CS1800 Situation Analysis

Attached is the **Major Cyberattack** Situation Analysis for CS1800.

Some things to remember:

- **Think multidimensionally**: cyber policy impacts many different issues, and it is important to identify potential risks and opportunities in your analysis. Consider the strengths and weaknesses of several possible responses and select the optimal response.
- **Engage the scenario**: Assume that the situation which we have provided you is plausible. At the same time, think critically about the information that you have been provided and its origins.
- **Consider interests:** Organizations have a broad and diverse set of interests. How might your decision impact other interests which your organization would like to secure? If you choose one course of action, would a different office at your organization reject your approach? Be sure to be able to justify your response as strongly as possible.
- **Think holistically:** It is important to also consider not just your interests, but *all* parties' interests, including states and non-state actors.

What you are responsible for:

1. A brief, informal oral presentation by your group in section. There are no requirements for using visual materials, nor are there requirements for how many members of your group must speak. Expect to outline your course of action for roughly five, but no more than ten, minutes.

2. Engaging in a brief Q&A from your classmates and your TAs afterwards. We will be assessing the degree to which you have prepared justifications for your course of action.

3. A brief, informal one-page summary of your proposed plan of action to be emailed to your TAs at 11:59 PM the day before your section. Formatting is not especially important – we just want a record of your approach for evaluation purposes. Bullet points are acceptable in this assignment. No bibliography is required.

4. Filling out a peer evaluation after your presentation, during which you will have the opportunity to inform the HTAs about whether all members of your group contributed fairly to your group assignment.

Disclaimer: While some situation analyses for CS1800 are entirely fictional, others are based on real events. You should think about the "date" of your scenario and discount any events that have occurred in the real world after that date.

DATE: March 16, 2020

You are a small team of cybersecurity strategists in the U.S. National Security Council (NSC) charged with defending America's interests in cyberspace. You must analyze information provided to you from your intelligence community (IC) partners regarding a recent cyberattack in the United States and decide on the best course of action to recommend to the President.

Attack Summary:

Just after 6 AM EST on March 14, 2020 in Washington D.C., all city streetlights malfunctioned and ceased operation for over 18 hours.

Background & Context:

Notably, the cyberattack occurred in the context of a tit-for-tat between the United States and Iran. The United States recently attacked Iranian militias in Iraq, and Iran retaliated by attacking American military interests in Syria. However, the back-and-forth had ended by February 2, 2020, and no other attacks between the parties occurred. After the pause in tensions, the government of Iran declared that its country sought peace and de-escalation. The U.S. President expressed similar thoughts, but also imposed new economic sanctions on Iran on the same day.

It may also be worth noting that in 2017, a high-ranking Chinese diplomat in the Chinese embassy in Washington floated the idea of the Chinese military "shutting off an American city's traffic lights" if the U.S. were to implement proposed tariffs against China. He later clarified that this was meant in jest.

Results of the Cyberattack:

- Hundreds of minor road accidents and dozens of major collisions occurred. As of March 15, 2020, three individuals died as a direct result of these motor accidents.
- Emergency services were unable to navigate or respond to emergencies effectively. As a result of this incapacitation, up to twelve individuals in D.C. died.
- Due to the incapacitation of emergency services, crime rose significantly during the day, resulting in a 400% increase in burglaries & robberies
- U.S. Federal Government offices were severely understaffed or not staffed at all. Perhaps a million man-hours of federal government work were not completed. It is still impossible to assess the consequence of a nearly total shutdown of U.S. government operations for almost an entire day.

Under pressure and seeking reelection later this year, the President has asked your team to determine a list of options and your recommended course of action moving forward. He requests a response within seven days.

