The Cyber 9/12 Student Challenge

Intelligence Report I

Instructions

Your team will take on the role of experienced cyber policy experts working for the Cybersecurity Directorate of the National Security Staff. The date is May 26, 2014, and a major cyber incident is occurring that affects US national security. The president needs information on the full range of policy response alternatives available to respond to this crisis, and your team has been tasked with developing policy recommendations to pass on to the National Security Council and the President. To do so, you will apply your understanding of cybersecurity, law, foreign policy, and security theory to synthesize useful policy measures from limited information.

This packet contains fictional information on the background and current situation of a major cyber attack on the United States. The attack takes place in May 2014, and the scenario presents a fictional account of political and economic developments leading up to the cyber incident. Teams are restricted to facts in the following pages for the purpose of formulating your response.

Keep in mind that you will use the fictional scenario material presented to perform two tasks:

• **Written Policy Brief:** Write an analytical policy brief discussing the implications of the cyber attack for different state and non-state actors and exploring the policy response alternatives you are recommending in depth. The length of the brief is limited to five single-sided pages in length.

• **Oral Policy Brief:** Prepare a ten-minute oral presentation outlining four possible policy response alternatives and recommending one to the National Security Council.

Before you begin, keep these tips in mind as you are reading and considering your policy response alternatives:

• *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) 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 competition is for competitors 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.

Note: All materials included are fictional and were created for the purpose of this competition. Some of the details in this fictional simulated scenario have been gathered from various news sources and others have been invented by the authors. All scenario content is for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

From: National Security Staff, Cybersecurity Office
Re: Cyber attack affecting financial sector

May 26, 2014

At the request of the National Security Council, the NSS Cybersecurity Office is contacting your team to solicit national policy solutions to respond to the situation. Given the unprecedented nature of this attack, the President is seeking to assemble a range of possible policy response alternatives before determining a course of action to announce when markets open for business on Tuesday May 27, 2014. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of each proposed policy response alternative before recommending the one best course of action.

When generating each of your four policy response alternatives, the National Security Staff requests that you address all the following potentially conflicting interests.

> Government Response vs. Private Sector Response
>
> What actions taken in response to the attack should be led by the private sector and what actions should be under the government's leadership? Actions to consider may include recovery from loss, defensive actions, and offensive actions.
>
> Diplomatic Response vs. Military Response
>
> Should the government prioritize a military or diplomatic response to the attack? How do we involve international partnerships with allies like South Korea, Japan, Australia, and Europe? What about international partnerships with Russia or China, or international organizations like the United Nations?

Additionally, this message is accompanied by several documents that may assist your team in preparing its policy response alternative recommendations for the NSC:

- Preliminary Report on Moonrok Attacks
- Order of Suspension of Trading on "MajorBank Corporation"
- Joint Security Awareness Report
- US Times article

Good luck.

Department of Homeland Security
Preliminary Report on Moonrok Attacks
May 26, 2014

Summary

The Department of Homeland Security is taking the lead in the investigation into an ongoing cyber attack that began on May 18, 2014. The attack started with escalating distributed denial-of-service (DDoS) attacks targeting US and Republic of Korea (ROK) financial institutions, followed by the emergence of destructive malware disrupting critical systems and requiring costly and logistically challenging replacement of hardware. The attack is currently affecting trading platforms in every major US financial institution across every US exchange and is impacting the ability of exchanges to clear and settle transactions of securities worldwide. Analysis of affected computer systems indicates that equipment malfunction was caused by a piece of malware called 'Moonrok' after a word embedded in its code.

Background

• *The US, Japan, and ROK carry out a routine military exercise.*
On 05/18, South Korea and Japan joined the US in a two-day joint military drill off the southern coast of the Korean peninsula. The drill involved the nuclear-powered aircraft carrier USS George Washington docked at the port of Busan, guided-missile ships, anti-submarine helicopters, early warning aircraft, and B52 bombers making flights over South Korea. Planned in accordance with a newly signed and updated contingency plan "designed to counter future North Korean provocations," US and ROK officials have described the drill as a search and rescue exercise to improve readiness for humanitarian disasters.

• *US and ROK financial sectors are the victim of DDoS attacks by unknown actors.*
Beginning on 05/18, a still-unverified group waged DDoS attacks to overwhelm financial-industry websites with traffic from hijacked computers. The attack flooded bank websites with 10 to 20 times more Internet traffic than normal, rendering them unavailable to consumers and disrupting transactions for hours at a time over a period of several days. The nature of this attack is sophisticated enough that even the largest of the financial institutions are finding it difficult to defend against.

