



# The Cyber 9/12 Student Challenge

## Intelligence Report I

### INSTRUCTIONS

Your team will take on the role of experienced cyber policy experts on the National Security Council Staff assembled to jointly advise the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism. This packet contains fictional information on the background and current situation involving a major cyber incident affecting critical infrastructure in the United States and abroad. The attacks notionally take place in late August 2018. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The President of the United States needs information on the full range of policy options available to the US regarding this incident. Your team has been tasked with developing **four** policy recommendations to pass on to the President and the National Security Council.

You are to consider as facts the following pages for formulating your response.

### You will use the fictional scenario material presented to perform three tasks:

- 1. Written Policy Brief:** Write a 500-word brief discussing the key elements and national security concerns that the President of the United States must understand. The written task is meant to not only test your team's ability to summarize the scenario, but more importantly to explain the reasons and confidence levels behind your analysis of the key issues and implications of the ongoing cyber incident.
- 2. Oral Policy Brief:** Prepare a ten-minute oral presentation outlining four possible policy options and recommending one to the National Security Council.
- 3. Decision Document:** Teams will also be required to submit a "decision document" accompanying their oral presentation at the beginning of the competition round. The "decision document" will be maximum two single-sided pages (one double-sided page) in length, outlining the team's policy response options, decision process, and recommendations. The teams should note that the document is not intended to summarize every detail of the recommendations, but to help the judges follow the oral presentation, and the judges will be given only 2 minutes to read it before the presentation begins.

**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 possible, observed, or reported as written. 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 and domains (e.g. private sector, military, law enforcement, diplomatic) and incorporate these insights along with cybersecurity.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct policy response option 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 Council Staff**  
**Re: Cyber Attack Against Critical Infrastructure**  
**Date: 29 August 2018**

The date is Tuesday, August 29, 2018, and a major cyber incident is occurring that could affect US national security. The Cybersecurity Directorate of the National Security Council is contacting your team to solicit policy options to respond to the unfolding situation.

Given the unprecedented nature of this incident, the President is seeking to assemble a range of possible policy response options before determining a course of action at the next National Security Council meeting on Thursday, August 31, 2018 at 9:30 a.m.

To do so, you will apply your understanding of cybersecurity, law, foreign policy, and security theory to synthesize useful policy measures from limited information. 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 Council requests that you consider the following potentially conflicting interests. These are provided as suggested starting points and are not meant to limit your policy responses.

- **Immediate Response vs. Delayed Response**  
What actions should be considered, if any, if there exists a possibility of U.S. involvement? What actions should be taken immediately after the incident versus those that should be taken later? How should leverage be maintained?
- **Government Response vs. Private Sector Response**  
What actions taken in response to the reports and incidents should be led by the private sector and what actions should be under the government's leadership? Actions to consider may include public acknowledgements, preventive and preemptive defensive actions, and offensive actions.
- **Explicit Deterrence vs. Implicit Deterrence**  
Should the U.S. respond openly to deter future attacks? Will the absence of a response – or a covert response – embolden future attackers? How should either option be messaged, if at all? What consideration should be given to escalatory potential of a response meant as deterrence?
- **Direct Response vs. Indirect Response**  
If action is to be taken, should it be a direct or indirect response to the incident? Should those responding act in secret, or reveal their cyber capabilities? Should no action be taken?

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

- **Tab 1– Cyber Marque and Reprisal Act of 2018**
- **Tab 2 – New York Times News Story**
- **Tab 3 – SCMagazine US News Article**
- **Tab 4 – <http://www.realnewsfromasia.com/post>**
- **Tab 5 – JP Morgan Chase CEO Email Communications**
- **Tab 6 – Office of the Director of National Intelligence Memo (Exercise Secret)**
- **Tab 7 –SANS Internet Storm Center (ISC) Blog Post**

# One Hundred Fifteenth Congress of the United States of America

AT THE SECOND SESSION

*Begun and held at the City of Washington on Tuesday, the  
third day of January, two thousand and eighteen*

## Joint Resolution

Granting the consent of Congress to the issuance of letters of marque and reprisal to counter hostile cyber-attacks against critical infrastructures

Whereas an "unprivileged enemy belligerent" is defined as an individual who: has engaged in hostilities against the United States of America or its coalition partners; or has purposely and materially supported hostilities against the United States of America or its coalition partners;

Whereas terrorists, rogue states, foreign enemies, and other entities engaged in electronic and digital piracy and cyber-attacks upon the United States and its interests are considered, as such or comprised thereof, unprivileged enemy belligerents;

Whereas cyber-attacks by unprivileged enemy belligerents against critical infrastructures of the United States destroy or degrade critical infrastructures of the United States; and such that the perpetrators of cyber-attacks are actively aided and abetted by technical means using the Internet for their commercial gain or to harm the United States and its interests;

*Resolved by the Senate and House of Representatives of the United States of America in Congress assembled,*

### **SECTION 1. CONGRESSIONAL CONSENT.**

Congress authorizes the President of the United States to issue letters of marque and reprisal with respect to certain acts of cyber-attack upon critical infrastructures of the United States, and other similar acts of hostility committed in the future.

### **SECTION 2. AUTHORITY OF PRESIDENT.**

(a) The President of the United States is authorized and requested to commission, under officially issued letters of marque and reprisal, so many of privately equipped persons and entities as, in his judgment, the service may require, with suitable instructions to the leaders thereof, to employ

electronic eavesdropping and intelligence gathering, cyber-attack, and all electronic or digital means reasonably necessary to attribute, stop, disrupt, deceive, or otherwise render ineffective cyber-attacks conducted by unprivileged enemy belligerents outside the geographic boundaries of the United States and its territories, of any co-conspirator, and of any conspirator who are responsible for cyber-attacks, aggressions and depredations perpetrated against the United States or harms against persons and entities resident in the United States, or attacks in-progress but discovered or detected after January 3, 2018, and for any planned future cyber-attacks, aggressions and depredations or other acts of war upon the United States of America and her people.

(b) The President of the United States is authorized to place a money bounty, drawn in his discretion from the \$10,000,000,000 appropriated on April 1, 2018, in the Emergency Supplemental Appropriations Act for Response to Cyber-Attacks on the United States or from private sources, for the incontrovertible attribution, disruption, or cessation of cyber-attacks upon the United States critical infrastructure, under the authority of any letter of marque or reprisal issued under this Act.

(c) No letter of marque and reprisal shall be issued by the President to any entity not deemed to be sufficiently qualified by such means as a review of command, control, and execution capabilities by defense and intelligence agency experts; nor, without requiring the posting of a security bond in such amount as the President shall determine is sufficient to ensure that the letter be executed according to the terms and conditions thereof.

