On June 15, 2013, the Atlantic Council's Cyber Statecraft Initiative, with Science Applications International Corporation (SAIC), held the first student competition devoted to high-level policy recommendations for day-after responses to a major cyber attack.

Held at American University's School of International Service, the competition brought together more than sixty-five students—from undergraduates to PhD candidates—organized into nineteen teams and representing seventeen universities. In addition, twenty-one experts drawn from the top ranks of the US Department of Defense, US Department of State, White House, and leading cyber security firms participated as judges.

Congratulations to ECIR's very own, Colonel William E. Young, Jr., Josephine Wolff and Evann Smith for winning the "Best Written Brief."

Please visit the Atlantic Council's website to see more about the competition (http://www.acus.org/content/inaugural-student-competition-features-day-after-responses-major-cyber-attack) and read the winning brief below.

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

The Atlantic Council's Cyber 9/12: Student Challenge Washington, DC June 15, 2013

Josephine Wolff, PhD Student
Engineering Systems Department, MIT

William E. Young, Jr. (Col, USAF), PhD Student
Engineering Systems Department, MIT

Evann Smith, PhD Candidate
Government Department, Harvard University

This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research

About the authors:

Evann Smith is a PhD Candidate in the Department of Government at Harvard University. Her research focuses uprisings, leaderless movements, and the emergence of protest as a self-organizing system. Central to this focus is an examination of communication technology, social media, and their impact on—and use within—social networks. She has conducted fieldwork in Egypt and resided in Cairo prior to beginning her studies at Harvard.

Josephine Wolff is a PhD student in the MIT Engineering Systems Division, working with David Clark in the advanced network architecture group on issues of online identity, cybersecurity, and Internet policy. She holds an AB in mathematics from Princeton University and has interned at the White House Office of Science and Technology Policy, the Center for Democracy & Technology, and the Microsoft Technology Policy Group.

Colonel William E. Young, **Jr**. is currently a PhD Candidate in the Engineering Systems Division at Massachusetts Institute of Technology's School of Engineering, where he is a member of the Complex Systems Research Lab. He is also an Air Force research liaison at Lincoln Laboratories in the Cyber System Assessments Group. His specialization area is cyberspace strategy, technology and systems. His research focuses on applying system-theoretic approaches to improve operational design, red teaming, and campaign-level mission assurance in cyberspace.

Background

The Atlantic Council's Cyber 9/12 Student Challenge competition consisted of 19 teams drawn from various universities across the United States. The teams were composed primarily of graduate students from a variety of disciplines. Both the basic scenario that guided development of the policy memorandum and the follow-on scenario that guided the afternoon policy brief are attached. We were late in forming our team due to being unaware of the competition. The ECIR notification was instrumental in our being able to not only form a team, but compete. MIT Political Science Professor Ken Oye agreed to act as our faculty coach. Our team was composed on two MIT PhD candidates from the Engineering Systems Division and one Harvard PhD Candidate in Political Science. The team members' mix of both technical and policy expertise seemed to work well.

Execution

Our approach to crafting the policy memo was largely based on trying to strike a balance between providing enough specificity to guide a potential recommendation to policy makers without going into too much technical detail. The competition guidelines imposed a 2500 word limit on the policy memo. We focused on providing a baseline technical remediation policy recommendation that could be supplemented with one of three additional increasingly aggressive options. Our winning submission is attached.

The first round of briefings consisted of each of the 19 teams presenting the analysis captured in their policy memo to a panel of three judges. Each team was allotted 15 minutes for their presentation. At the end of the time the judges consulted and scored the teams. After scoring each team completed a short question-and-answer period with the judges. During this time, the judges provided critiques and feedback to the team on the quality and content of their presentation.

After the first round, each team was provided an updated intelligence scenario from which to plan their afternoon oral presentation. Teams had approximately 4 hours to prepare for the afternoon round. During the afternoon round each team presented to a different panel of judges. The guidelines for presentation and feedback remained the same as the morning session.

At the completion of their second presentation, teams were free to watch other teams' presentations. After all of the presentations were complete, Gen. Hayden, former Director of the Central Intelligence Agency and National Security Agency, provided a keynote address as scores were tabulated. At the end of the day the winning teams were announced.

Lessons Learned

In general, the experience was both positive and educational for our team. One of the most important lessons was the value of having a team that could address both the policy impacts and the technical demands of the particular scenario with equal clarity and specificity. This

allowed our team to not only consider a potentially broader range of options, but provide recommendations that were feasible from both a technical and policy perspective. Additionally, the challenge of making an oral presentation without any type of electronic or visual aids was an excellent exercise, sharpening both our thought and oral argument processes. Another extremely valuable aspect of the competition was receiving direct feedback from panel members with first-hand experience coping with policy challenges similar to those in the scenarios. For example, our afternoon panel included a former member of the national Security Council who specialized in cyber policy.

Summary and Recommendations

Competing in a national collegiate cyber policy competition was both personally stimulating and professionally rewarding. We recommend that ECIR sponsor at least one team in future competitions.