• *Attacks evolve from disruptive to destructive.*
New attacks emerging on 05/23, with the introduction of the 'Moonrok' malware, sought to destroy data and take over or shut down financial networks that provide accurate pricing information and run trading platforms. Unlike viruses that aim to hit as many targets as possible, this one appears designed to cripple computers on specific networks identified by the culprits. Moonrok appears to be exclusively targeting companies in the financial sector and involve inject vectors that are previously unseen, fully-autonomous, and widely undetectable.

• *US financial sector significantly affected.*
By 10:00 AM on 05/23, every major financial institution was reporting computer irregularities in their trading platforms and massive trading disruptions. Citing exigent and unprecedented circumstances, the Securities Exchange Commission suspended trading on many Fortune 100 companies, including "MajorBank Corporation." The inability of exchanges to price securities and clear and settle transactions affected every US exchange market, some suffering a record 10% loss in value. By the end of the day, every US market had voluntarily halted trading before the normal closing bell.

• *North Korea claims responsibility.*
On 05/26 as a "show of force," the North Korean government claimed responsibility for the crippling attacks on U.S. financial institutions. They cite recent joint U.S., Japan, and ROK military exercises as motivation for retaliation. While these claims cannot be proven, North Korean officials released a block of I.P. addresses targeted in the attack on Pastebin, a website often used by hackers to claim responsibility for attacks. While these addresses could only have been gathered by the perpetrators of the attack, DHS continues to investigate. Additionally, it is unlikely that North Korea has the capability to create malware of the level of sophistication of Moonrok.

• *State Department mobilizing diplomatic resources.*
While not directly involved in the investigation, the State Department is working closely with DHS and the Department of Defense to coordinate requests for information sharing with other governments. The Secretary of State and the ambassadors to China and the UN are being briefed on the situation regularly in preparation for possible diplomatic action. Additionally, China's leadership has offered to act as a mediator in any potential conflict on the Korean peninsula, an act that has the potential to greatly strengthen the future of US and China's diplomatic relationship.

• *All options are on the table.*
Military as well as diplomatic options were weighed at a high level White House meeting this week, including possible retaliation and counterattacks against self-identified attackers, North Korea. Overall, the financial services industry is still split over whether a response should take on a more forceful role. Some argued that any response should go after the hackers, while others cautioned that offensive action could lead to retaliation, additional attacks against the banks, or unforeseen consequences. Other options include government action in the form of complaining through diplomatic channels.

• *Private sector engagement.*
Bank officials are asserting that financial firms have spent millions of dollars responding to the attacks and that they can't be expected to fend off attacks from a foreign government without violating existing US domestic laws. A number of affected financial institutions would like the government to let the private sector block the attacks or even take down the network of computers mounting attacks.

Analysis

• *Attacks appear to be for sabotage.*
Previous DDoS attacks proved to have been cover for looting bank accounts and stealing customers' or employees' personal information, but there's no evidence so far that the latest attack has included theft. It appears that this time, the attackers' aim is not espionage but sabotage. Most attacks against American companies—especially those coming from China—have been attempts to obtain confidential information, steal trade secrets, and gain competitive advantage.

• *Attacks are distributed and appear to be from somewhere in Asia.*
The attackers are using a network of tens of thousands of infected computers running corporate websites, coming from computers that could have legitimate reasons to communicate with the banks. Roughly half of those computers are overseas and out of the reach of US law enforcement. Although pinpointing a specific source of the attacks is tricky, some believe that China—itself the victim of multiple computer attacks—may have played a role. There is no conclusive forensic evidence, because by design, Moonrok covers its tracks by erasing data on computer hard drives. We are still not certain exactly where the attacks are coming from, or whether they are state-sponsored or the work of hackers or criminals, but the source seems to be somewhere in Asia.

• *Threat may not be limited to financial sector.*
Moonrok poses an ongoing threat to national cybersecurity. Moonrok's ability to spread via network connections and USB devices could result in widespread computer infections, meaning that critical infrastructure could be at risk. If the financial industry, which spends more on Internet security than any other industry and has its largest and most extensive defenses, can't handle this, it is unclear whether any critical infrastructure industry can.