### **SECTION 3. RIGHT TO ALTER, AMEND, OR REPEAL.**

The right to alter, amend, or repeal this Act is hereby expressly reserved.

*Speaker of the House of Representatives.*

*Vice President of the United States and  
President of the Senate.*

# The New York Times

## Trump, Changing Course on “One China” Policy, May Start Trade War

By JOHN PERLEY JUL 16, 2018

BEIJING – President Trump is again straining the relationship with America’s most powerful rival. Returning to the stance he took upon his election to office, President Trump over the weekend publicly targeted the central basis for diplomatic relations between Washington and Beijing – known as the “One China” policy – as a “bad idea” and needing to be changed.

Under the decades-old policy, the United States severed diplomatic ties with Taiwan as part of its recognition of the People’s Republic of China. But in early December of 2016, Mr. Trump stunned officials across the globe by becoming the first president or president-elect to speak to a Taiwanese leader since at least 1979. While he eventually softened his position, he has over the past six months publicly touted his conversations with Taiwan, discussing possible trade and other issues.



Then on Sunday, he most sensitive of what the

*President Trump boarding Air Force One in Florida on Sunday. Mr. Trump’s reversal on Taiwan could mean a tougher negotiating position in Beijing on trade, North Korea and other issues. Credit Stephen Crowley/The New York Times*

reiterated that adhering to the One China policy may not be the most beneficial course of action for the United States. “I don’t know why we have to be bound by a One China policy unless it’s good for us,” he said in an interview with Greta Wall One America News Network.

In trying to use Taiwan that way, President Trump hit the

Chinese Communist Party calls its “core interests.” While Washington has not formally recognized Taiwan, President Trump’s continued conversations with the leadership of Taiwan has the Chinese using economic leverage to retaliate.

China has just backed out of a \$13 billion deal with Boeing to produce more planes this year,

mostly 737s that have become the workhorse of China's rapidly expanding airlines. The Global Times reported that China has switched orders to Boeing's European competitor, Airbus. This deal impacts the \$1.025 trillion forecast in the next 20 years for Chinese airlines purchasing American-made planes. Boeing (BA, -4.9%) stock continues to drop.

It seems President Trump's stance on the One China policy continues to backfire. The Chinese government has begun seizing manufacturing supplies and fining US companies for what it said were trade and licensing infractions.

Last week China sold a large portion of its holdings of Treasuries, pushing up interest rates in the United States. Its

holdings of Treasuries peaked at \$1.65 trillion in March 2014, declining to about \$1.2 trillion, said Brad Sezner at the Council on Foreign Relations.

President Trump's threats of a trade war may be the beginning of more than just a war of trade practices.

---

### Tab 3: SCMagazine US News Article



by Dan Marsters, Managing Editor



---

August 22, 2018

## Agricultural Bank of China target of a Distributed Denial of Service Attack



Agricultural Bank of China, one of China's largest and fastest growing banks with nearly US\$4 trillion in assets, suffered a massive Distributed Denial of Service (DDoS) attack over the course of 2 days, severely affecting the daily operations of the bank, disrupting interbank transactions, and affecting availability of funds to the Chinese public, across its 30,000 branches.



China has become the most targeted country for denial of service attacks, accounting for nearly 77 percent of all DDOS attacks last quarter, a slight uptick from the previous quarter, followed by the US which accounted for almost 13 percent of the attacks.

Researchers also spotted four main trends: the demise of amplification-type attacks, rising popularity of attacks on applications along with their increase in encryption usage, rising popularity in WordPress Pingback attacks and the use of IOT botnets to carry out DDoS attacks.

A new trend began in 2016, DDoS attacks launched via huge botnets made up of vulnerable IoT devices, of which Mirai is one example. "2016 was rich in noteworthy DDoS attacks against a broad range of targets, including Dyn's Domain Name System, Deutsche Telekom and some of Russia's largest banks," Kaspersky Lab North America Senior Vice President Richard Caravan told SC Media. While the full story is not currently known, a poorly secured internet of things (IoT) may be to blame.

Cyber 9/12 | Intelligence Report

---

*Disclaimer: The details in this fictional simulated scenario are for academic purposes only and are not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*



Caravan said it appears that cybercriminals are testing new tools, attack scenarios, and determining how victims can withstand them and also looking for opportunities to monetize DDoS attacks whenever possible. In order to combat the threats of the changing DDoS landscape, IoT manufacturers and developers need to work to better implement a security by design approach and to work with the security industry when creating and installing new products.

“This could include, for example, the capability to prompt password resets or to patch and distribute updates for software after a bug has been detected,” Caravan said.

He said the best approach to preventing attacks is to have a reliable anti-DDoS solution in place. “In addition, companies can migrate public resources to another IP address, adjust a firewall to fight SYN flood attacks and relocate business critical applications to the cloud or a separate public subnet,” he said.



TOPICS: DENIAL OF SERVICE ATTACK INTERNET OF THINGS BANKING

# US Starting Next World War?

## Botnets created from US malware involved in Agricultural Bank of China cyber-attack.

By Michael Dan

August 22, 2018



Diplomatic sources say the attack against the Agricultural Bank of China that lasted for two full days appears to have originated from the United States, according to South Korea's Yonhap news agency. US Intelligence organizations are likely to blame for a new kind of Internet of Things (IoT) weapon against China as the trade war between the two countries heats up.

The top-secret massive distributed denial of service attack (DDoS) that shut down the Chinese bank was a cover-up for US intelligence gathering activities. The Yonhap news agency interviewed diplomatic sources involved in the clandestine program called Trade Secrets. None of them agreed to have his name mentioned due to the highly sensitive nature of the operation. But sources say that China was just the first use of this cyber-attack and that other countries are next. Linksys executives deny involvement in the development of a US cyber weapon that targets their routers.

### promoted links from around the web

Recommended by Real News From Asia



---

## Tab 5: JP Morgan Chase CEO Email Communications

### Jamie Dimon

---

**From:** Jamie Dimon <jamie.dimon@jpmchase.com>  
**Sent:** Tuesday, August 28, 2018 06:45 AM  
**To:** Honorable John F. Kelly, DHS Secretary <dhssec@hq.dhs.gov>  
**Cc:** dhsexecsec@hq.dhs.gov

**Importance:** High

John - by now you know J.P. Morgan Chase has been under a massive, coordinated denial of service attack since early yesterday afternoon, affecting operations - particularly institutional transactions. The attack is starting to garner public attention, and my executive team is already receiving queries from major news orgs about the attack. I expect to release a public statement about our ongoing investigation and cooperation with the US government within an hour.