Cyber 9/12 Student Challenge Policy Brief

Evann Smith (Harvard), Josephine Wolff (MIT) & Bill Young (MIT)

SECTION 1: INTRODUCTION

The Cobalt malware, which has shut down thirteen oil refineries in the past week, requires an immediate, direct, and discriminate policy framework to both mitigate the damage to U.S. infrastructure and respond in a whole of government approach to this sophisticated, highly targeted attack on the United States. The National Security Council is challenged with (1) developing a technical and economic mitigation strategy which will clean the infected systems, stop the malware's spread, and minimize economic impact; while (2) responding to future threats from as of yet unknown perpetrators (that intelligence reports have linked to Russia).

The vital national interests relevant in crafting this response include avoiding worsening relations with Russia, stabilizing the U.S. economy, deterring future attacks on the homeland while simultaneously increasing critical infrastructure resilience, and maintaining public confidence in the nation's ability to defend itself against emerging threats. The central cyber policy question the National Security Council must address is therefore: How do we work productively with private sector partners to resume critical operations as quickly and safely as possible and maintain the U.S. peoples' confidence that their infrastructure is secure, while simultaneously conveying that this is an unacceptable attack on our nation which will not be tolerated?

SECTION 2: OVERVIEW OF PROPOSED POLICY ALTERNATIVES

In light of the unusual nature of the attack, there is no clear precedent for response. We have identified four basic policy alternatives (PA1 - 4). Each policy alternative is consistent with U.S. laws and policies and is designed to ensure mitigation of the present damage, as well as prevention of future infections and disruptions of America's critical infrastructure.

PA-1: Ongoing Technical Analysis and Remediation

This response involves downplaying suspicions that Cobalt may have been state-sponsored and instead addressing technical aspects of the underlying exploited refinery vulnerabilities and the resulting economic consequences. The baseline mitigation actions specified in this PA are included in all future response scenarios, as well, though the policy statements vary. This PA deliberately avoids placing blame or "shaming" states such as Russia to prevent worsening of strained relations or acting impulsively on uncertain intelligence.

Policy Statement: The United States Government, in coordination with public and private utilities owners, is vigorously investigating the technical causes of disruption and will subsequently seek long-term improvement in overall resilience of the nation's critical infrastructure networks.

Policy Actions: (1) Provide government assistance in scrubbing all affected machines and replacing infected hardware, where necessary, to resume refinery operations as quickly as possible; (2) Monitor other refineries and potential public and private target networks for irregular activity using out-of-band verification methods; (3) Recommend and assist industry to extend defensive measures for critical infrastructure networks by deactivating USB ports and terminating remote access procedures; (4) Form a public-private working group to establish security standards for critical infrastructure networks, as well as auditing regimes with regular updating and revision; (5) Invest in new defensive technologies and strategies for protecting critical networks and increasing their resilience; (6) Monitor price spike in refine oil products, focusing on high risk areas including areas immediately surrounding the affected refineries, as well as the interior of the country served via pipeline; (7) Implement an Emergency Fuel Waiver in the affected areas should an inability to meet the need for refined product occur; and, (8) Manage public concern about the incident by assuring the public of swift and effective mitigation measures, and easing fears about rising fuel prices.

PA-2: Cyber Criminal or Terrorist Act

This policy alternative incorporates the objectives of PA-1, but also publicly identifies a responsible *non-state sponsored* transnational third party, motivated by ideology or financial gain. This response also entails engaging in diplomatic talks to strengthen international response to cyber crimes and attacks. This PA views the situation as a diplomacy problem. It asserts a minimal level of state responsibility and aims to use the incident as a means for strengthening international cooperation around addressing collective action to disrupt and deter extremist and criminal network activity in cyberspace.

Policy Statement: The United States Government, in coordination with international partners, will pursue and bring to justice the responsible criminal or terrorist parties and strengthen diplomatic relations in order to more effectively police and prevent future cyber attacks.

Policy Actions: (1) All actions in PA-1; (2) Identify responsible group(s) and bring them to justice, (3) Call for international summit on the cross-jurisdictional pursuit of malevolent actors in cyberspace, and, (4) Institute international partnerships between relevant law enforcement and intelligence gathering agencies to police and prosecute cybercrime and terrorism.

PA-3: State-Sponsored Cyber Attack

This PA incorporates the mitigation efforts of PA-1, but unlike PA-2 it publicly identifies the Cobalt malware as a deliberate cyber attack, directly sponsored or conducted by a nation state. This PA is the most aggressive. However, it is also most firmly rooted in the norms and rules of state diplomacy by viewing cyberspace as a new domain in which attacks may be conducted. Rather than focus on the domain, this PA responds to the effects of the attack.

Policy Statement: The U.S. will determine the responsible nations and hold them accountable using all instruments of power, including military force if required.

Policy Actions: (1) All actions in PA-1, (2) Invoke Article 4 of the North Atlantic Treaty and issue a demarche through the United Nations, (3) Ensure responsible nation makes financial restitution to affected U.S. industries, (4) Demonstrate U.S. resolve to respond decisively to any

and all attacks on its soil, regardless of the means used to deliver the attack, and, (5) Direct Defense Department to prepare military courses of action to inflict a commensurate level of damage on the responsible nation, through either physical or cyber attacks on critical infrastructure.

