ISSN: 2473-4901
v9 n5912

Truth or Media: Fallacies of Perceived Cyber Attribution

Tamirat Abegaz
tamirat.abegaz@ung.edu

Bryson Payne Abegaz
bryson.pyane@ung.edu

Chuck Robertson
chuck.roberson@uncg.edu

University of North Georgia
Dahlonega, GA 30597 USA

Abstract

The abstract should This paper examines the fallacies of cyber attribution and discusses how biased the public is in accepting media-claimed cyber attribution. The research objective is to show the complexity of cyber attribution and the bias of media in the matter. To demonstrate the bias, this research uses a cyber wargame simulation. Forty cybersecurity and related major students who have enrolled in an upper-level computer security course were recruited for the study. In the study, participants were provided multiple cyber-attack scenarios on a hypothetical US state named Magneta. Subsequent cyber-attack scenarios and follow-up questions were provided to eight groups of five. The participants, as a team, have come to a few conclusions regarding how the situation should be resolved. Each team also responded to multiple questions related to cyber attribution. The research intends to demonstrate the public bias in media claimed cyber attribution through comparing the students' attribution results with the statistical results of cyber-attacks national news from GDELT event database. The true value of the paper is to expose the manner in which respondents attributed the attacks. Overall, the results indicate that media-based cyber attribution has influenced even those participants who have better knowledge of cybersecurity. And such tenuous attribution is dangerous in an unstable world. If this is how (future) professionals attribute attacks, the consequences will be dire. This research paper calls for action from educators

Keywords: Cyber-Attribution, Cyber-Breach, Cyber-Attack, Cyber Threat, Adversaries, Cyber Conflict

1. INTRODUCTION

The Cyber-attacks have threatened the well-being, productivity, creativity, and safety of our society. Most recently, cyber-attacks have caused significant harm to society by disrupting financial and healthcare systems, and by shutting down critical infrastructure. Cyber attribution is the process of tracking down the adversary who conducted a cyber-attack. However, the process of cyber attribution has proved to be extremely complex since wrongful blame can lead to unfortunate consequences for a nation-state. In fact, cyber attribution is a notoriously difficult intelligence requirement that needs to pass through a thorough investigation to reach a reasonable conclusion. It is more of a weighted assessment rather than a set of determinant facts.

Unlike conventional warfare strategies, cyberspace reaches beyond national boundaries, making all countries vulnerable to cyber-attacks. Cyber-attacks can be initiated by individuals, groups, or a nation-state. For instance, one can conduct a cyber-attack to make a political statement, cause fear to society, or demand ransom for financial gains.
Effective cyber attribution requires technical, cognitive, and behavioral analysis to minimize ambiguity and biases (Banks, 2019). Unfortunately, attribution has often become a blame game without proof of forensic evidence. Nowadays, it is a prevailing trend to observe media outlets approaching cyber attribution in a manner akin to a 'Simon says' game, often devoid of any accompanying substantiating evidence. (Edwards et al., 2017, Linda, 2017). In this analogy, media sources often make assertions about the origins or perpetrators of cyber incidents without consistently providing the necessary supporting evidence. This kind of attribution is also known as Free Attribution or Faith-Based Attribution (Carr, 2016). Collectively, these elements contributed to the development of cognitive bias linked to cyber attribution.

Various media outlets tend to assign cyber attribution culpability to a handful of countries (Tran, 2018, Gopal, 2021, Tsagourias et al., 2020, Tannery, 2019, Khan et. al). Unfortunately, these condemnations create bias not only within society but also among cybersecurity professionals. Therefore, this research is based on the following hypothesis: *Media-based attributions bias the public toward China, Russia, and Iran for cyber-attack blame.* To investigate this, the researchers created a cyber-war game.

This paper examines how biased the public is in accepting media-based cyber attribution and discusses the factors, which might exacerbate such bias. The research recommends a thorough cyber investigation before reaching a conclusion, since false attribution can have a devastating effect on nation-states. This work aims to provide insight into the impact of media outlets on news consumers, which makes it difficult to disseminate the complexity of cyber attribution to regular users. The main motivation for this research is to present how complex cyber-attribution is and how biased the media is when it comes to cyber attribution.