Our customer-facing systems have not yet been affected, but our individual and business retail customers are now increasingly affected by intermittent errors. I'm now looking at all my options – to include what we discussed at the White House concerning our rights to take action under the Cyber Marque and Reprisal Act of 2018. We agreed then to let you know if we were considering this extraordinary option. I'm doing so now.

I have requested activation of our support agreement with and the standing authorization of Bakatax – the first and only endorsed company for this action, to date. My team informed me they are the well-equipped to disable the systems conducting the attack. Their actions will commence at midnight tonight.

Also, while our investigation hasn't revealed an intrusion, my team is working with the FBI and the FS-ISAC to see if this is affecting others in the sector.

As you know, John, I have to consider my customers and our communities – and protecting my company so that we remain strong and can continue to be here for them is most important for me. I believe this action will give us all comfort and a clear signal of our strength. - Jamie

## JPMORGAN CHASE & CO.

---

James Dimon  
Chairman and Chief Executive Officer  
Direct: (212) 270-6001

**Tab 6: Office of the Director of National Intelligence Memo (Exercise Secret)**

**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
WASHINGTON, DC 20511**

August 28, 2018

MEMORANDUM FOR THE VICE PRESIDENT  
THE SECRETARY OF STATE  
THE SECRETARY OF DEFENSE  
THE ATTORNEY GENERAL  
THE SECRETARY OF HOMELAND SECURITY  
CHIEF OF STAFF TO THE PRESIDENT  
ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS  
ASSISTANT TO THE PRESIDENT FOR HOMELAND SECURITY AND  
COUNTERTERRORISM  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

SUBJECT: Memo on Questions Posed - Chinese Network  
Vulnerabilities

As agreed to during the Principals Committee meeting on August 26, 2018, I have completed my preliminary review of the political situation in China as a result of the degradation of elements of their banking infrastructure. Below is my assessment for your consideration.

Report to NSC Staff by The Director of the Defense Intelligence Agency, provided August 27, 2018:

On August 25, 2018, five days after the degradation of Chinese banking infrastructure, the President of the People's Republic of China, President Xi Jinping, made an extraordinary address on Chinese television accusing the US of perpetrating attacks against major banks, Chinese companies, and government agencies.

In his broadcast address President Xi did not specify details about the attack; however, he made a rare admission indicating the attacks initially halted some Chinese banking operations and continue to degrade services.

President Xi stated the attackers were able to exploit common open source software libraries developed, at least in part, by software

Cyber 9/12 | Intelligence Report

---

*Disclaimer: The details in this fictional simulated scenario are for academic purposes only and are not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

developers paid or coerced by the US government to deliberately undermine the integrity of the software. President Xi called out the US intelligence community by name, and stated this reinforces the Chinese Peoples' concerns about the security of US technology after Edward Snowden revealed confidential information about the National Security Agency.

#### Technical Assessment:

CIA and DIA analysts believe President Xi's comments are diplomatic posturing and concealing. Over the past half-decade, China has expended significant resources to essentially "expel" US technology from their critical infrastructure, to include their banking infrastructure.

Forensics experts with the DoD Cyber Crime Center (DC3) believe the most likely scenario based on what NSA and DIA analysts have read on Chinese tech blogs and intercepted communications is attackers likely compromised the banking infrastructure through a vulnerability in the Huawei routers' HTTP implementation. The only other product manufacturer known to be affected at this time is Linksys, and there is some speculation that Huawei is using software code stolen from Cisco when they owned the Linksys brand. (Acquired by Belkin in 2013.)

AgBank China's network is built on these routers, particularly at its 30,000 rural branches which often use 4G modems and microwave to connect to the Internet.

The apparent DDoS it suffered earlier this week may have been due primarily to the size of the attack surface, rather than a concerted attack against the bank itself. We believe vulnerable equipment was then joined into a botnet used to conduct a distributed denial of service attack against JPMorgan Chase and Co. (JPMC) operations that commenced on August 27. AgBank's network infrastructure participated in the attack against JPMC, and were themselves further overwhelmed.


Reports intercepted from AgBank staff indicate a significant cleanup effort was undertaken to remove malware and disable remote HTTP. This effort has not yet concluded, and may take many more days.

#### ODNI Assessment:

There exists a small window of time - approximately 48 hours - to leverage this vulnerability for intelligence gathering on AgBank infrastructure elements. Since this is a commodity attack - easily obtained and used by low skilled attackers - there would exist some modicum of plausible deniability and existing equities would be preserved that might otherwise be used and lost.

## Tab 7: SANS Internet Storm Center (ISC) Blog Post

Threat Level: **GREEN** Handler on Duty: **Brad Duncan**

 **SANS ISC InfoSec Forums**

Keyword, Domain, Port, IP or Header

Email  Password

[Sign Up for Free!](#) [Forgot Password?](#)

August 22, 2018

### Shellshock + Busybox = Busyshock?

A new network worm is making the rounds, as reported to the Storm Center by several sources, that seems to be using an exploit that targets the same bug in Bash as Shellshock. This variant takes advantage of a quirk in the way busybox HTTP server processes Cookies. Busybox is used in a number of home routers and IoT devices. This one seems to be hit-and-miss.

**UPDATE 1:** It looks like this malware also tries to spread by guessing default passwords. What did we tell you kids about not changing defaults? There are some odd ones we don't normally see. Add these to your Nexpose/Nessus/Hydra lists I guess.

backdoor:backdoor

servicetech:servicetech

root:#bigguy1

analyst:analyst

administrator:100

**UPDATE 2:** We're hearing that the Shellshock exploit code only seems to work against Linksys devices. Take this with a grain of salt, for now.

**UPDATE 3:** Our handler, Xavier Martens, pointed out that at least one of the malware samples looks an awful lot like a modified version of one of the public forks of the Mirai botnet, with a small modification for this new Shellshock method.

Past posts on Shellshock:

<https://isc.sans.edu/forums/diary/Shellshock+keeps+on+giving/19197/>

<https://isc.sans.edu/forums/diary/Update+on+CVE20146271+Vulnerability+in+bash+shellshock/18707>

<https://isc.sans.edu/forums/diary/Shellshock+More+details+released+about+CVE20146277+and+CVE20146278+Also+Does+Windows+have+a+shellshock+problem/18769>



# The Cyber 9/12 Student Challenge

## Intelligence Report II

### INSTRUCTIONS

Your team will take on the role of experienced cyber policy experts on the National Security Council Staff assembled to jointly advise the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism. This packet contains fictional information on the background and current situation involving a major cyber incident affecting critical infrastructure in the United States and abroad. The incident notionally takes place in late August and early September 2018. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The President of the United States needs information on the full range of policy options available to the US regarding this incident. Your team has been tasked with developing **four** policy recommendations to pass on to the President and the National Security Council.