PA-4: Hybrid Option

This policy option applies PA-1 overtly, pursuing mitigation objectives and only publicly announcing an ongoing U.S. investigation. Without publicly assigning blame for the attack, PA-4 goes further covertly. It involves conducting further analysis and investigation with the goal of determining Russia's level of involvement and culpability. If and when that level is determined, the U.S. will then initiate covert action in combination with direct, high-level diplomacy to compel Russia to cease their actions and adhere to activities consistent with global and U.S. norms and interests.

This PA views responding to the Cobalt incident as a series of interconnected problems, which must be delicately handled. It postpones publicly assigning blame until attribution can be performed with greater certainty and aims for the establishment of U.S.-Russia bilateral norms addressing electronic attacks on critical infrastructure by avoiding escalation of U.S.-Russia tensions while compelling Russia to cease current actions and deterring them from repeating similar acts in the future. This PA is a measured response that buys time while implementing the short-term fixes identified in PA-1.

Policy Statement: The United States Government, in coordination with public and private utilities owners, is vigorously investigating the technical causes of disruption and will subsequently seek long-term improvement in overall resilience of the nation's critical infrastructure networks.

Policy Actions: (1) All actions in PA-1, (2) Collect further intelligence to determine Russia's level of involvement, (3) Initiate diplomatic talks with Russia to address tensions surrounding the production and export of shale oil, (4) Increase the level of covert hard power as certainty of attribution increases, and, (5) Direct Defense Department to prepare military covert courses of action to inflict a commensurate level of damage on the responsible nation, through cyber attacks.

SECTION 3: ANALYSIS AND IMPACT OF POLICY RESPONSE ALTERNATIVES

PA-1: Ongoing Technical Analysis and Remediation

- Purpose: Identify and remediate technical vulnerabilities while maintaining confidence of American public in critical infrastructure security and minimizing economic impact.
- Expected Outcomes:
    - Technical vulnerabilities and economic consequences identified and remediated across affected industries;
    - Affected industries restrained from retaliation;
    - U.S. public reassured;
    - No escalation of international tensions.

- Justification: The U.S. Government has a responsibility to promote the common good by maintaining reliable, resilient critical infrastructure, and unilateral actions by affected companies would likely violate U.S. law, while acting on hasty conclusions drawn from uncertain intelligence could jeopardize crucial international relationships.

Analysis:
The strengths of PA-1 lie in its focus on devoting resources to dealing with the immediate technical and economic aspects of the problem, allaying fears of the public, and avoiding the escalation of international conflict. The primary weakness of this PA is its failure to address intelligence report information about Russian involvement, and the exclusion of any punishment or deterrent measures aimed at the responsible parties.

The most significant opportunities associated with this response are the potential to address long-term critical infrastructure resilience in a meaningful manner and strengthen the often tenuous public-private partnership governing critical infrastructure security. The most significant threat to PA-1 is the possibility of emboldening Russia and other nations to launch similar attacks in the absence of any clear consequences for such actions.

PA-2: Cyber Criminal or Terrorist Act

- Purpose: Disable responsible group and increase capacity of governments to combat cyber attacks.
- Expected Outcomes:
    - Mitigate technical and economic impacts;
    - International investigative partnership surrounding cybercrime and terrorism.
- Justification: This response is justified by the U.S. Government's responsibility to protect its citizens, as well as by international norms of bilateral assistance and cooperation in dealing with sub-nation group violations of norms.

Analysis:
The strength of this PA is its focus on international partnerships for increasing capacity to combat cyber criminals and terrorists. It is less intrusive than PA-3, though more aggressive than PA-1. The weakness of this PA is its requirement of international support and disregard of intelligence on Cobalt's state-supported origins.

PA-2 provides an opportunity for developing international cyber norms and reversing the deteriorating United States-Russia relationship. If Cobalt originated from terrorist or criminal activity within the nation, then partnering with Russia to deal with the threat might present an opportunity for a public shared win, the success of which might permeate other areas of bilateral interest.

The critical threat to this PA is an uncooperative state. Reluctance on the part of a government will present a significant problem maintaining domestic support for the policy. Additionally, if the attacks were in fact state-sponsored, attributing the attack to a transnational network organization avoids consequences for the responsible state which may embolden it, and others, to undertake similar actions in the future.

PA-3: State-Sponsored Cyber Attack

- Purpose: Punish the responsible party and deter future attacks by reaffirming U.S. hard power.
- Expected Outcomes:
    - Mitigate technical and economic impacts;
    - Demonstrate the dire consequences of cyber attacks on the U.S.
- Justification: Cyber attacks on U.S. critical infrastructure may be viewed as tantamount to acts of war[1] and may therefore elicit military response as part of the government's responsibility to protect the nation.

Analysis:
The strength of this PA is that it clearly demonstrates strength and national resolve to protect critical infrastructure against all forms of attack and acts as a powerful deterrent to any actors considering similar such actions.