Overall, the aim of this research project is to evaluate the bias that media can have on attributing responsibilities of cyberattacks, based on the analysis of simulated cyberattacks submitted to a group of participants. This paper is organized as follows. Part 2 of this article will briefly explain related work associated with cyber attribution and its challenges. Part 3 discusses the methodology, and Part 4 presents the results. Finally, it provides a conclusive remark about the fallacies of cyber attribution and explains the need for security practitioners to educate media reporters and the public about the complexity of cyber attribution.

2. RELATED WORK

Khan et al. indicated that cyber attribution is a useful, but extremely difficult, process to aid in the investigation following a cyberattack [10]. Cyber attribution can be impossible to establish with 100% certainty. There are several models proposed by various researchers that claim to improve the analytical efficiency, effectiveness, and accuracy of cyber attribution (Garvey & Lunt, 1991, Hutchins et. al, 2011, Caltagirone et .al, 2013, Kuang et. al, 2014, Al-Mohannadi, et al, 2016). Most cybersecurity researchers and practitioners use the Diamond Model of intrusion analysis (, Kuang et. al, 2014) for conducting cyber attribution analysis. According to the Diamond Model, there are four essential elements: adversary, infrastructure, capability, and victim (Al-Mohannadi, et al, 2016). This model integrates the Cyber Kill Chain framework to better assess cyber attribution (Berghel,, 2017). As shown in Figure 1, the model gets its name from the shape of these four interconnected elements.

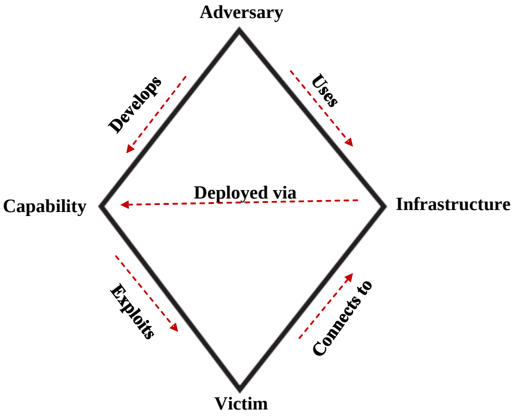


Figure 1: Diamond Model of Cyber Attribution

An adversary is an entity responsible for leveraging a capability (by deploying infrastructure) against a victim to achieve its targeted goals. Infrastructure is either the physical or the logical communication system through which an adversary delivers a capability. A victim is a target entity against which capabilities are used, or against whom infrastructures are deployed. A capability refers to the set of techniques, tactics, and procedures (TTPs) used by an adversary during cyber-attacks.

In simple terms, the Diamond Model describes how an "adversary" uses its "capability" over a specified "infrastructure" against a target "victim.". Analyzing cyber-attack incidents involves piecing together this model, using bits of information collected about these four facets to understand the threat in its proper context. In fact, in cyber attribution, victims, infrastructure, and capabilities are gathered facts. There must be a victim, and there should be an infrastructure and a deployed capability. However, the adversary element is the only one that is being assessed. Since it is an assessment there is a confidence level associated with it. Effective attribution uses three rules of thumb for confidence assessment: high, moderate, and low. High confidence involves multiple pieces of supporting evidence. In addition, to achieve a high confidence level, there should not be considerable evidence contradicting the assessment conclusion. Moderate attribution confidence depicts the existence of tangible evidence, but there is some evidence missing that could invalidate the assessment. On the other hand, low attribution confidence states that other hypotheses are possible, and there is limited evidence to reach a conclusion.

This research is based on the Diamond Model to indirectly engage participants to conduct a cyber attribution exercise on a simulated cyber-attack scenario. The participants were asked to provide evidence for their attribution assessment. This research adopts four categories of confidence levels. The participants were asked to provide the following confidence levels during their assessment in cyber attribution: very-confident which maps to high-confidence, confident (moderate confidence), somehow confident (low confidence), and guessing, for no confidence. This approach models for the students the way that a true cyber attribution assessment is expected to include both evidence and a confidence level.