You are to consider as facts the following pages for formulating your response.

**You will use the fictional scenario material presented to perform two tasks:**

- 4. Oral Policy Brief:** Prepare a ten-minute oral presentation outlining four possible policy options and recommending one to the National Security Council.
- 5. Decision Document:** Teams will also be required to submit a “decision document” accompanying their oral presentation at the beginning of the competition round. The “decision document” will be a prepared form, maximum of two single-sided pages (one double-sided page) in length, outlining the team’s policy response options, decision process, and recommendations. This document will allow the judges to familiarize themselves with the proposed policy options in an efficient manner.

**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 possible, observed, or reported as written. 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 and domains (e.g. private sector, military, law enforcement, diplomatic) and incorporate these insights along with cybersecurity.

- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct policy response option 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 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.*

EXERCISE



---

**From:** National Security Council Staff  
**Re:** Cyber Attack Against Critical Infrastructure | UPDATE  
**Date:** 3 September 2018

The date is Monday, September 3, 2018, and your team has recently presented policy options to the National Security Council (NSC) outlining your recommendations for responding to the major cyber-attacks targeting critical infrastructure in the US, and abroad. Since then, a US company initiated active defense measures pursuant to marque and reprisal authorities.

Given the unprecedented nature of this incident, the President has asked the NSC to consider the latest information available and develop additional policy response options.

Your team will consider the information contained here.

You will apply your understanding of cybersecurity, law, foreign policy, and security theory to synthesize useful policy measures from limited information. 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 Council requests that you consider the following potentially conflicting interests. These are provided as suggested starting points and are not meant to limit your policy responses.

- **Immediate Response vs. Delayed Response**  
What actions should be considered, if any, if there exists a possibility of US involvement? What actions should be taken immediately after the incident versus those that should be taken later? How should leverage be maintained?
- **Intelligence and Technical Gain / Loss**  
Should information about the vulnerability be shared with affected US critical infrastructure owners and operators? With the NCCIC? Should defense and mitigation measures be shared?
- **Government Response vs. Private Sector Response**  
What actions taken in response to the reports and incidents should be led by the private sector and what actions should be under the government's leadership? Actions to consider may include public acknowledgements, preventive and preemptive defensive actions, and offensive actions.
- **Offensive Cyber Capabilities vs. Defensive Cyber Capabilities**  
In its call to action in response to the incident, should the government prioritize strengthening capabilities of offense or defense?

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

- **Tab 1– FDA Safety Communications**
- **Tab 2 – News Article THE WASHINGTON POST**
- **Tab 3 – CLASSIFIED Intelligence Memo on Targeting of “Internet of Things” Devices**
- **Tab 4 – News Article DER SPIEGEL**
- **Tab 5 – CLASSIFIED US Intelligence Reporting**
- **Tab 6 – Online Press Reporting**
- **Tab 7 – State Department Message**

Tab 1: FDA Safety Communications

---

**EXERCISE**

**EXERCISE**

**EXERCISE**



## **Cybersecurity Vulnerabilities of Hospira LifeCare PCA™ Infusion Systems: FDA Safety Communications**

**Date Issued:** August 30, 2018

**Audience:** Health care facilities using the Hospira PCA Infusion System

**Device:** PCA Infusion System, all fielded versions

The Hospira LifeCare™ PCA Infusion System is a computerized pump designed for the continuous delivery of general infusion therapy for a broad patient population.

It is primarily used in hospitals, or other acute and non-acute health care facilities, such as nursing homes and outpatient care centers. This infusion system can communicate with a Hospital Information System (HIS) via a wired or wireless connection over facility network infrastructures.

### **Purpose:**

The FDA is alerting users of the Hospira PCA Infusion System to cybersecurity vulnerabilities with this infusion pump, and active / ongoing cyber attacks targeting these pumps which cause them to stop working. We strongly encourage that health care facilities discontinue use of these pumps in any networked environment.

### **Summary of Problem and Scope:**

The FDA, the US Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and Hospira are aware of cybersecurity vulnerabilities associated with the PCA Infusion System.

Hospira and the ICS-CERT confirmed that Hospira's PCA Infusion System can be accessed remotely through a hospital's network. This could allow an unauthorized user

to control the device and change the dosage the pump delivers, which could lead to over- or under-infusion of critical patient therapies. The FDA, Hospira, and the ICS-CERT have confirmed numerous adverse impacts to these systems as a result of ongoing cyber attacks by unknown actors, to include rendering these pumps inoperative in a number of cases.

### **Recommendations for Health Care Facilities:**

While transitioning to an alternative infusion system, consider taking the following steps to reduce the risk of unauthorized system access:

- Disconnect the affected products from the network.

**CAUTION: Disconnecting the affected product from the network will have operational impacts. Disconnecting the device will require drug libraries to be updated manually. Manual updates to each pump can be labor intensive and prone to entry error.**

- Implement a firewall that blocks UDP and TCP Port 80/HTTP and Port 8080.
- Monitor and log all network traffic attempting to reach the affected product via Port 80/HTTP and Port 8080.

The FDA recommends health care facilities follow the good cybersecurity hygiene practices outlined in the FDA Safety Communication Cybersecurity for Medical Devices and Hospital Networks, posted in June 2013.

### **FDA Activities:**

The FDA is actively investigating the situation based on current information. If new information becomes available about patient risks and any additional steps users should take, the FDA will communicate such information publicly.

### **Reporting Problems to the FDA:**

Prompt reporting of adverse events can help the FDA identify and better understand the risks associated with medical devices. If you are experiencing problems with your device, we encourage you to file a voluntary report through MedWatch, the FDA Safety Information and Adverse Event Reporting program.

Health care personnel employed by facilities that are subject to the FDA's user facility reporting requirements should follow the reporting procedures established by their facilities.

Device manufacturers must comply with the Medical Device Reporting (MDR) regulations.

**Other Resources:**

In June 2013, the FDA published a Safety Communication on Cybersecurity for Medical Devices and Hospital Networks.

**Contact Information:**

For additional information or questions about the PCA Infusion System, contact Hospira's technical support at 1-800-241-4002.

If you have questions about this communication, please contact the Division of Industry and Consumer Education (DICE) at [DICE@FDA.HHS.GOV](mailto:DICE@FDA.HHS.GOV), 800-638-2041 or 301-796-7100.