We have attached several documents for your reference. These documents may be useful to your decision making:

1. A report sent to you from U.S. Cyber Command, describing the technical details of the attack
2. A report sent to you from CIA summarizing intelligence based on human sources
3. A New York Times article describing recent events
4. The ODNI's Guide to Cyber Attribution

When deciding your response, first be sure to understand the fundamentals of deterrence in cyberspace (check course readings if you need to). Be sure to consider the following:

- Your degree of certainty of **attribution**, especially considering the technical details.
- How that certainty influences the ways in which you can or should **retaliate**
- How the **nature of the attack** (its "salience") influences the way in which you can or should retaliate
- The **speed** at which you should retaliate (if at all) given the information that you currently possess
- How **defensive measures** can play into your deterrence strategy
- What **political consequences** your proposed actions might have

To: NSC Cybersecurity Division
From: US Cyber Command
Subject: Technical Details and Context of Recent Cyber attack

On March 14, 2020, a cyberattack was conducted against the civilian road traffic networks of the Washington, D.C. Metropolitan Area Transit Authority (WMATA). The attack was somewhat sophisticated: it was not a denial of service attack, but instead consisted of several logic bombs which were planted in WMATA control systems. Specifically, the attackers took command of the control systems that manage the 1,652 traffic signals in the District, taking them offline. The attack persisted for 18 hours before a federal CERT (Computer Emergency Response Team) was able to regain control of WMATA's network.

The logic bombs were planted on WMATA's network on or around March 5, 2020, but network logs indicate that network reconnaissance was underway by February 27, 2020 at the earliest.

The proximate IP address of the attacker was **119.27.169.88,** which resolves to an internet service provider based in Beijing, China. Other IP addresses based in the Beijing region were also used as vectors for the attackers.

It is important to note that this attack does **not** bear the hallmarks of other known attacks or reconnaissance operations conducted by China. In 2019, we followed a known Chinese APT conducting network reconnaissance in the US for over five months, and in the UK for seven months. The very brief reconnaissance of the recent WMATA attack, then, is not consistent with Beijing's typically long-term attack preparations.

Moreover, previous Chinese attacks have almost always been routed through non-Chinese networks, typically in Europe or East Asia. A Chinese attack conducted through a Chinese network would represent a major reduction in Beijing's operational security. Finally, the code present in the logic bombs was not as sophisticated as the code typically seen in Beijing's APT operations. The software engineers behind this code are likely not trained in network exploitation to the same high degree as known Chinese actors like APT40.

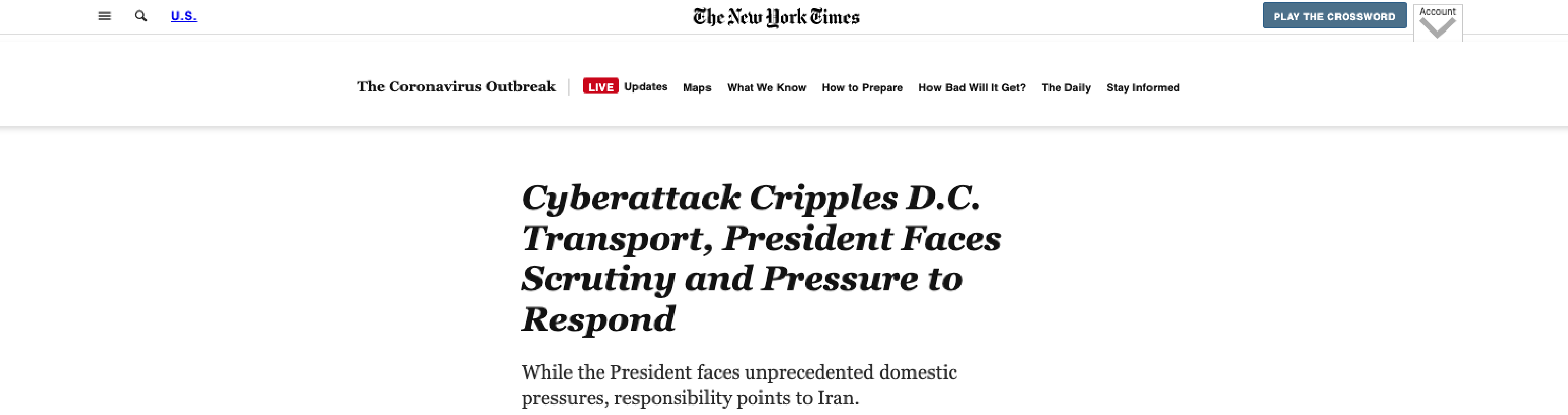
We will update you with any further details of the attack.