3. METHODOLOGY

In this study, forty cybersecurity and related major students who have enrolled in an upper-level computer security course were recruited for the study. The participants were provided multiple cyber-attack scenarios on a hypothetical US state named Magneta. Based on a particular scenario, each team was asked to decide what option to follow and report the reasons behind the decision. Each team also responded to multiple questions related to cyber attribution. All students who have enrolled in the upper-level cybersecurity course have completed the task whether they agree to be in the study or not. However, a consent form was provided to each student to request permission to use the report for research purposes. The consent form stated, *"If any member of the group does not consent to having their coursework used for research purposes, then the group's work will not be used for research purposes".* The study spanned approximately 3 months. Only the reports in which all members of a group have consented to having their work used for research purposes have been included in the research.

At the beginning of the semester, the cyber wargame simulation was assigned to the participants. Out of 40, 4 students dropped the course. Only 4 out of 36 were female participants. The participants were presented with a hypothetical situation in which a US state named Magneta, has had a cyber-attack in which the state education system has been compromised. The background information about a fictitious US state named Magneta was provided to participants as follows:

The state of Magneta is a southeastern US state whose terrain spans coastal beaches, farmland, and mountains. Capital city Lotona is the seat of many prominent high-tech industries and National Historic Sites, the state is bordered to the west by the Gulf of Mexico, to the northwest by Ferocine, to the east by the Atlantic Ocean, and to the south by the Straits of Cordova which stretches from the Mexican border along the Pacific.

Magneta has 58 counties and as in the federal government, the power to govern is divided among three equal branches: the executive, the legislative, and the judicial. The Executive branch of government executes the laws enacted by the Legislature. The state possesses a stable agricultural and high-tech economy. Several large multinational corporations are headquartered in the state of Magneta, notably in the technological, agricultural, healthcare, and manufacturing sectors, which provide it with the fifth-largest economy by nominal GDP and manufacturing sectors.

Magneta has one of the highest proportions of Internet usage in the United States, with over

70% of its residents making use of it for their everyday activities. Digital connections and paperless transactions are encouraged and supported by the governor's office. Most residents conduct their bureaucratic and government business using the Internet. The state is also currently exploring the possibility of conducting voting electronically using digital ID cards. The main state and national election is conducted every 4 years. It is one of the swing states that can determine national elections. The state has a low tax rate, with the main source of the state tax income coming from sales tax. Magneta enjoys a low unemployment rate, at less than 4%, and has a foreign citizen population of 10%. The state of Magneta does not provide health insurance, and instead, the residents are encouraged to buy insurance from private insurance companies.

Magneta's educational system is managed by the board of education, which provides the statewide leadership necessary to ensure the opportunity for each public-school student to be successful. The Magneta Department of Education oversees public education throughout the state, ensuring that laws and regulations pertaining to education are followed and that state and federal money appropriated for education is properly allocated to local school systems. The department also informs parents, teachers, government officials, and the media of education-related news.

As a result of the breach, upper management, public relations, and the legal teams for the state were brought into the situation. Upper management's involvement was crucial in understanding the impact of the breach and taking the necessary steps to mitigate the damage. They may also be responsible for communicating with affected parties, stakeholders, and the public, as well as making decisions about the organization's response to the incident.

Public relations' involvement was necessary to manage the organization's reputation and ensure that it remains intact in the aftermath of the breach. They may be responsible for communicating with the media and other stakeholders, issuing press releases, and creating strategies to restore the organization's image in the long-term. The legal team's involvement was important in assessing the legal implications of the breach, ensuring that the organization is in compliance with relevant laws and regulations, and minimizing legal risks. They may also be responsible for determining the organization's liability and potential exposure, and developing strategies to address any legal issues that may arise. Subsequent scenarios of a cyber breach attack and follow-up questions are presented below.