---

**EXERCISE**

**EXERCISE**

**EXERCISE**

EXERCISE

EXERCISE

EXERCISE



**U.S. FOOD & DRUG**  
ADMINISTRATION

## **Cybersecurity Vulnerabilities of GE Optima™ Diagnostic Imaging Systems: FDA Safety Communications**

**Date Issued:** August 30, 2018

**Audience:** Health care facilities using the GE Optima Diagnostic Imaging System

**Device:** Optima CT5xx Diagnostic Imaging System, all fielded CT5xx versions

The Optima CT Diagnostic Imaging System is a computed tomography (CT) scanning system which uses computer-processed combinations of many X-ray images taken from different angles to produce cross-sectional (tomographic) images (virtual "slices") of specific areas of a scanned object, allowing the user to see inside the object without cutting.

It is primarily used in hospitals, or other specialty health care facilities, such as neurologic and orthopedic care centers. The use of CT scans has been the greatest in two fields: screening of adults (screening CT of the lung in smokers, virtual colonoscopy, CT cardiac screening, and whole-body CT in asymptomatic patients) and CT imaging of children. This imaging device can communicate with a Hospital Information System (HIS) via a wired or wireless connection over facility network infrastructures.

### **Purpose:**

The FDA is alerting users of the GE Optima Diagnostic Imaging System to cybersecurity vulnerabilities with this family of imaging systems, and active / ongoing cyber attacks targeting these systems which cause them to malfunction. We strongly encourage that health care facilities discontinue use of these diagnostic imaging systems in any networked environment.

## Summary of Problem and Scope:

The FDA, the US Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and GE are aware of cybersecurity vulnerabilities associated with the Optima Diagnostic Imaging System. Attacks conducted by Internet actors have rendered these systems unreliable in a number of cases, when connected to the Internet.

## Recommendations for Health Care Facilities:

While transitioning to an alternative imaging system, consider taking the following steps to reduce the risk of unauthorized system access:

- Disconnect the affected products from the network.

**CAUTION: Disconnecting the affected product from the network will have operational impacts. Disconnecting the device will require completed CT scans to be uploaded manually. Manual updates to each system can be labor intensive and prone to entry error.**

- Implement a firewall that blocks UDP and TCP Port 80/HTTP and Port 8080.
- Monitor and log all network traffic attempting to reach the affected product via Port 80/HTTP and Port 8080.

## FDA Activities:

The FDA is actively investigating the situation based on current information. If new information becomes available about patient risks and any additional steps users should take, the FDA will communicate such information publicly.

## Reporting Problems to the FDA:

Prompt reporting of adverse events can help the FDA identify and better understand the risks associated with medical devices. If you are experiencing problems with your device, we encourage you to file a voluntary report through MedWatch, the FDA Safety Information and Adverse Event Reporting program.

Health care personnel employed by facilities that are subject to the FDA's user facility reporting requirements should follow the reporting procedures established by their facilities.

Device manufacturers must comply with the Medical Device Reporting (MDR) regulations.

## Other Resources:

In June 2013, the FDA published a Safety Communication on Cybersecurity for Medical Devices and Hospital Networks.

## Contact Information:

For additional information or questions about the Optima Diagnostic Imaging System, contact GE's technical support at 1-800-555-5555.

If you have questions about this communication, please contact the Division of Industry and Consumer Education (DICE) at [DICE@FDA.HHS.GOV](mailto:DICE@FDA.HHS.GOV), 800-638-2041 or 301-796-7100.

---

**EXERCISE**

**EXERCISE**

**EXERCISE**

# The Washington Post

---

Saturday, September 1, 2018

---

## Trump blasts Xi on false claims

---

Presidents rail against one another over US role in cyber attacks

---

BY DANIEL DE BEAU

President Trump took his message directly to the American people, as he has done so often throughout his Presidency. In a televised address, last night, he delivered a stinging rebuke to President Xi Jinping of China for what Trump calls false claims of US involvement in recent cyber-attacks that affected Chinese banks.

Trump blamed Chinese hackers for the events in late August, and stated vigorously the United States government had nothing to do at all with the attacks.

He highlighted recent attacks against specific American banks as proof the Chinese were responsible for degrading the operations of the Agricultural Bank of China.

In mid-August, the AgBank of China, one of China's largest and fastest growing banks with nearly US\$4 trillion in assets, was hit with a Distributed Denial of Service (DDoS) attack that lasted over two days.

Cyber security experts have said the attacks were the result of a botnet consisting of over one million compromised attack "zombies" that included many Internet-facing household network devices and security cameras.

In last night's address, Trump accused the Chinese government of waging unprovoked cyber warfare against the US.

His statements come on the heels of increased rhetoric between the two world leaders over a variety of policy issues.

President Trump has repeatedly highlighted China's frequent espionage and propaganda efforts as proof the government of President Xi Jinping is not a serious leader in the world community.

He stated the Chinese government was engaged in fake news regarding their assertions of US complicity in the recent attacks against Chinese banks.

The President also implied China regularly colludes with hacker groups to initiate attacks against US companies.



# EXERCISE

**Tab 3: CLASSIFIED Intelligence Memo on Targeting of “Internet of Things” Devices  
(EXERCISE)**

---

**EXERCISE**

**EXERCISE**

**EXERCISE**



**NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE  
FORT GEORGE G. MEADE, MARYLAND 30785-6000**



September 1, 2018

MEMORANDUM FOR DIRECTOR OF NATIONAL INTELLIGENCE  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF

SUBJECT: Memo on Potential for Targeting of “Internet of Things”  
Devices

In light of my preliminary report on August 26, 2017, regarding the attacks affecting Chinese banking infrastructure, I am providing the following supplementary information and assessment based on my office’s continuing analysis of the situation.

On August 25, 2018, PRC President Xi Jinping publically stated attackers exploited common open source software libraries developed, at least in part, by software developers paid or coerced by the US government to deliberately undermine the integrity of banking operations.

NSA analysts have reviewed Chinese tech blogs and public-facing communications and reaffirmed our assessment that the attackers likely compromised the banking infrastructure through a vulnerability in the Huawei routers’ HTTP implementation.

Additional Information:

The NSA reports open communications between a previously unknown hacker group – possibly related to the Democratic People’s Republic of Korea (DPRK) group responsible for the “Dark Seoul” cyber attack against Republic of Korea (ROK) financial institutions in 2013 and the attacks against Sony Pictures in 2014 – and operatives believed to be with the

Honker Union hacker group. The communications appear to be instructions for identifying and exploiting vulnerable IoT devices.

There is no evidence of Chinese government oversights of the Honker Union group, but they have leveraged the efforts of the group as a proxy force in the past. Open source reporting also alleges members of the group have benefited from their relationship with the Chinese government, and members of the Honker's Union have been recruited into security and military forces.