• *The attacks may not be over.*
Cybersecurity and data storage companies believe that additional infections involving Moonrok remain a possibility. Interdependencies between telecommunication and financial sectors require that operations not be segregated from a company's internal communications network, the primary method of infection. While the immediate focus is on work replacing the hard drives of tens of thousands of its PCs, finance executives are unsure that the internal communications networks can't be used to hit again.

Conclusions

Moonrok poses the single biggest threat to US cybersecurity witnessed to date. Stopping Moonrok and mitigating its damage will take a concerted effort from both public and private entities. In what is regarded as the most destructive act of computer sabotage to date, the malware erased data—documents, spreadsheets, emails, files—on three quarters of PCs of exchanges, financial institutions, trading platforms, and financial regulators. The challenge will be managing our nation's offensive and defensive capabilities requiring a very broad engagement across the private sector.

At the moment, DHS cannot identify the attacker conclusively. However, indications are that this is very likely a state-supported attack, with significant evidence pointing to the involvement of North Korea. DHS will coordinate further with the Department of State, the Department of Defense, and intelligence services to develop more information on the origin of the attack.

UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION
May 23, 2014

In the Matter of

MajorBank Corporation,

File No. 912-1

ORDER OF SUSPENSION OF TRADING

It appears to the Securities and Exchange Commission that there is a lack of current, accurate, and adequate information concerning the securities of MajorBank Corp. because of potential market manipulation, and the inability of exchanges to clear and settle transactions of securities across multiple exchanges.

The Commission is of the opinion that the public interest and the protection of investors require a suspension of trading in all securities the above-listed company. Therefore, it is ordered, pursuant to Section 12(k) of the Securities Exchange Act of 1934, that trading in the securities on the above-listed company are suspended from 2:45 p.m. EST on May 23, 2014 through 11:59 p.m. EST on June 6, 2014.

By the Commission.

Klara Jordan
Assistant Secretary

Joint Security Awareness Report (JSAR-14-912-01A)
Moonrok/ Malware (Update A)
Original release date: May 23, 2014 | Last revised: May 26, 2014

Overview

"Moonrok," is an information-stealing malware that also includes a destructive module. Moonrok renders infected systems useless by destroying the BIOS as well as data overwriting the Master Boot Record (MBR), the partition tables, and most of the files with random data. Once overwritten, the data are not recoverable.

Based on initial reporting and analysis of the malware, no evidence exists that Moonrok specifically targets industrial control systems (ICSs) components or U.S. government agencies.

According to multiple cybersecurity and ICS companies, Moonrok has three primary functional components:

- Dropper—the main component and source of the original infection. It installs a number of other modules.
- Wiper—this module is responsible for the destructive functionality of the malware.
- Reporter—this module is responsible for reporting infection information back to the attacker.
- After the initial infection, Moonrok spreads via network shares to infect additional machines on the network. Multiple cybersecurity companies first detected Moonrok on May 23, 2014, and estimates infections existing worldwide are limited to only few companies (less than 100).

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT and US-CERT for tracking and correlation against other incidents.

Impact

Because of the highly destructive functionality of the Moonrok "Wiper" module, an organization infected with the malware could experience operational impacts including loss of intellectual property (IP), disruption of critical systems, and damage requiring costly and logistically challenging replacement of hardware. Actual impact to organizations may vary, depending on the type and number of systems impacted.

The US Times (May 26, 2014)

North Korea Claims Responsibility for Devastating Cyber Attack

The North Korean government on May 26 claimed responsibility for a series of crippling attacks on U.S. financial institutions, and experts say that current evidence supports the veracity of these claims.

On the morning of May 23 a trickle of traders began reporting computer irregularities in their trading platforms. By 10:00 AM, the levy had broken and reports from every major financial institution and securities exchange indicated massive trading disruptions -- it was clear that a critical problem, impacting all U.S. financial markets, had occurred.

After a record 10% plunge in nearly every exchange market, the Securities Exchange Commission suspended trading on many Fortune 100 companies, including "MajorBank Corporation," before the scheduled close of business on May 23. Initial reports from the SEC indicated that an unprecedented cyber attack on the U.S. financial markets had been perpetrated by assailants using previously unknown malware called "Moonrok." Government official have been unable to say who initiated this assault on the U.S. economy and why.