The weakness of this policy alternative is that it requires both domestic and international support and, if the United States responds in kind, it may reveal potential technical exploits that might have been used in the future. Additionally, this PA likely exacerbates the underlying Russian economic problem.

The greatest opportunity associated with this policy alternative is its potential to serve as a global deterrent for actors considering attacks on American critical of structure. It may also serve as an impetus for high-level discussions to generate international norms for cyber war.
The most serious threat associated with this policy alternative is its high potential for worsening relations. This PA may lead to a new Cold War. Short of such extreme outcomes, it may still lead to a rise in Russian nationalism or further destabilization of the country.

PA-4: Hybrid Option

- Purpose: Deal with the short-term national security problem while identifying the level of nation-state culpability and punishing the responsible party.
- Expected Outcomes:
    - Mitigate technical and economic impacts;
    - Strengthen US critical infrastructure resilience;
    - Responsible parties identified and deterred from launching future cyber attacks.
- Justification: The U.S. Government has a responsibility to promote the common good by maintaining reliable, resilient critical infrastructure, protect its citizens and borders, and maintain strong foreign relations even in the absence of compelling, concrete evidence.

---

[1] U.S. Department of State. "International Law in Cyberpace." Remarks by Legal Advisor U.S. Department of State Harold Hongju Koh at the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, September 18, 2012. Available from http://www.state.gov/s/l/releases/remarks/197924.htm.

Analysis:
The strengths of this policy alternative are that it addresses the short-term technical vulnerabilities, as well as the perpetrators and their underlying motivations. The approach is measured and gradual, and does not constrain the entire range of options available to the government in the future. It avoids public "shaming" of Russia and the risk of rapid escalation presented by PA-3.

The weaknesses of this approach are that it requires time, as well as coordination of a complicated combination of overt and covert maneuvers. Should technical or economic effects cascade, immediate overt action may be necessary.

The primary opportunity this alternative presents is that of addressing the larger Russian economic root problem and establishing a new norm of trust that can be leveraged in future cases of unacceptable state behavior in cyberspace.

The threat to this policy alternative is that the covert action or high-level back-channel communications may be leaked at some point, leading to demands by the U.S. public for some type of overt action against Russia. Additionally, it is possible that the United States will be unable to convincingly determine the level of Russian state involvement in the attack.

SECTION 4: RECOMMENDED POLICY RESPONSE ALTERNATIVE

These policy alternatives were evaluated against a variety of criteria to determine which should be pursued. PA-4 was selected on the basis of its flexibility and potential for creating the greatest long-term gain for the United States, our allies, and even Russia.

The policy is based on several significant assumptions. First, baseline technical and economic mitigation measures enumerated in PA-1 will correct the disruption in a reasonable amount of time. Second, no further attacks will occur in the immediate future. Third, Russia does not desire a new Cold War or similarly poor relations with the U.S. This means that if given an opportunity, Russia will solve their long-term economic problem in a manner that come that does not come at the expense of its relationship with the U.S.

Given these assumptions, this policy best satisfies the concerns of a variety of different stakeholders, including the U.S. public, the larger international community, and the private industry actors who own and operate critical infrastructure networks. It includes all essential technical and economic mitigation measures to reassure the public, but does not initiate a controversial, and potentially violent, international conflict. The recommended response is necessary, distinct, and proportional, drawing on diplomacy and conflict resolution measures short of all-out war. Finally, this policy offers effected private sector industries the assistance needed to restore their operations without threatening their independent operation. Therefore, this policy is most likely to win the cooperation of all involved parties, while promoting the U.S.'s role as a powerful and responsible international player.

The Cyber 9/12 Student Challenge

Intelligence Report I

Instructions

Your team will take on the role of the Cyber Policy Working Group, a team of experienced cyber policy experts working for the Cybersecurity Directorate of the National Security Staff. The date is June 15, 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. 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 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 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, 2,500 words maximum, 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.

• **Oral Policy Brief:** Prepare a fifteen-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.

The Cyber 9/12 Student Challenge

Competition Instructions

The Cyber 9/12 Student Challenge requires student teams to respond to a simulated major cyber attack that evolves over the course of the competition. Competition teams will write a cyber policy brief and have the opportunity to deliver two oral presentations to a panel of expert judges. The final score will be determined by combining the score of a written cyber policy brief submitted before the competition, the score from an oral presentation based on the prepared cyber policy brief, and the score from an oral presentation responding to new intelligence revealed the day of the competition.

For response, teams must produce up to four potential policy response alternatives that counteract, mitigate, and/or disrupt the damage and continued threat of the current cyber attack. When planning responses, teams should keep in mind that policy response alternatives should go beyond purely technical solutions, and may include legal, political, and diplomatic response alternatives. Teams should consider a variety of offensive and defensive response alternatives that take into account the roles of state, private sector, and international actors. In particular, teams should consider the role of cooperation between different actors necessary to achieve desired policy outcomes.