Our analysts suggest the potential linkage between DPRK and PRC groups could have developed as a way to combine expertise in botnets which leverage IoT devices with expertise in banking infrastructures. We have no evidence to suggest the groups are sharing operational control or target intelligence, beyond information on general tactics and techniques.

Classified by: DIRNSA [EXERCISE]  
Reason: 1.5(c)  
Declassify on: 25X

**EXERCISE**

**EXERCISE**

**EXERCISE**

English Site > World > NSA Cyber > US Intelligence Involved in Cyber War

## New Revelations **NSA Developed Tools to Attack Using Internet of Things**

**Shadow Brokers obtained the NSA's hack tools, and now reveals the intelligence community's heavyweight also pioneered attacks using common household items.**

By *Jergen Buntgon*



US cyber warrior "at work"  
Spiegel Images



September 01, 2018 05:23 PM

[Print Feedback Comment](#)

The super-hacker group [The Shadow Brokers](#) has again provided fresh insights into the activities of the [National Security Agency](#) (NSA). The ultra-secretive group became (in)famous for several leaks in late 2016 (of specifically, exploits and vulnerabilities targeting enterprise firewalls, anti-virus products and Microsoft products), tied to the [Equation Group](#) threat actor - NSA's Tailored Access Operations (TAO).

In a series of private on-line conversations with a member of the group, **DER SPIEGEL** has learned the US intelligence community was behind a [top-secret program](#) to exploit vulnerabilities in commercial communications and networking appliances, and that many of these highly-sophisticated weapons found their way into the hands of private US companies.

The highly-sensitive tool-building effort was aimed at creating cyber weapons using the [Internet of Things](#) – devices that connect to the Internet often without the user aware of it.

Equipment designers have for years been harnessing the power of the Internet to make their devices and appliances smarter and easier to upgrade. Now, it seems, the US intelligence community is leveraging these same “smart” devices as weapons to attack other countries’ critical infrastructure.

---

**Article...**

[Print](#) | [Feedback](#)



**EXERCISE**

**EXERCISE**

**EXERCISE**

**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
WASHINGTON, DC 20511**

September 1, 2018

MEMORANDUM FOR THE VICE PRESIDENT  
THE SECRETARY OF STATE  
THE SECRETARY OF DEFENSE  
THE ATTORNEY GENERAL  
THE SECRETARY OF HOMELAND SECURITY  
CHIEF OF STAFF TO THE PRESIDENT  
ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS  
ASSISTANT TO THE PRESIDENT FOR HOMELAND SECURITY AND  
COUNTERTERRORISM  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

SUBJECT: Intelligence Memorandum on Situation Involving use of  
Marque and Reprisal Authorities

On August 28, 2018, my office received communications indicating a US bank requested initiation of active cyber defense measures pursuant to the Cyber Marque and Reprisal Act. Since this represented the first use of this nascent authority, I directed my staff to monitor the situation to the extent they were able to do so without interfering in or otherwise supporting the execution of the activities.

To date, the only company who has been vetted and authorized under the Cyber Marque and Reprisal Act is Bakatax. They are based in San Antonio, Texas, and meet the requirements for command, control, and security as prescribed in the implementation guidance for actions under this authority. They received their General Letter of Marque and Reprisal in July of this year.

Our analysis indicates reprisal activities began on or about August 28th and were directed against the attack infrastructure responsible for the attacks against bank operators. Initial indications show the attacks against the bank have been significantly reduced or stopped altogether. However, we also observed indications the attacks have caused effects outside the scope of the covered activities.

## Technical Assessment:

Based on our analysis and private conversations with the CEO of Bakatax, we believe the attack tools used by the Bakatax team targeted various Internet-facing devices comprising the bulk of the targeted botnet's attack infrastructure. The tools used by Bakatax are designed to disable devices known to be susceptible to the automated bot-harvesting attacks by using nearly identical exploit code. Once the device had been compromised by the Bakatax countermeasure, accompanying computer code causes the device to either reboot, if the botnet malware is memory-resident only, or to become inoperable, if the botnet malware is persistent. The tools were tested extensively on various makes and models of communications appliances and were 100% effective against equipment made by Linksys, Cisco, and Juniper Networks.

Further, Bakatax limited its scope to avoid unintended consequences. The only systems targeted by Bakatax were those actively sending attack traffic immediately (within a 10-minute window) preceding the countermeasure. Target ranges for countermeasures excluded IP ranges known to belong to the Chinese financial sector. At the time they began their countermeasures, the volume of such nodes was well within the capability of the American bank's DDoS protections to withstand. Given the sensitivities and President Xi's remarks of August 25th, this exclusion was deemed necessary to avoid any perception of government-sanctioned attack against the Chinese infrastructure, or an attack against a business competitor.

However, we now believe some percentage of the targeted systems were permanently and without warning disabled. According to intelligence reporting, most of the known collateral damage resulting from Bakatax's reprisal actions have been to routers and switches made by Huawei, and two classes of medical devices: an infusion pump made by Hospira and medical imaging equipment made by GE. The areas most affected are the Chinese healthcare sector and Asian-Pacific markets where Huawei network devices are prevalent. These devices run BusyBox, which has a recently-discovered software defect that is known to have been exploited in the botnet attacks, and used to achieve effects in the original denial of service attacks. Credentials the botnet uses to attempt logging into devices also match known passwords for some medical devices.

## Emerging OPREP-3 situation:

Preliminary communications from ISR assets in the PACOM AOR indicate the effects against medical devices may have resulted in casualties within Chinese government circles or Peoples' Liberation Army forces. It is unknown at this time if any patients have died, though several regions have requested PLA doctors and nurses to cover the increased resource demands. Unsubstantiated intercepts indicate at least one high-ranking Chinese official undergoing medical treatment was

adversely affected. Additional details will be forthcoming under separate cover.