Cyber Attack Scenario 1

Friday night, September 3rd, Bobby, the director of the Magneta state educational system, was finishing dinner with her family, and her phone rang. She looked at the screen, it was the CIO of the educational technology division. Forty-five minutes later she was in the technology center, watching the chaos unfold. The information that emerged was catastrophic. It seems that highly professional hackers broke in through the state's school information system and stole complete student account data, personally identifiable information (PII), past and present student grades, academic and disciplinary-related information, healthcare records, and parents' and teachers' information. As of yet, there is no report that the data has been published, but both the CIO and Bobby know it may be a matter of time, and that extremely confidential data such as Social Security and academic disciplinary information were exposed. The Incident Response (IR) and risk management teams are tasked to assess the damage and plan the next tactical strategy for crisis management. The Business Continuity team was tasked to explore all options to enable the education system to continue operations. Upper management, public relations, and legal teams were informed.

Whom should the office alert first? Explain? A. All the parents, B. All affected parents, C. The police and regulatory agencies, and D. Nobody, for now, until the situation is clear.

September 6th: Various news outlets are reporting that all the past and present students' (including several prominent political figures) confidential information has been compromised.
When should the public learn about this fact? And who should notify them? Explain?

Cyber Attack Scenario 2

It is

If you were the director of the board of education of the state, where the current president's education records are stored, what actions would you take? Explain? A. Inform the media that such a scenario for your state is three months later, and Bobby finally senses that the storm is over. She has done with the damage control, the security holes are patched, and the cyber experts have added enough new defenses to give the educational sector some peace. It is election time, and all local and international news outlets are covering the fierce battle between the democratic and republican candidates. When Bobby arrives at her office on Monday morning, she and her team discovered that details of the previous attacks have been leaked to the public. Both academic and disciplinary records of one of the prominent political candidates were leaked. Dozens of local and international media outlets share the news. Cybersecurity experts now tell reporters that they have found evidence that the attackers leveraged holes in the software of one of the educational system's critical contractors, and that the same contractor provides services to dozens of states. Other state officials scramble with the news leaks. The presidential candidates start to call their respective schools. The government declares that it is under cyber-attack indicates that multiple nation-state actors might be involved to undermine the nation's democratic process.

unlikely to occur, B. Inform the public that the board of education takes this event seriously and is working to learn lessons, C. Stay quiet, do not discuss the event in any way to avoid confrontational dialogue, D. End the relationship with the suspected supplier thereby preventing customers from executing critical services.

Perceived attribution from which countries do cyber-attacks against the state of Magneta originate? List your top three separately in the boxes (if you are unsure, please leave blank)?

How confident are you in your attribution of the above countries? A. Very confident, B. Confident, C. Somehow confident, and D. Guessing
List the evidence you can provide in your attribution for country 'A' (if you are unsure, please leave blank)?

Do the same for countries 'B' and 'C'

To summarize, Magneta's school information system was attacked by an adversary. While in the system, the adversary compromised an extensive list of sensitive data including personally identifiable information (PII), past and present students' grade records, social security numbers, healthcare records, disciplinary records, as well as records of parents and teachers. As a result of the breach, upper management, public relations, and legal teams for the state were brought into the situation. Each team has to work on the cyber-breach scenarios to conclude regarding how the situation should be resolved. The perceived attribution was intended to lead or guide the participants into formulating hypotheses for who may be responsible for the stated attack scenarios. In other words, based on the survey we hoped that the participants would formulate three hypotheses to attribute the responsible entity/organization/ or nation-state. It is important to emphasize that definitively ascertaining the intentions of a nation-state remains challenging due to the complexity of discerning these intentions. Given the extent to which media across Europe and many global regions echo narratives from the United States, an inclination is anticipated among the majority of participants to attribute cyber incidents to Russia, China, and Iran, even without substantial supporting evidence.

4. RESULTS

As stated in the methodology section, a data breach on a hypothetical US state was reported. Subsequent cyber-attack scenarios and follow-up questions were provided to eight groups of five. The participants, as a team, came to a few conclusions regarding how the situation should be resolved. In other words, based on a particular scenario, each team was asked to decide what path to follow and report the reasons behind their decisions during the incident handling process.

Explanation about cyber-attack scenario one: Whom should the office alert first? Explain? When should the public learn about this fact? And who should notify them? Explain? These questions require participants to think critically before choosing the options. Many of the groups attempted to provide detailed explanations about their decisions. The following subsections present the response provided by the participants.