Written Policy Brief (maximum 2,500-words**)**

Your team must prepare a detailed written document that analyzes the implications of the cyber attack for various actors (such as government agencies, private sector stakeholders, and average citizens) and its relation to national cybersecurity policy. Each team should propose up to four policy response alternatives that address the cyber attack and briefly discuss the advantages and disadvantages associated with each policy response alternative. The competition is not meant to test a team's ability to spot issues, but rather to analyze and explain the reasons supporting the best cyber policy recommendation. Submissions that exceed the maximum word limit will be penalized.

The following outline is strongly suggested for structuring the prepared policy brief.

I. Cyber Policy Question Presented

Identify and clearly explain the cyber policy question facing the National Security Council.

II. Proposed Policy Response Alternatives

Identify and clearly explain the policy response alternatives the team has formulated to answer the cyber policy question facing the National Security Council. It may be helpful for teams to clearly list the four alternatives (E.g., Alternative 1, Alternative 2, Alternative 3, Alternative 4). Please do not include more than four alternatives.

III. Analysis and Impact of Policy Response Alternatives

Analyze the strengths, weaknesses, opportunities, and threats of each of the policy response alternatives. Each policy response alternative should describe the purpose of the proposed policy action, the expected outcomes, and the theoretical justification.

IV. Justification for Recommended Policy Response Alternative

Select one policy response alternative to recommend to the National Security Council. Compare and contrast the selected alternative and provide an explanation that justifies your selection.

Oral Policy Brief (15-minute presentation**)**

Building on the policy response alternatives in the written policy brief, design an oral presentation delivered to a panel of judges representing the National Security Council. Responses should draw on the analysis of the policy response alternatives from the written brief, while touching on the strengths, weaknesses, opportunities and threats outlined in the written policy brief. In addition, you must highlight one policy response alternative as your team's preferred recommendation to the National Security Council and explain the teams reasoning and justification. Teams will be kept advised of the time using a "green-yellow-red" system of cards. At the five-minute mark a staff member will display a green card to the team presenting; at the one-minute mark a staff member will display a yellow card; and at the time limit a staff member will display a red card. A penalty will be assessed for teams exceeding the time limit.

Teams will have until 11:59 p.m. Friday June 7, 2013 to submit their written cyber policy brief via e-mail to cyber912@acus.org. Late submission will be penalized. If there are any questions or problems, please contact Jason Thelen (JThelen@acus.org) at the Atlantic Council.

• *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.

Note: All materials included are fictional and were created for the purpose of this competition. The details in this fictional simulated scenario are for academic purposes and are not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

Setting the scene…

The following scenario presents a fictional cyber incident involving the United States and Russia. The subsequent background is based loosely on the following facts:

- The advancement in US shale gas production has contributed to lower gas prices around the world and has put the US in the position to become a major natural gas exporter.
- American energy companies are lobbying the US government for the opportunity to export liquefied natural gas, but so far the only deals that have been passed are with countries the US has free trade agreements with and the United Kingdom. Debate continues over the potential export of natural gas to other European markets.
- Nations, such as Russia, that are heavily reliant on gas and oil to finance their economy are being negatively affected by lower gas prices. It has been speculated that Russia will enter a recession in the near future. While this is only partly due to oil and gas prices, a further decline in prices could significantly increase the likeliness of a recession in Russia.

Recent events leading up to June 2014

In the past decade advances in the extraction of shale gas in the United States have had a dramatic effect on the energy landscape worldwide. As the US has increased its energy self-sufficiency through these new technologies, it has demanded less of the world supply and created a buyer's market for the rest of the world. The European market in particular has seen a dramatic decrease in prices as nations importing gas are placed in a stronger bargaining position relative to those exporting it. An additional factor in this situation is the surprising move by the White House to ease restrictions on the export of shale gas, particularly to Europe. This development has come after successful lobbying by American energy companies over those who claimed that the export of natural gas would hurt the US production.

Since the change in policy the Department of Energy has approved a flurry of export deals between US companies and European partners. In 2013 the first such approval was given to Sabine Pass in Louisiana, and has quickly been followed by approval for several more

companies to ship liquefied natural gas around the world. Within the next couple of years, US gas will be responsible for heating millions of Western European homes.

Some political observers see this move as related to the cooling off of US-Russia relations that has taken place since the end of the "Reset" policy in 2012. The change in US policy followed an unproductive G20 Leaders' Summit in September 2013 in which cooperation between the US and Russia on issues such as Syria, Iran, North Korea, and human rights remained elusive.

Complicating the tensions has been the recent decline of the Russian economy into recession. With the federal budget closely linked to oil and gas revenues, rumors have started to surface in Russia that this decline is primarily due to the US influence in the European market. The US and US energy companies have been major supporters of planned gas pipelines from Central Asia that would increase European independence from Russian energy suppliers, and now the US exports of liquefied natural gas that will commence soon are driving down the price and demand for Russian gas contracts. The state controlled media has reported that some Russian officials suspect a conspiracy by the US and other countries to prevent Russia from experiencing its own shale gas boom. Cited in these conspiracy theories is the January 2014 withdrawal of MobileX from a joint venture with Russian state oil company Nosensoft to provide technical assistance in the extraction of shale gas from Siberia.