The answer to these questions may have just been offered by the perpetrators themselves. In a forceful statement issued Monday morning, Kim Jong-un, the supreme leader of the Democratic People's Republic of Korea, claimed responsibility for the attacks and condemned U.S. arrogance and imperialism for instigating the assault.

After Jong-un's remarks, North Korean officials released blocks of I.P. addresses on Pastebin, a Web site often used by hackers to claim responsibility for their attacks. The officials claimed that these I.P. addresses belong to computers that they infected with the Moonrok malware.

North Korea's claim for responsibility for the attacks come after a week of escalating distributed denial-of-service (DDoS) attacks and other threats of retaliation for recent joint U.S., Japan, and Republic of Korea military exercises held around the Korean peninsula from May 18 to 19.

The now familiar threats leveled by North Korea in response to periodic military exercises included threats of preemptive strikes and assertions that the 1954 armistice has been invalidated. In addition, the Supreme Command of the North Korean military said, "we will put on the highest alert all the field artillery units, including strategic rocket units and long-range artillery units, which are assigned to strike bases of the U.S. imperialist aggressor troops in the U.S. mainland."

On May 20 North Korea renewed warnings to the United States of a "horrible disaster" resulting from the recently concluded military exercise and put its troops on alert. The United States is "wholly accountable for the unexpected horrible disaster" that was coming to its "imperialist aggression forces," a North Korean military spokesman said.

In a separate statement, Jong-un said, "[U.S. leaders] must bear it in mind that reckless provocative acts would meet our retaliatory strikes and lead to an all-out war of justice for a final showdown with the United States." Jong-un said that he will not beg for peace and will protect his nuclear-armed nation against all enemies with strong self-defense measures.

In response to questions over the decision to publicly take credit for the largest and most damaging cyber attack in history, Jong-un responded that the show of force was to "demonstrate North Korea's power as the greatest cyber warrior, even greater than the might of its nuclear strength."

Though a large scale cyber strike against the U.S. does not fit neatly with the threats levied by North Korea, the country has lashed out online before. After new U.N. sanctions and the March 2013 joint military exercise, the South Korean financial sector was hit with DDoS attack later attributed to North Korean hackers.

North Korea's latest announcement comes after some experts previously speculated that Pyongyang may initiate an attack on the U.S. economy, inspired during Dennis Rodman's recent visit with Jong-un. John Junper, a former member of the Wall Street Warbucks professional basketball team who accompanied Rodman on his recent visit to North Korea, told the US Times about an exchange he overheard during an official dinner in January.

"Rodman looked over to Kim [Jong-un] and said, 'Man, if you really want to win in the U.S. you've got to take down Wall Street,'" Junper said. "I thought he was hassling me and my old team, but after the banks all went down. . . Well I just don't know."

The Cyber 9/12 Student Challenge

Intelligence Report II

Instructions

Your team will take on the role of experienced cyber policy experts working for the Cybersecurity Directorate of the National Security Staff. The date is now Friday May 30, 2014, and it has been one week since the introduction of the 'Moonrok' malware significantly affecting US national security. The president needs information on the full range of policy response alternatives available to respond to the new developments in this crisis, and your team has been tasked with developing policy recommendations to pass on to the National Security Council and the President. To do so, you will apply your understanding of cybersecurity, law, foreign policy, and security theory and practice to synthesize useful policy measures from limited information.

This packet contains fictional information on the background and current situation of a major cyber attack on the United States. The attack takes place in May 2014, and the scenario presents a fictional account of political and economic developments leading up to the cyber incident. Teams are restricted to facts in the following pages and prior intelligence reports for the purpose of formulating your response.

Keep in mind that you will use the fictional scenario material presented to perform only one task:

• **Oral Policy Brief:** Prepare a ten-minute oral presentation outlining four possible policy response alternatives and recommending one to the National Security Council.

Before you begin, keep these tips in mind as you are reading and considering your policy response alternatives:

• *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) 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 competition is for competitors 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.

Note: All materials included are fictional and were created for the purpose of this competition. Some of the details in this fictional simulated scenario have been gathered from various news sources and others have been invented by the authors. All scenario content is for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

From: National Security Staff, Cybersecurity Office
Re: Cyber attack affecting financial sector | UPDATE

May 30, 2014

At the request of the National Security Council's Principal's Committee, the NSS Cybersecurity Directorate is contacting your team to solicit national policy solutions to respond to the situation. Given the unprecedented nature of this attack, the President is seeking to assemble a range of possible policy response alternatives before determining a course of action to take.

Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of each proposed policy response alternative before recommending the one best course of action. When generating each of your four policy response alternatives, the National Security Staff requests that you address all the following potentially conflicting interests.

Offensive Cyber Capabilities vs. Defensive Cyber Capabilities

In its call to action in response to the attack, should the government prioritize strengthening capabilities of offense or defense?

Covert Response vs. Overt Response

In deciding to pursue potential countermeasures, should the government act in secret, or reveal US Cyber capabilities to the world?

Additionally, this message is accompanied by several documents that may assist your team in preparing its policy response alternative recommendations for the NSC:

- Report Update on Moonrok Attacks
- US Times article
- US Department of State Office of the Legal Advisor Opinion

Good luck.

Department of Homeland Security
Report Update on Moonrok Attacks
May 30, 2014

Summary

The Department of Homeland Security investigation into the 'Moonrok' cyber attacks that began on May 23, 2014 has concluded that while the malware spread pervasively, it only resulted in wiping a relatively small set of targeted machines. It appears that the memory-wiping mechanism was simply a way to remove evidence of earlier incursions, during which hackers might have stolen intelligence or intellectual property. While analysis of the attack is ongoing, various industry Information Sharing and Analysis Centers (ISAC) and other responsible groups have met to share information in a joint effort to step up protections against future attacks.

Background

• *Financial Markets Recover.*
By the time markets opened on Tuesday 05/27, appearances of the 'Moonrok' malware greatly decreased in number and effect. Disruptions to critical systems have been fully addressed and replacement of hardware across the US financial sector has been viewed as impressively successful. Affected trading platforms in every major US financial institution across every US exchange have recovered and exchanges are facing no issues clearing and settling transactions of securities worldwide.

• *Private Sector Calls for Government Restraint.*
After the swift and successful recovery of the financial sector, industry leaders from every major financial institution have come forward, giving interviews and writing Op-Eds demanding more cyberdefense spending. The sentiment from the private sector is trending on social media and in major news outlets as a call for less military instigation that led to retribution against the private sector. One bank executive is quoted saying he "resents governments acting illegally and riling each other up, when the net effect is governments attacking each others' private sectors."

• *IP Theft Revealed.*
Shortly after the attacks, a major defense contractor, and member of the Defense Industrial Base program, contacted the Department of Defense to report that after analyzing the attacks, parts of the 'Moonrok" malware were created by its employees. Without disclosing sources and methods, NSA and the Department of Defense have concluded that the defense contractor was a victim of cyberespionage action and that the technology was stolen. Further, these actions have been positively attributed to hacker crews in China on behalf of the PLA. To protect the sources and methods of this attribution, the government will not pursue domestic prosecution.

• *Diplomatic Efforts Stall.*
On 05/27, the US Times publicly reveals a leaked memorandum from the US Government to a defense contractor acknowledging the development of offensive cyber weaponry that made up part of the 'Moonrok' malware. The leak also identifies hacker crews in China acting on behalf of the PLA as the perpetrators of the cyberespionage. On 05/28, the Chinese and North Korean governments announce their outrage at the accusations revealed in the leaked memo. To date, the US Department of State has not been able to reach a principal in the Chinese Government who is willing to meet with members of the US Government by phone or in person. It is unclear whether China has formally withdrawn its offer to facilitate communication on the Korean Peninsula, or if the internal politics within the Government and political party in China have created an internal stalemate regarding a possible response. It appears for the moment that all diplomatic efforts with China are effectively on hold.

• *Legal Advisor Declares No War.*
On 05/30, the US Department of State Office of the Legal Advisor issues an opinion that precludes the use of force amounting to an armed attack, meaning acts of war. The opinion does, however, leave the door open for countermeasure operations designed to compel the responsible State to cease and desist from its pattern of conduct. Shortly after the opinion is released, it is rumored that the President has ordered the creation of countermeasures amounting to a "proportional response in cyber."

Analysis

• *Intelligence Sources Point to China.*
Without disclosing sources and methods, NSA and the Department of Defense have concluded that the Chinese provided the stolen 'Moonrok' capability to the North Koreans and encouraged them to launch the attacks to provide cover for an escalated cyberespionage action on behalf of the PLA. It appears that the Chinese are using the North Koreans as a proxy for their own purpose under the cover of destruction/disruption to comprehensively map out all systemic vulnerabilities in the financial sector for development of future capabilities for truly crippling economic attacks.