Early Alert: For attack scenario one, question one (Who should be notified?), as shown in Table 1, some participants selected multiple options to be conducted at the same time, such as notifying the law enforcement at the same time as alerting all the parents. For instance, below is a response of one group: "It is recommended that the office should alert all the parents, police, and regulatory agencies immediately. All parents should know because time is of the utmost importance for the discovery of APT responsible for the breach. While every parent is not affected, it is important to let the parents know that their information may have been compromised. The police and regulatory agencies should also know because they can aid in the recovery process, as well as in identifying the bad actors in the breach. Failure to act with a sense of urgency in the notification process could result in widespread panic for those infected." As shown in Table, the result shows most of the participants selected option C (notifying the police and regulatory agencies). The common justification provided by the participants is that law enforcement officials have better technical capabilities for incident handling. Below are four show samples of the reasoning behind selecting option C.

Who should be notified	Number of Participants
All the parents	5
All Affected Parents	8
The police and regulatory Agencies	28
Nobody, for now, until the situation is clear	5

Table 1: Response to "Who should be notified?"

For the first prompt, the situation from just after the breach and initial notifications, it is asked whom the office of education should alert first. We conclude that contact with law enforcement is critical to attribution as the resources and technical skills needed to retrieve forensic evidence can rarely be done in-house. Cooperation will also provide the facts needed regarding the attack to prepare a well-informed statement for the public. If instead the parents were contacted first, then any statement would only attempt to placate the public relations situation, not resolve the attribution of the attack or find any unknown impact. Contacting nobody would likewise be negligent as the situation is clear enough to require intervention. Once the authorities have found their evidence, then it is best to work with public relations on going forward with whom to contact next.

The school should contact the proper authorities first, then the parents affected to tell them their children's information had been compromised. Afterward, officials should notify all parents that their system has been breached. Companies, including schools, are required to announce that their systems have been compromised to minimize fines and allow customers to implement damage control of potential identity theft. These cybercriminals could get business, medical or healthcare, financial, and educational data from the breach. It's common sense to contact the police first to file an official report as a crime has just happened. Additionally, both past and former students and their parents have the right to know that their children's information has been compromised, and to provide the perception that school authorities are not withholding information about a crime.

After reading the scenario and debating all possible options, we decided on that option. Alerting the police and related regulatory agencies would be the best course of action to take using responsible disclosure. Alerting all parents or only the affected parents that some of their personally identifiable information is currently known by a set of hackers seems like a plausible choice, however it is also unnecessary disclosure of information. If the police and regulatory agencies were told, they could provide potential help through private investigation and patching up the database before even more sensitive information is captured. Option D, alerting nobody, is a bad choice due to the time constraint Bobby has. It was said that the stolen information has not been published yet, and the longer they wait the more likely this sensitive information will spread and be released to the public.

Alerting the parents first would cause an uproar, especially considering that all the facts might not have been discovered about the case. The parents should be alerted, as anyone who is affected by a data breach should be, but the first external groups to call would be Law Enforcement and Regulatory Agencies. Federal Law Enforcement agencies like the FBI have specialized cybercrime units that are much better equipped to attempt to attribute the attack than any state education IT department can ever be. Considering the nature of the data that was breached, getting regulatory agencies involved at the same time is a wise decision. Breaches of Personally Identifiable Information and Social Security Numbers are serious deals, with specific agencies usually dealing with them.

It is *interesting to note that one group (5 participants) has selected option four, not to inform anyone until the situation is clear. Their justification is that "We are currently unsure if any of this data has been copied. We are working to notify everyone that has information in the locations of supposed accessed data, expecting that data was copied and might be leaked" Overall, as cybersecurity aware participants, their recommended option is the most viable option currently advised during cyber incidents*.

Media Response: As can be seen from Table 2, some participants selected multiple options. The result shows most of the participants have chosen option B (Immediately, by the state top officials) followed by option A (Immediately, by mass notification via news outlet). It is important to note that no participants selected option C (Immediately, by the teacher). Below are four (two for each) showcases of the reasoning behind selecting options A and B, respectively.