While the Winter Olympics in February served as a distraction from the economic and political challenges plaguing the international community, these unresolved issues are bound to resurface now that the games have ended. It seems that US-Russian relations will not experience a second reset as tensions continue to grow. The return to hostile politics is already becoming a reality as increasingly anti-American rhetoric is expressed in the Russian media and among pro-Kremlin groups on the Internet.

From: National Security Staff, Cybersecurity Office
To: Cyber Policy Working Group
Re: Cyber attack affecting energy industry

June 15, 2014

As you are aware, in the past week thirteen oil refineries have been taken off line due to a dangerous piece of malware known as "Cobalt." This malware has the potential to threaten not only oil refineries and energy infrastructure, but also a much wider range of SCADA systems involved in industry and critical infrastructure. The Department of Homeland Security is spearheading the criminal investigation into the attacks with the help of all relevant government agencies, in addition to several private security firms retained by the energy companies.

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.

This message is accompanied by several documents to assist your team in preparing its policy response alternative recommendations for the NSC:

- Initial report from the DHS lead investigator

- Article from the US Times describing the refinery outage

- ICS-CERT initial report on Cobalt malware

These documents should provide you with enough details on the incident to formulate your policy response alternative recommendations.

Good luck.

Department of Homeland Security
Preliminary Report on Refinery Outages

Summary

The Department of Homeland Security is taking the lead in the investigation into the refinery outages that occurred beginning on June 10, 2014. The outages are currently affecting thirteen oil refineries in four different states. Analysis of the refineries' computer systems indicates that equipment malfunction was caused by a piece of malware called Cobalt.

Details

• *Infected targets belong to three companies:* The thirteen confirmed affected refineries belong to three different companies: MobileX (4 refineries, ~1,560,000 bbl/d capacity); Steves 88 (6 refineries, ~1,138,000 bbl/d capacity); and Arrow (3 refineries, ~891,000 bbl/day capacity). Both MobileX and Arrow are considered part of the five "supermajor" energy companies and are in the Top 10 of the Fortune 500 corporations. Steves 88 was spun off from CannoSteves in 2012, but CannoSteves was formerly considered the sixth "supermajor". All companies are based in the United States.

• *Attacks were closely coordinated:* Malfunctions began to occur at all refineries during a 48-hour window beginning on June 10, 2014. The exact activation method of the malware remains uncertain, although at least one refinery was connected to via a serial port server from an IP address in Russia immediately preceding the attack.

• *Analysis indicates advanced design:* Reverse engineering and analysis of the Cobalt malware is being coordinated by ICS-CERT. They have already determined that Cobalt is an extremely sophisticated piece of malware, with a modular design similar to Stuxnet and Shamoon. Analysis is incomplete, but researchers from Kaspersky Labs have identified at least three zero-day exploits used by the malware as well as four different unique rootkits targeting programmable logic controllers from different vendors.

• *Code scrubbed of identifying elements:* The authors of the Cobalt malware were careful to remove any identifying comments or language from most of the code. However, at least one subprogram contained comments in Russian. The FBI and NSA are working to try to establish the author of the code based on the comments and other distinguishing code features.

• *Intelligence suggests involvement of Russian hacker:* The FBI reports that intelligence obtained from surveillance of a known Russian "black hat" chat forum several months ago indicate a former Russian military hacker may have been involved with the production of code targeting some of the programmable logic controllers affected by the attack under contract by an unknown buyer. Information on the hacker's background and experience in the Russian military is limited. The FBI is comparing its intelligence to information from other sources.

• *Identification of infections difficult:* Investigators have yet to determine a way to scan for systems infected with Cobalt. As a result, all SCADA system operators need to remain on alert for irregularities in operations.

• *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 Russia and the UN are being briefed on the situation regularly in preparation for diplomatic action.

Analysis

• *Strong indications of state support:* While analysis is ongoing, the complexity of the malware strongly indicates state support in the development of Cobalt. The sophistication of the design rivals Stuxnet, and there are other indications the code required a resource intensive development process.

• *Attack appears highly planned and targeted:* The geographic distribution of the infections supports the theory that the attack specifically targeted these companies and that physical security was breached in order to deliver the code. DHS is investigating the possibility that the attacker may have employed agents on the ground in those areas to infiltrate facilities or compromise staff members with access to supervisory control and data acquisition (SCADA) systems.

• *Threat not limited to refinery systems:* Cobalt poses an ongoing threat to national cybersecurity. Cobalt's ability to spread via network connections and USB devices could result in widespread computer infections beyond the refineries, similar to the spread of Stuxnet. Critical infrastructure in particular could be at risk because of Cobalt's ability to cause malfunctions in SCADA equipment.

• *Defensive strategy complicated:* The sophistication of the Cobalt malware could pose challenges for the defense of domestic networks and systems. Defense of national networks could require the involvement of the Department of Defense or other federal agencies to coordinate efforts and provide resources. Private companies may be tempted to employ offensive measures to deter further attacks based on limited information of Cobalt's source and design.

Conclusions

Cobalt poses the single biggest threat to US cybersecurity witnessed to date. Stopping Cobalt and mitigating its damage will take a concerted effort from both public and private entities.