Classified by: DNI [EXERCISE]

Reason: 1.5 (c)

Declassify on: 25X

**EXERCISE**

**EXERCISE**

**EXERCISE**

EXERCISE



## Tab 6: Online Press Reporting

---

[Home](#) [Hacking](#) [Tech](#) [Deals](#) [Cyber Attacks](#) [Malware](#) [Spying](#)



# The Hacker News™

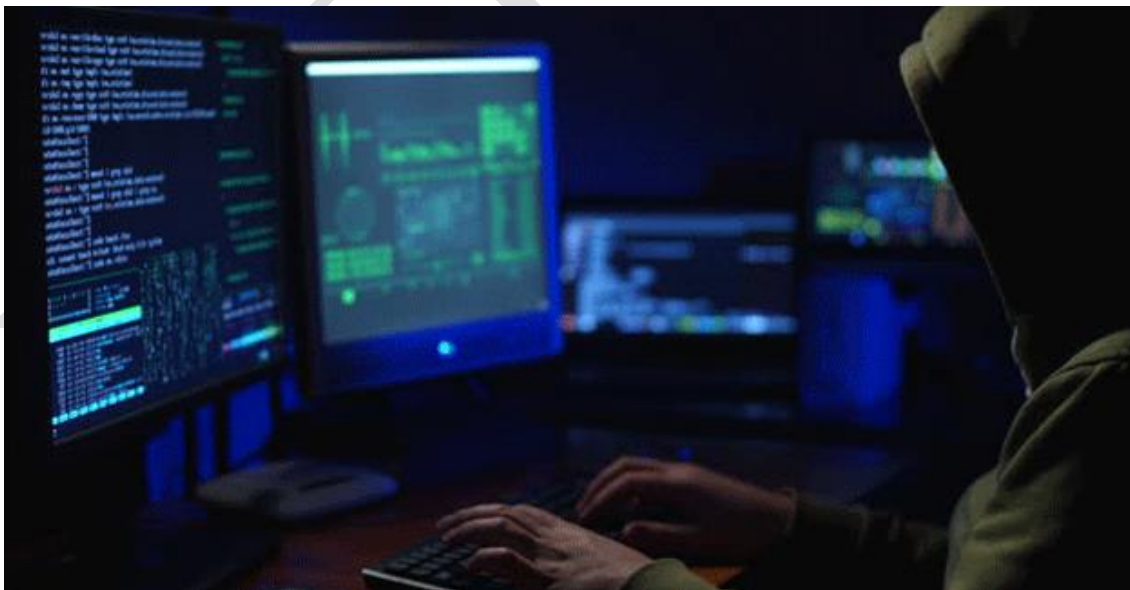
Security in a serious way

## Hacker war or American “hack-back” gone bad?

A large Twitter storm of people complaining about “bricked” routers affecting households and small businesses all day today. The hashtag #DeLinksys is trending, with thousands tweeting about it. Some of these systems seem to work fine after a reboot, some after resetting to factory settings, and some don’t come back at all. Outages are mostly in the United States, China, and Latin America.

📅 Sunday, September 02, 2018 👤 Chez Enrice

[G+1](#) 55 [Like](#) 4K [Share](#) 2946 [Tweet](#) 966 [in Share](#) 443 [Share](#) 4850

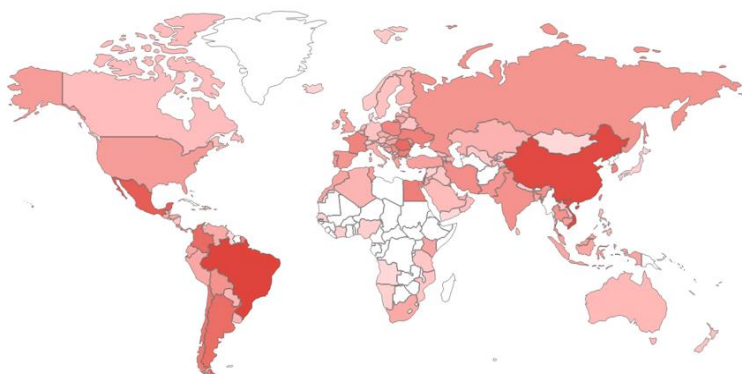


## No one is reporting a vulnerability – who’s doing the damage?

Cyber 9/12 | Intelligence Report III

---

*Disclaimer: The details in this fictional simulated scenario are for academic purposes only and are not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*



### Top Countries

1. China	203,154
2. Brazil	104,141
3. Argentina	94,002
4. Mexico	83,023
5. United States	67,854

Most of the devices involved appear to be the same ones involved in the botnet that raged a few days ago – but that’s mostly gone now. There’s a connection maybe (?) according to MassScan data provided by Errata Security. A search on Shodan.io reveals that there are over 700,000 devices worldwide that may be impacted by some combination of known vulnerabilities in IoT devices like the one targeted in the most recent botnet attacks. The graphic (left) shows that the correlation is pretty high.

We don’t know if this is deliberate vigilantism, ... a so-called “white worm”, ... warring bot herders looking for control, ... a mistake in the malware (such as what happened with German Telekom customers in December 2016). Or it is something else?

## Did the US unleash cyber-privateers?

An unnamed source in the Trump administration is saying an American financial institution is using the Cyber Marque and Reprisal Act (CyMRA) to take care of their DDoS issues. If true, this may be the first legal use of so-called “hack back” in the United States. And it may have gone very wrong.

## If you are the victim of a hacking attack, is it wrong to counter with an independent “hack back”?

— this has been a long time debate.

While many countries consider hacking back practices as illegal, many security firms and experts believe it as “a terrible idea” and officially “caution” victims against it, even if they use it as a part of an active defense strategy.

Accessing a system that does not belong to you or distributing code designed to enable unauthorized access to anyone’s system is an illegal practice.

However, this doesn’t mean that this practice is not at all performed. In some cases, retribution is part of

current defense offerings, and many security firms do occasionally hack the infrastructure of threat groups to unmask several high-profile malware campaigns.

## Hacking Back is legal maybe in your country, but what about others where your attacker resides?

This law might grant you authority to hack back, but if your attacker resides in the different country, you could face hacking charges in that nation by violating their law.

So, in this case, you inadvertently become a cyber criminal for that country.

## What about the cyber crimes that will take place in the name of Hacking Back?

In the whole discussion, one cannot neglect sophisticated hackers, who always found some ways to carry out internet crimes.

When hacking back is illegal under the Computer Fraud and Abuse Act, it's quite easy for anyone to judge who is a criminal and who is a victim.



Chez Enrice [f](#) [t](#) [i](#) [g+](#) [in](#) [e](#)

Entrepreneur, Hacker, Speaker, Founder and CEO – The Hacker News and The Hackers Conference.