Conclusions

While Moonrok was the most destructive act of computer sabotage to date, the coordination of the private sector represents the most successful response in history. Bringing stability to the financial sector illustrates the flexibility, subject-matter expertise, and coordination of the private sector and shows resilience to a single cyber attack. As the focus shifts from reaction to a crisis to moving forward to protect, defend, and deter against future attacks, the challenge will be managing our nation's offensive and defensive capabilities requiring.

The leaked memorandum has damaged existing sources and methods and stunted any diplomatic way forward. Additionally, these public disclosures of classified operations has renewed public calls for transparency and accountability for actions in cyberspace creating new barriers as the government explores offensive and defensive options for deterrence.

LEGAL OPINION ON AVAILABLE RESPONSE OPTIONS TO MOONROK CYBER ATTACKS ON UNITED STATES FINANCIAL SYSTEM

MEMORANDUM OPINION FOR THE
Secretary of State

The Moonrok attacks represent the single biggest threat to US cybersecurity witnessed to date.

Having considered the extent of destruction of IT infrastructure and the financial loss, we conclude that the United States is facing cyber operation which constitute a use of force of a lesser gravity than an armed attack.

States bear responsibility for their internationally wrongful acts pursuant to the law of State responsibility. Under International Law Commissions Articles on State Responsibility and the customary law of state responsibility, States are responsible for acts committed under their instructions, directions, or control. The available intelligence suggests that perpetrators of the attacks have acted as an agent of a state and their actions can qualify as those of a state.

In light of the abovementioned we conclude that under the international law doctrine of countermeasures, the United States may respond to these hostile cyber acts and resort to countermeasures which have to comply with the requirements of necessity and proportionality.

The available options are either diplomatic protests, economic sanctions or cyber or kinetic actions bellow the armed attack threshold.

In light of the current ambiguity regarding the origins and the full extent of the damage caused by the attack, we suggest that the countermeasure must be designed to compel the responsible State to police the cyber infrastructure and activities on its territory.

It is important to bear in mind that countermeasures shall be terminated has soon as the responsible State has complied with its obligations in relation to the internationally wrongful act. However, countermeasures remain available when the internationally wrongful act is but one in a series of wrongful acts. In a case of a series of DDoS attacks it is be reasonable to conclude that further attacks will take place, and the injured State may take countermeasures to induce the responsible State to desist from its pattern of conduct.

The US Times (May 28, 2014)

CHINESE LEADERSHIP DECRIES US ALLEGATIONS IN LEAKED EMAILS

Representatives of the People's Republic of China and Democratic People's Republic of Korea on May 28 held a joint press conference condemning leaked allegations by the United States Department of Defense that Chinese hackers supplied the North Korean government with the tools for its May 23 cyber-assault on U.S. financial markets.

An email from the Department of Defense to a long-running defense contractor surfaced on May 27 and revealed explosive new details of those responsible for the recent financial mayhem. The email explains that key portions of the computer code language initializing the "Moonrok" attacks originated from a cyber-weapon that U.S. contractors were developing for the U.S. Cyber Command.

The DoD, in the email, acknowledged that the code provisions used against the U.S. were stolen from what were thought of as secure servers used by contractors.

As to who stole the cyber atom-bomb, the email indicates that Chinese hackers employed by the People's Liberation Army breached contractor security and "made off with a draft of the weapon's coding."

The response from Beijing was nearly immediate. In the early hours of May 28, Chinese and North Korean spokesmen denied that the weapon used in the attacks originated in China. "The PLA does not undertake espionage activities in the United States through computer hacking or other nefarious means," the Chinese spokesman said. "To allege otherwise is a brazen assault on China's position in the international community and clearly indicates that the United States wants to bring China into its ongoing conflict with North Korea."

The North Korean spokesman also decried the U.S. allegations. "The grand North Korean Republic did not receive any knowledge or expertise from China when preparing to bring the American imperialists to their knees. Our military is strong and prepared to carryout further retaliations for any new imperialist aggressions committed against North Korean or Chinese sovereign interests."

The North Korean spokesmen closed the press announcement by declaring all relations and communications with the United States to be terminated immediately and permanently until such time that the United States admitted its violations of international law and paid restitution for its attacks against North Korea.