At the moment, DHS cannot determine a clear motive for the attack, nor can it establish the identity of the attacker. However, indications are that this may be a state-supported attack, with some evidence pointing to the involvement of Russia, Russian citizens, or Russian-speaking individuals. 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.

The US Times (June 14, 2014)

Multiple refinery outages threaten summer fuel prices

Since at least Wednesday, more than ten oil refineries in four different states have shut down in response to equipment problems, taking almost one-fifth of the United States' refining capacity offline. While the cause of the outages remains unknown, the loss of refining capacity will almost surely create headaches for a variety of petrochemical consumers.

The refineries, located in Texas, Louisiana, Mississippi, and California, are owned by several different companies. Though the affected companies are not disclosing the extent of the outages, the Times has confirmed that refineries owned by MobileX, Arrow, and Steves 88 are among those affected. These companies are facing millions of dollars in lost revenue for each day their refineries aren't operating, but beyond the financial damage the effects of this disruption in production are difficult to predict, especially for the country's fragile economic recovery.

The effects of such a mass refinery outage are unknown, but the situation during Hurricane Katrina does share some similarities. Roughly 1.9 million barrels per day of refining capacity in the Gulf Coast was taken offline during the storm, in addition to the shutdown of offshore oil platforms and regional pipelines due to weather and electricity problems. Oil companies lost millions of dollars due to production disruptions, while fuel prices across the US suffered due to supply and transport problems.

It is unlikely that the current refinery outages will have the same impact, but if reports on the affected refineries are true, the current refining capacity taken offline is close to 3 million barrels per day. This is a problem because the US has a typical utilization rate of around 95% of refinery capacity, meaning any long-term outage could result in significant supply problems. However, with over 27 days worth of finished gasoline in circulation in the US market according to statistics from the Energy Information Agency, it is unlikely that shortages would become critical for months even with the refineries offline.

In the short-term, the most visible effect of the outage will be higher fuel prices for businesses and consumers. Gasoline prices have already risen several cents around the US as the busy summer travel season ramps up. In California, where several refineries have been affected, consumers have already seen price jumps as large as 25 cents. Drivers around the country will almost certainly face additional price increases in the weeks ahead as the oil companies and the government craft a response plan.

While economists and analysts continue to focus on the economic damage resulting from the refinery outage, the investigation into causes is just beginning to ramp up. According to one anonymous official, the government has already created an investigatory team to assist the affected companies, but their response has been delayed by the secretiveness of the energy companies involved. Worried about the effects on stock prices, the energy companies have yet to reveal any details on the outages to government or the public.

While few potential clues as to the cause of the outages have been revealed, it is rumored that computer security firms McAfee and Kaspersky Labs have been retained in the cases. This raises the troubling possibility that the outages resulted from a cyber attack or malware infection. If so, many more refineries and other facilities could be at risk. However, sources from McAfee, Kaspersky Labs, and the oil companies still refuse to comment on their involvement in the ongoing incident.

ICS-CERT
ICS-ALERT-13-XXX-XX
Initial Report on Cobalt Malware Targeting Energy Industry

Summary

ICS-CERT is investigating the cyber attacks against oil refineries in the southern and western United States. Initial analysis of the malware used in the attack, nicknamed Cobalt, indicates a sophisticated operation using multiple variants to infect different systems at three separate energy companies. The modular structure of the malware and significant number of previously unknown vulnerabilities used in the code indicate extreme technical proficiency on the part of the attacker and possible state support for the operation.

Overview

Beginning on June 10, 2014, the three affected companies (MobileX, CannoSteves, and Arrow) began experiencing subtle irregularities to refinery operations caused by malfunctioning elements of the supervisory control and data acquisition (SCADA) system, including programmable logic controllers (PLCs). Technicians did not examine the SCADA systems as the source of the malfunctions until equipment damage forced refineries to idle production, delaying the discovery of the malware for several days.

The affected companies contacted McAfee and Kaspersky Labs for technical support on June 13, 2014. Recognizing the sophistication of the malware involved, ICS-CERT was contacted the next day to coordinate the investigation.

Preliminary forensic analysis of the malware in conjunction with McAfee and Kaspersky Labs indicates a two-part modular structure. The first module infects PCs operating SCADA system control software or connected via a local network to the SCADA control system, with variants for both Linux and Windows devices. Once inside the SCADA network, the first module installs an additional vendor-specific PLC exploit module that causes equipment malfunction.

Similar to the Stuxnet malware, initial infection likely occurs via USB drive, though the investigation also indicates use of serial port servers to gain access to refinery networks remotely. Further infections can occur via network shares and SQL databases. However, unlike Stuxnet, the use of multiple vendor-specific PLC exploit tools makes Cobalt a more robust threat to industry. The investigation has already determined that the malware has deployed modules affecting Siemens, Honeywell, GE, and Rockwell Automation equipment.

Infection Risk

The danger posed to industry and critical infrastructure by Cobalt cannot be understated. Given the adaptive nature of the software, all operators of SCADA systems should be on alert for indications of system infection or malfunction. ICS-CERT is working closely with security firms to identify the complete set of SCADA vendors and products potentially affected by Cobalt.

