be identifying and classified. In this particular situation, the government must first provide a warning or opportunity to be vigilant and comply with government requests.

Second, the government must provide a reasonable timeline to supply the requested data. If for example the government has reasonable suspicion to believe that a company is a target, the company should be given a certain reasonable amount of time to become more vigilant and provide the government with the requested data. After this is provided, if the government continues to believe that there is an imminent threat, the government must take over without allowing the company to fight to keep its server. However, if the company does nothing to make the situation any better, the government can use the [Contingency Plan] to make note of this and to provide a warning to the company and to ask that they comply with the government.

Third, if the government has reason to believe that the private sector is a target, the

government must provide immediate protective measures. For example, if the energy

company, who is unprepared to protect their network, there is no time for notice or time to

recover, the government must be proactive in making sure that the company is protected.

In this particular case, the government must provide a warning of a potential malware

or attack and then must seize the server prior to the cyber criminal attack. This

will help to ensure that the government has a leg to stand on if there is a dispute in the

future with the company.

Fourth, the consequence for failure to provide adequate security measures, must be clearly communicated by the government to the affected company. An example of this is that the company, who is unprepared to defend against the hacker and the cyber attack, must be required to provide the server or be fined by the government and must then provide the server. Failure to comply with these requirements must not be allowed.

**Conclusion**

In conclusion the new host of threats to the US cyber environment will continue to require a strong response by the government. It is vital that the government take a strong leadership role in defending the public and private sectors in the United States against all enemies, both internal and external. If a response is deemed necessary, it should be built on a foundation of sound policy and sound practice. The continued development of standards and best practices is imperative, as private companies cannot adequately conduct the security of their networks and systems. The government should educate government agencies in how to better protect their systems and systems with information they hold in the cyber domain. Funding must be sufficient so that education, research and improvement can be successful. The government should also assist companies that ask for its assistance. Finally, the government must not only defend itself in the cyber domain, it must also defend itself in cyber crime. All these steps will begin to prepare the United States government for a new cyber reality.