To: NSC Cybersecurity Division
From: Central Intelligence Agency, Office of Transnational Issues
Subject: Memo Regarding Human Intelligence on Recent Cyberattack in D.C.

Recent first-hand human intelligence collected by our agency indicates that several senior members of the military and political establishments of three of our four major “cyber adversaries” did not have foreknowledge of the March 14 cyberattack conducted against the D.C. WMATA. These adversaries include Russia, China, and North Korea. We have medium confidence in this assessment.

Regarding our fourth major cyber adversary, Iran: our preferred covert sources in the Iranian government have not yet responded to our request for information. Based on second-hand intelligence, another covert source in the Iranian government reported that Tehran also did not have foreknowledge of the attack. We have low confidence in this assessment, since this source has previously provided our agency with intelligence which could not be corroborated.

Our liaison officers in the other “FVEY” states (Canada, United Kingdom, Australia, and New Zealand) have confirmed that their governments’ intelligence services also do not have indications of responsibility for the attack.



Cyberattack Cripples D.C. Transport, President Faces Scrutiny and Pressure to Respond

While the President faces unprecedented domestic pressures, responsibility points to Iran.

U.S. Capitol police block the entrance to the Capitol Building during massive traffic light malfunctions. David Ryder/Reuters

By Mike Baker, Sheri Fink, Nicholas Bogel-Burroughs and Jack Healy

March 15, 2020 Updated 11:05 p.m. ET

Washington, D.C. - The transportation system of the District of Columbia was taken offline for 18 hours yesterday, resulting in highly publicized deaths and as of yet immeasurable economic losses.

The cyberattack was highly sophisticated and likely originated from a state actor, according to several officials familiar with the matter. The officials provided the information on the condition of anonymity, since they were not authorized to discuss the ongoing classified matter with the press. Another anonymous official told the New York Times that the National Security Agency suspected Iran of conducting the attack.

The attack comes in the context of increased politicization of cybersecurity issues in the run-up to the November Presidential election, for which President Trump has sought to demonstrate his national security bona fides against a Democratic opponent.

The President tweeted on Wednesday that the situation was under control, but Democratic rivals Joe Biden and Bernie Sanders argued that the President's lack of decisive action showed "weakness." At a campaign rally, Biden told a crowd, "We need a president that will stand up to thugs around the world. Our president is not that man. On my first day in office, I will respond to this attack forcefully and unequivocally."

However, major Republican figures have come to President Trump's aid. This morning, Senate Majority Leader Mitch McConnell released a statement claiming that the D.C. cyberattack was "purely a result of the Democratic Party's obsession over the unnecessary nationalization of election security. Taking away this power from states has forced our intelligence agencies to divert their efforts away from the truly important cybersecurity issue of critical infrastructure security."

This is a developing story. Updates are forthcoming. Please subscribe to the New York Times for more breaking journalism.

Office of the Director of National Intelligence

A Guide to Cyber Attribution

Leading Intelligence Integration

14 September 2018

(U) KEY TAKEAWAY

Scope Note: *This memo explains the key concepts the US Intelligence Community (IC) uses to identify the perpetrators of malicious cyber activities. This memorandum was prepared under the auspices of the National Intelligence Officer (NIO) for Cyber Issues. It was drafted by the NIO and the National Intelligence Manager for Cyber.*

Establishing attribution for cyber operations is difficult but not impossible. No simple technical process or automated solution for determining responsibility for cyber operations exists. The painstaking work in many cases requires weeks or months of analyzing intelligence and forensics to assess culpability. In some instances, the IC can establish cyber attribution within hours of an incident but the accuracy and confidence of the attribution will vary depending on available data.

To help with this process, the IC has identified several key indicators to evaluate and determine responsibility for an attack. We also have identified best practices for assessing cyber attribution and presenting our related assessments. A common approach to attribution can help to standardize communications with policymakers on cyber attribution and facilitate timely sharing of data and analytic collaboration.