While Cobalt is believed to have been deployed as part of a carefully targeted attack, the vulnerabilities utilized in the malware could also allow the software to spread to a far wider range of PCs in the same manner as Stuxnet. Organizations should be careful to isolate industrial production and control networks from connections to outside networks, computers, and portable drives.

Additionally, researchers are still working to develop a tool to identify machines infected by Cobalt. Until such a tool is developed, operators should treat all external network connections to infrastructure and industrial control systems as infection risks and act accordingly.

Mitigation

As ICS-CERT is only in the initial stages of reverse engineering and analyzing this malware, SCADA system vendors and operators are advised to closely monitor the ICS-CERT website for additional information as it becomes available.

ICS-CERT strongly encourages all operators of SCADA systems, regardless of vendor, to immediately take defensive action to secure their systems using defense-in-depth principles. ICS-CERT also reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures. However, organizations are reminded to be mindful of legal restrictions on the use of countermeasures in responding to attacks and malicious infections, especially when retaining outside security firms to assist them.

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

The Cyber 9/12 Student Challenge

Judging Instructions

Competition Process

At the beginning of each round the team will enter the room. Before they begin their oral presentation, the timekeeper will explain the rules to the team and judges. The teams will then have 15 minutes to present their policy recommendations to the judges.

The teams will NOT be permitted to use any presentation aids (e.g., PowerPoint, props, handouts, and posters) during their oral presentations. Additionally, judges will NOT be allowed to ask questions during the presentations.

The timekeeper will hold up a yellow sign when the team has 5 minutes left and a red sign when there is 1 minute remaining.

Once the team finishes their presentation the timekeeper will instruct them to take a seat. The judges will have 5 minutes to score the team's presentation on the scorecards provided, according to the standards outlined below. Judges should NOT consult with each other or competitors to decide scores. Any questions about scoring should be directed to the timekeeper. When the scoring period is over the timekeeper will collect the scorecards.

Once the scorecards have been collected the judges will have 5 minutes to provide feedback to the team. It is during this time the judges may ask questions and give teams feedback.

After the 5 minutes of feedback, the timekeeper will ask the team to leave the room. Judges will have 10 minute break before the next round.

Team Awards

- *Best Oral Presentation* – Judges should nominate teams from both morning and afternoon sessions who show an advanced mastery of the oral briefing. Judges are free to nominate multiple teams.
- *Best Teamwork* – Judges should nominate teams from both morning and afternoon sessions who show strong collaborative skills and present a cohesive brief as a team. Judges are free to nominate multiple teams.
- *Most Creative Policy Response Alternative* – Judges should nominate teams from both morning and afternoon sessions who show nuanced, plausible, policy response alternatives that also show a high degree of creativity and originality. Judges are free to nominate multiple teams.

Understanding of Cyber Policy

- [4 points] The team demonstrated a superior knowledge of cyber conflict policy issues, named specific actors, and applicable instruments
- [3 points] The team demonstrated a comprehensive knowledge of cyber conflict policy issues, identified appropriate actors and instruments
- [2 points] The team demonstrated a sufficient knowledge and general understanding of cyber conflict policy
- [1 point] The team demonstrated a limited knowledge of cyber conflict policy issues

Identification of key issues

- [4 points] The team successfully identified and fully responded to critical cyber conflict policy issues posed by the scenario
- [3 points] The team identified and responded to the main policy issues posed by the scenario
- [2 points] The team identified few of the salient cyber conflict policy issues posed by the scenario or failed to respond fully to some of the policy issues identified
- [1 point] The team referenced few general cyber conflict policy issues and/or focused on issues not associated with the scenario

Analysis of policy response alternatives

- [4 points] The team's suggested policy response and alternatives effectively addressed the scenario, and the team thoroughly analyzed the tradeoffs involved with other policy alternatives
- [3 points] The team's suggested policy response and alternatives only partially addressed the scenario and/or some sections lacked sufficient analysis or justification
- [2 point] The team's analysis of policy response alternatives is not properly grounded in cyber conflict related theory and/or did not appear to be relevant to the competition scenario
- [1 point] The team's suggested policy response was not properly supported by analysis and/or the team did not appear to analyze other policy response alternatives

Structure and Organization

- [4 points] The team clearly and concisely presented policy response alternatives and fully communicated the analysis supporting their recommended response and all alternatives
- [3 points] The team effectively presented their policy response alternatives and recommended response, but did not fully communicate the analysis of alternatives and/or justification of their recommended response
- [2 points] The team adequately presented their policy response alternatives and recommended response, but the presentation lacked coherent analysis of policy response alternatives
- [1 point] The team's presentation lacked coherence and conciseness, hindering the effective communication of policy responses to the intended audience

Originality and Creativity

- [4 points] The team offered original, creative, and innovative solutions to the scenario that go beyond existing canonical cyber conflict policy literature
- [3 points] The team exhibited a distinctive approach to the scenario, but largely drew on well-known solutions
- [2 points] The team relied on repeating well-known policy solutions from obvious sources with little adaptation
- [1 point] The team approached the scenario by only drawing on material provided, offering nothing original