### ★ Popular THN Deals

**ALIEN VAULT** EBOOK  
**How to Build a Security Operations Center (On a Budget)**  
GET YOUR FREE COPY ▶

Credit Source: Adapted from The Hacker News website, “Proposed Bill Would Legally Allow Cyber Crime Victims to Hack Back” dated 8 March 2017, by Mohit Kumar (<http://thehackernews.com/2017/03/hacking-back-hackers.html>)



**EXERCISE**

**EXERCISE**

**EXERCISE**

CLASSIFIED SECSTATE 45873

VZCF76HYRTGI98KMDIQRRR5257  
RR RUEHKO  
DE RUEHC #5688 3081818  
ZNR SSSSS ZZH  
R 021818Z SEP 18  
FM RUEHKO/AMEMBASSY BEIJING  
TO SECSTATE WASHDC  
INFO RUEHKO/HQNONSTATPOST BEIJING CN  
BT  
CLASSIFIED STATE 329145

E.O. 18004: N/A  
TAGS: ACOA, KSMT  
SUBJECT: PRC FM Seeking Redress

1. PRC FOREIGN MINISTER WANG YI contacted AMEMBASSY BEIJING and AMBASSADOR BRANSTAD demanding justice for cyber attacks conducted by private sector firm Bakatax. FM Yi stated US government sanctioned the attacks and is responsible.
2. FM Yi stated PRC leadership will use all means available to seek redress for the attacks, to include demanding immediate repayment of \$1.3T in US Treasury notes, use of military and cyber capabilities, and immediate suspension of US - China treaties and agreements in AP region. FM Yi relays message from PRC President Xi that "no cards off the table" in seeking redress.
3. AMEMBASSY BEIJING assesses situation critical regarding status of medical devices within PRC.
4. Troubling assertion by FM Yi that the attacks affecting medical devices was intentional "smokescreen" to mask attempted assassination of a government leader. Unclear at this time which Chinese leader affected or current status.

BRANSTAD  
BT  
#5688  
NNNN

**EXERCISE**

**EXERCISE**

**EXERCISE**



# The Cyber 9/12 Student Challenge

## Intelligence Report III

### INSTRUCTIONS

Your team will take on the role of experienced cyber policy experts on the National Security Council Staff assembled to jointly advise the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism. This packet contains fictional information on the background and current situation involving a major cyber incident affecting critical infrastructure in the United States and abroad. The attacks notionally take place in late August and early September 2018. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The President of the United States needs information on the full range of policy options available to the US regarding this incident. Your team has been tasked with developing **four** policy recommendations to pass on to the President and the National Security Council.

You are to consider as facts the following pages for formulating your response.

**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 options and recommending one to the National Security Council.

**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 possible, observed, or reported as written. 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 and domains (e.g. private sector, military, law enforcement, diplomatic) and incorporate these insights along with cybersecurity.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct policy response option 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 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.*

EXERCISE

---

**From: National Security Council Staff**

**Re: Cyber Attack Against Critical Infrastructure | IMMEDIATE ACTION REQUIRED**

**Date: 5 September 2018**

The date is Wednesday, September 5, 2018, and your team received the critical updates to the situation regarding US responsibility for errant active defense measures conducted pursuant to use of Cyber Marque and Reprisal Act authorities. At the request of the National Security Advisor, your team is being solicited to provide a range of possible policy response options to respond to the unfolding situation.

You will apply your understanding of cybersecurity, law, foreign policy, and security theory to synthesize useful policy measures from limited information. 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 Council requests that you consider the following potentially conflicting interests. These are provided as suggested starting points and are not meant to limit your policy responses.

- **What conditions would be required for the President to justify the use of military force against a nation state?**
- **How difficult is attribution in this case?**
- **How should the US message a potential need to respond with apparent proof culpability?**

Additionally, this message is accompanied by a document that may assist your team in preparing its policy response alternative recommendations for the President and NSC:

- **Tab – CLASSIFIED OPREP-3 PINNACLE (EXERCISE)**





**EXERCISE**

**EXERCISE**

**EXERCISE**

IMMEDIATE

I 051301Z SEP 18 ZYB

FROM: HQ USPACOM CAMP SMITH HI

TO: COMSEVENTHFLT YOKOSUKA JP

PACAF HICKAM AFB HI

HQ USSOCOM MACDILL AFB FL

HQ USJFCOM NORFOLK VA

HQ USSTRATCOM OFFUTT AFB NE

INFO: CJCS WASHINGTON DC

CSA WASHINGTON DC

CNO WASHINGTON DC

CSAF WASHINGTON DC

CMC WASHINGTON DC

NSACSS FT GEORGE G MEADE MD

COMJICPAC MAKALAPA PEARL HARBOR HI

COMNETWARCOM NORFOLK VA

COMTENTHFLT FT MEADE MD

CTF 1010 NORFOLK VA

AIG 5555

[EXERCISE CLASSIFIED]

OPREP-3P/FFBSD0/025/9999/INTELLIGENCE REPORT USPACOM AOR

1. (S) AT 042315Z SEP 18, USS BLUE RIDGE (LCC-19) REPORTED DISRUPTION OF ON-BOARD COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, AND INTELLIGENCE (C4I) SYSTEMS WHILE OPERATING APPROXIMATELY 200 NM WSW OF OKINAWA JP. CTF-1010 AND JICPAC ANALYSIS INDICATES PLA DIRECTED SPACE-BASED ELECTRONIC WARFARE AND CYBER CAPABILITIES AGAINST THE BLUE RIDGE. ISR AND C4I SYSTEMS ON-BOARD USS BLUE RIDGE (LCC-19) REMAIN DEGRADED.

2. (S) AT 050115Z SEP 18, NAVAL MQ-4C TRITON ASSETS OPERATING IN THE EAST CHINA SEA AOR OBTAINED IMAGERY AND COMMUNICATIONS INTERCEPTS INDICATING PLA 2ND ARTILLERY FORCES IN ADVANCED PREPARATION FOR DEPLOYMENT OF DF-15 SHORT-RANGE BALLISTIC MISSILES (SRBM) AND ASSOCIATED MOBILE TRANSPORTER-ERECTOR-LAUNCHERS (TELS). REQUEST JICPAC CONFIRMATION OF IMAGERY ANALYSIS.

A. (S) OBSERVED AND ASSESSED PREPARATIONS SUPPORT RECENT PLA NOTIFICATION OF INITIATION OF MILITARY EXERCISES WITHIN FUJIAN PROVINCE.

B. (S) COMSEVENTHFLT-N2/N39 ASSESSED THE DEPLOYMENT OF SRBM/TEL FLEETS AS ATYPICAL AND INCONSISTENT WITH PREVIOUS MILITARY EXERCISE MOVEMENTS.

3. (S) ADDITIONAL REPORTING BY AIRBORNE ISR ASSETS OPERATING FROM THE USS GERALD FORD (CVN-78) IN THE EAST CHINA SEA REPORTS DEPARTURE OF PLA-NAVY EAST SEA FLEET RAPID RESPONSE FORCE FROM ZHOUSHAN NAVAL BASE, INCLUDING THE JIANGKAI-CLASS FRIGATE WENZHOU AND THE LUYANG II-CLASS DESTROYER JINAN.

4. (S) OPREP-3 PINNACLE REPORTING CONTINUES.

CLASSIFIED BY: COMSEVENTHFLT [EXERCISE]

REASON: 1.5(C)

DECLASSIFY ON: 25X

**EXERCISE**

**EXERCISE**

**EXERCISE**