Attribution: Difficult First Step for National Response

Russia, China, Iran, North Korea, and malign actors all use cyber operations as a low-cost tool to advance their interests, and we assess that unless they face clear repercussions for such actions will continue to do so. Cyber attribution, or the identification of the actor responsible for a cyber attack, therefore is a critical step in formulating a national response to such attacks.

Every kind of cyber operation—malicious or not—leaves a trail. Our analysts use this information, along with their knowledge of previous events and the tools and methods of known malicious actors, to attempt to trace these operations back to their sources. Analysts compare the new information to existing knowledge, weigh the evidence to determine a confidence level for their judgments, and consider alternative hypotheses and ambiguities to produce cyber attribution assessments.

There is no simple technical process or automated solution to determine responsibility for cyber operations. This painstaking work in many cases requires several weeks or months of analyzing intelligence and forensics. In some instances in which analysts can determine responsibility for a cyber attack within hours of an incident the accuracy and level of confidence is likely to vary depending on the available data.

- Analysts can assess responsibility for a cyber attack in three ways: the point of origin, such as a specific country; a specific digital device or online persona; or the individual or organization that directed the activity.

- This third category often is the most difficult to assess because we have to link malicious cyber activities to the specific individuals and assess the sponsor and motivators of these individuals.

Key Indicators That Enable Attribution

Attributing an attack to a particular country or actor requires collecting as much data as possible to establish connections to online actors, individuals, and entities. Because this often results in hundreds of conflicting indicators, we identified key indicators to guide us in seeking timely, accurate attribution. The primary indicators are **tradecraft**, **infrastructure, malware, and intent**. We also rely on **indicators from external sources**, such as open-source reports from the private cybersecurity firms.

- **Tradecraft:** Behavior frequently used to conduct cyber attack or espionage. This is the most important indicator because habits are more difficult to change than technical tools. An attacker's tools, techniques, and procedures can reveal attack patterns, but these unique tradecraft indicators diminish in importance once they become public and other actors can mimic them.

- **Infrastructure:** The physical and/or virtual communication structures used to deliver a cyber capability or maintain command and control of capabilities. Attackers can buy, lease, share, and compromise servers and networks to build their infrastructure. They frequently establish infrastructure using legitimate online services, from free trials of commercial cloud services to social media accounts. Some are loath to abandon infrastructure, while others will do so because they can rebuild it within hours. Some routinely change infrastructure between or even within operations to impede detection.

- **Malware:** Malicious software designed to enable unauthorized functions on a compromised computer system such as key logging, screen capture, audio recording, remote command and control, and persistent access. An increasing number of cyber actors can modify some malware indicators within minutes or hours of suspected compromise, and some routinely change malware between or within operations to impede detection and attribution.

- **Intent:** An attacker's commitment to carry out certain actions based on the context. Covert, deniable cyber attacks often are launched against opponents before or during regional conflicts or to suppress and harass enemies of the state.

- **Indicators from External Sources:** We also use reports from the private industry, the media, academia, and think tanks to provide such data or share hypotheses about the perpetrators.

Best Practices for Determining Attribution

Identifying these key indicators requires rapid and careful work. We identified three practices that can aid in the identification of cyber attackers.

- **Looking for Human Error.** Almost all cyber attribution successes have resulted from discovery and exploitation of the attackers' operational security errors. Cyber intruders have often made mistakes related to tradecraft and the use of cyber infrastructure. Our adversaries have sought to minimize these errors with varying degrees of success.

- **Timely Collaboration, Information Sharing, and Documentation.** Attribution efforts benefit from combining the expertise of regional, political, and cybersecurity analysts and the collaboration of network defenders, law enforcement, private cybersecurity firms, and victims. Acquisition, documentation, and recovery of data within twenty-four hours of a cyber incident also is critical because data-deletion cyber attacks can erase the log data necessary for forensics, advance malware dissipates in computer memory, and adversaries may abandon cyber infrastructure within hours of its discovery.