While the Chinese spokesman did not make similar declarations, he followed the North Korean spokesman out of the press conference. It remains unclear whether China will follow North Korea in severing diplomatic ties, but one unnamed source at the US Department of State is quoted as saying, "we can't even get them on the phone."

The Cyber 9/12 Student Challenge

Intelligence Report III

Instructions

Your team will take on the role of experienced cyber policy experts working for the Cybersecurity Directorate of the National Security Staff. The date is now Monday June 2, 2014, and events over the weekend have presented additional challenges requiring your team to present recommendations immediately to the National Security Council and the President. To do so, you will apply your understanding of cybersecurity, law, foreign policy, and security theory and practice to synthesize useful policy measures from limited information.

This report contains fictional information on the background and current situation of a major cyber attack on the United States. The attack takes place in May/June 2014, and the scenario presents a fictional account of political and economic developments leading up to the cyber incident. Teams are restricted to facts in the following pages and prior intelligence reports for the purpose of formulating your response.

Keep in mind that you will use the fictional scenario material presented to perform only one task:

• **Oral Policy Brief:** Prepare a ten-minute oral presentation outlining four possible policy response alternatives and recommending one to the National Security Council.

Before you begin, keep these tips in mind as you are reading and considering your policy response alternatives:

• *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) 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 competition is for competitors 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.

Note: All materials included are fictional and were created for the purpose of this competition. Some of the details in this fictional simulated scenario have been gathered from various news sources and others have been invented by the authors. All scenario content is for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

From: National Security Staff, Cybersecurity Office
Re: Cyber attack affecting financial sector | IMMEDIATE ACTION REQUIRED

June 2, 2014

At the request of the National Security Council's Principal's Committee, the NSS Cybersecurity Directorate has contacting your team to deliver national policy solutions responding to this crisis situation. Given the dangerous and pressing nature of this attack, the President is seeking to assemble a range of national policy solutions on a course of action to take.

Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of each proposed policy solution before recommending the one best course of action. When generating your policy response alternatives, the National Security Staff requests that you consider the following questions.

> How does the United States recover its footing in the international community?
>
> What conditions (e.g., future damage) would be required for the President to justify the use military force against a nation state? non-state actor?

Additionally, this message is accompanied by an "URGENT Report Update" on Moonrok Attacks that may assist your team in preparing its policy response alternative recommendations for the NSC.

Good luck.

Department of Homeland Security
FLASH Report on Moonrok Attacks
June 2, 2014

Background

• *US Launches 'BotNet' Inoculation Campaign.*
Though it was not part of your recommendation, the US has used the unprecedented Mookrok attacks to justify launching a new, and unannounced, "active defense" cyber capability, codenamed 'Operation Panacea.' The US created software that inoculates effected machines eliminating known malware that contribute to botnets. The covert injection of this new capability was intended to greatly reduce the global span of botnets that played a key role in the success of the Moonrok malware attacks.

• *Hackers of the World Unite*
Operation Panacea is almost immediately discovered by the major computer security companies and catches the US private sector completely unaware. Governments, private sector companies, and individuals within the US and abroad express outrage in the uninvited intervention of the US government into private computers. The international community was shocked by Operation Panacea's blatant violation of state sovereignty. Patriotic hackers conducting DDoS attacks, transnational criminal organizations conducting cybercrime, and state sponsored hacker crews conducting espionage from all over the world begin calling for unified retaliation against critical infrastructure in the United States.

• *'Moonrok' Malware Copycat Attacks Cascade.*
Hackers using retooled versions of the Moonrok malware and fresh exploits immediately begin carrying out attacks against US critical infrastructure. In only a few days, the finance, telecommunication, and energy sectors are devastated. The damage requires among other things, difficult hardware replacement for many previously unforeseen dependencies. Further complex and unidentified dependencies on finance, telecommunication, and energy are forcing the CEO of every US company to examine the viability and sustainability of core business functions.

• *Real-World Damages Mount.*
As failures cascade across US critical infrastructure, large-scale disruption in power, internet, and telecommunications occur. In the ensuing communications blackout federal and local authorities have difficult coordinating emergency response efforts. Credit cards, ATMs, and point of sale systems stop operating in most locations. Without essential services, panic spreads. Hospitals report an expected loss of life, the energy sector is unable to estimate when power will be restored.

Conclusions

The attacks keep coming. The damages are consistent with the aftermath of a massive terrorist attack or act of war. The physical effects of these cascading failures are expected to only get worse.