When should the public learn about this fact	Number of Participants
Immediately, by mass notification via news outlet	15
Immediately, by the state top officials	18
Immediately, by the teachers	0
Once the office has better ideas of the motives of the hackers and the implications	5

Table 2. Response to "When should the public learn about this fact?"

If various news outlets are already reporting that confidential information has been compromised, then the public should learn about this fact immediately. They should also be notified by the top state officials as the compromise includes a portion of them. Another reason that the state officials should be notifying the public immediately is that they can talk about what measures they have in place and give the public, mainly those who were past and who are present students, ideas on what to do in this situation. Those officials also usually know those who are taking measures to assess the damage and can have them give instructions or just notify them that they will be constantly and consistently monitoring everything and giving constant updates.

News outlets are reporting that all the past and present students' confidential information has been compromised. The public should be notified immediately by the top state official to avoid panic. In order to show control over the situation, it is the top officials' responsibility to address the concerns of the public in order to gain trust and confidence. Access to such confidential information could lead to extortion or blackmail. By allowing the state's top officials to control the reporting of the incident, it initiates a report of findings on a need-to-know basis in order to control the possibility of mass hysteria. It also allows the officials to help decide the proper steps going forward, as it is imperative that everyone works as a team to mitigate damages and leaked personal information.

Following reporting to affected parents and persons and regulatory agencies, some information was leaked to various news outlets. The Magneta Board of Education believed it would be in the best interest to have a press briefing from their state's top officials reporting to the public. In this briefing, the top officials make sure to include that their highest priority was reporting to those affected, as well as involving regulatory agencies, before reporting to everyone else, as well as reporting that the Board of Education would be strengthening their security posture to ensure that no more data would be leaked. Magenta's state officials also stated that they were planning to keep those affected up to date with information regarding the information leak. Following the press briefing, the Magneta Board of Education sent out a mass notification to news outlets to make sure that citizens were aware of the problems going on. Magneta believed that the information should come from their state.

Various news outlets are reporting confidential information of present and past students. This is due to the state's policies mandating that if more than a thousand individuals have their personally identifiable information potentially compromised in a cyber breach, agencies must report it within 72 hours. Furthermore, the policies require that there should not be an unreasonable delay in notifications. Given that we are a governing body, we should ask the top officials of the state to notify the public as that would be the most professional response. The written notification should also be sent as soon as possible because the people affected by the information breaches can respond with the necessary precautions to activate their credit monitoring and change any information that they deem essential. Failure to notify customers of a breach can result in daily fines from the government.

Table 2 shows that no group chose option three, citing uncertainty about whether the data was copied and their ongoing efforts to notify affected parties. Their recommended option, which is currently advised during cyber incidents, is considered the most viable one by these cybersecurity-aware participants.

Director's Action: Table 3 shows the selection option about cyber-attack scenario two: "If you were the director of the board of education of the state, where the current president's education records stored, what actions would you take? Explain." As can be seen from Table 3, some participants selected multiple options. The result shows most of the participants selected option B (Inform the public that the board of education takes this event seriously and is working to learn lessons). One group did not provide any response. Below are three showcases of the reasoning behind selecting option B.

When should the public learn about this fact? And who should notify them?	Number of Participants
Inform the media that such a scenario for your state is unlikely to occur	15
Inform the public that the board of education takes this event seriously and is working to learn lessons	18
Stay quiet, do not discuss the event in any way in order to avoid confrontational dialogue	0
End the relationship with the suspected supplier thereby preventing customers from executing critical services.	5

Table 3. Response to "What actions should be taken by the director of the board of education?"