- **Rigorous Analytic Tradecraft.** Analysts may start with a set of plausible actors in mind, based on the nature of the cyber incident, the targets, and the context but must be careful to avoid cognitive bias. To minimize this risk, analysts can use techniques such as Analysis of Competing Hypotheses, which helps to evaluate multiple competing hypotheses based on the observed data and uncover data that might reveal other potential actors.

Best Practices for Presenting Attribution Analysis

Our best practices for presenting analysis related to cyber attribution include **de-layering the attribution assessment, providing the confidence level, and identifying gaps**. Our attribution assessments typically include a series of judgments that describe whether the event was an isolated incident or not, the likely perpetrator, possible motivations, and whether a foreign government played a role.

De-layer the Judgment. A statement of attribution should include a clear distinction among the following: the physical location where the activities originated, the individual actors or groups involved, and whether leadership sponsorship or direction could be determined.

Provide Confidence Level. Our analysts evaluate three components when assigning probabilistic language and confidence levels: the timeliness and reliability of the evidence, the strength of the logic linking the evidence, and the type of evidence (direct, indirect, circumstantial, or contextual). In many cases, analysts also consider competing hypothesis in order to uncover possible alternative actors.

- **High Confidence.** This level of confidence is used when analysts judge the totality of evidence and context to be beyond a reasonable doubt with no reasonable alternative. For example: “The Xandi Cyber Force (XCF) almost certainly is responsible for the destructive cyber attack on the Terran oil company. We have high confidence in this assessment because XCF operators discussed how they compromised the oil company and the steps they took to damage the company’s systems.”

- **Moderate Confidence.** This level of confidence is used when analysts judge the totality of evidence and context to be clear and convincing, with only circumstantial cases for alternatives. For example*:* “Xandi security services are very likely responsible for hacking the e-mail accounts of several Terran human rights activists. We have moderate confidence in this judgment because the hacking operations are linked to known Xandi intelligence infrastructure and the victims are also the Xandi’s priority targets.”

- **Low Confidence.** Analysts use this level of confidence when they judge that more than half of the body of evidence points to one thing, but there are significant information gaps. For example: “Terra probably was responsible for the data deletion attack on a Xandi bank last week after Xandi sanctions were imposed on multiple Terran companies. We have low confidence in our judgment because the actor used publicly available tools, which although previously associated with Terran intelligence, also are used by criminals.”

Identify Gaps. In cases where analysts do not have enough data for a judgment or confidence statement because there are insufficient indicators, they should state this explicitly. For example, “We do not yet have enough information to assess who is responsible for the disruptive cyber attack on the Xandi energy company. We suspect the attackers used a botnet originating from Terra. The attack did not coincide with any bilateral tension between the Xandi and known adversaries.”

Cyber Attribution Examples

The chart below shows how we use analysis of competing hypotheses in combination with the key attribution indicators to show what data we have to link the cyber incident to the actor.

Data to associate with incident: ● Sufficient ◒ Limited

CYBER INCIDENT			ADVERSARY	KEY INDICATORS FOR ATTRIBUTION				
				Tradecraft	Infrastructure	Malware	Intent	External Sources
2017	MARCH	Major Compromises of Global IT Firms	RUSSIA					
			CHINA*	●	◒	●	●	●
			NORTH KOREA					
			IRAN					
			NON-STATE	●		●	●	
	MAY	Wannacry Attacks	RUSSIA					
			CHINA					
			NORTH KOREA*	●	●	●	●	●
			IRAN					
			NON-STATE	●			●	●
	JUNE	NotPetya Attacks	RUSSIA*	●	●	●	●	●
			CHINA					
			NORTH KOREA					
			IRAN					
			NON-STATE	●			●	
	DECEMBER	Saudi Petrochemical Facility Attack	RUSSIA	◒				
			CHINA					
			NORTH KOREA					
			IRAN	◒			●	●
			NON-STATE					●

* We highlight the actor we assess to be responsible for the cyber incident when we have a sufficient body of information to link the actor's tradecraft, infrastructure and/or malware to malicious cyber activities.