Before we explain why we chose it, let's talk about why the other options would not be as effective and efficient as Option B. Option A does not make sense and it is very unclear; there is no point to lie and try to hide something that has already happened, future lies would only cause more problems. Option C is very popular and since the people already know about everything, the government would only make fun of itself and make citizens stop believing everything it says. Furthermore, information like this would appear in the media sooner or later, and then the government would still have to explain it (or lie). Option D will cause bad consequences and pretend that nothing wrong has happened or trying to blame somebody else never works out pretty well. When it comes to option B, the government from the beginning would be honest and transparent. Even though something bad happened, they do not want to hide anything from citizens; a situation like this might also help in the future because the people will know that a problem like that occurs in the future; the government will share this information and do everything to prevent it. At the same time, I think it would be important to perhaps not "work to learn a lesson" rather than be prepared for the next time if something similar happens. At the end of the day, the authority cannot show that it is afraid or makes a lot of mistakes because people have to believe and feel safe. By telling people everything, you make your life easier in order to cooperate with them, make their life safer, and make a crucial decision to improve a bad situation. Admitting to mistakes and then showing that a suitable solution has been found, which will ensure that the risk of its recurrence will decrease in the future; it creates a bond as well as a trust which is an undetectable part of building appropriate relationships in the country.

The best option out of the four above is option B, as a cyber security specialist you can never promise that your system will always be 100% protected therefore there is always the possibility that a system could be compromised. Staying quiet about the situation as well would not go well. This is because you as the director need to alert the public and those affected of what you plan to do in order to protect further information from being exposed or just address the issue in general because that information cannot be retrieved now that it has been released. As for ending the relationship with the supplier, it may seem like a good idea, but ending a relationship abruptly would cause a lot of problems. One example of this is the fact that it would cause the services provided by the provider to not be usable and another thing is that there would not be another supplier lined up to take over those services. It would have to be something that has to be planned out carefully as it could lead to many problems.

If we were the director of the Board of Education for Magneta, we would take the following actions. Now would be the time to inform the public and issue statements that the Magneta Board of Education takes these types of events seriously and is working to learn lessons from the incident. Additionally, the press release would also mention that an official final report would be forthcoming with in-depth details of the breach later upon completion of the investigation by law enforcement and cybersecurity investigators. With the government declaring that the cyber-attacks suggest multiple nation-states were responsible to undermine the nation's democratic process also led to more federal resources to help with the investigation.

Perceived Attribution: Instructions provided at the end of the project were as follows: "Explain your perceived attribution conclusions: From which countries do cyber-attacks against the state of Magneta originate? List your top three separately in the boxes (if you are unsure, please leave blank). How confident are you in your attribution of the above countries? List the evidence you can provide in your attribution for each country (if you are unsure, please leave blank)."

Many participants took the time to answer the questions. The following paragraphs present the selected answers from the participants, one from each group.

Attributed Countries	Number of Participants
Russia (with high or medium confidence)	21
China (with high or medium confidence)	16
North Korea (with high or medium confidence)	14
Ukraine (with high or medium confidence)	5
Argentina (with high or medium confidence)	5
Iran (with medium or low confidence)	2

Table 4. Perceived Attribution

As can be seen from Table 4, the top three countries identified were Russia, China, and North Korea. This is not a surprise, since the media is reporting these three countries as adversaries.... One group described their attribution as follows "The cyber-attacks against the state of Magneta most likely originated from the "BigThree" - the countries of China, Russia, and Iran. We are very confident in our assessment that these three nation states carried out the attack due to their ability and the fact that most cyber-attacks on the United States originate from these countries" Below are some justifications provided by the participants:

*Attribution for this incident is difficult, as is typical for nation-*state level attacks. No clear adversary is obvious in this situation; however, it is possible to make some correlations based on past events. Due to the growing unrest with the US, China is one potential culprit. It is known that they have a very capable cyber warfare department, and it is very possible this could have been a test for their hackers to prepare for a potential war with the United States. Russia is also a suspect. It has been suspected that they have meddled with US elections in the past, so for them to do it again would not be surprising. They have already demonstrated their hacking capabilities many times and have conducted campaigns with similar objectives. The last suspect is North Korea. North Korea has been building their hacking capabilities for years now and regularly tries to attack the US or US-based companies. They may not have a specific reason that we can point to, because their government as a whole is the opposite of transparent. An attack like this could be a part of their ongoing attempts to weaken the western world. Russia: Confidence Level A, China: Confidence Level B, Russia: Confidence Level C.

Russia could potentially have involvement in Magenta's recent cyber-attacks due to the processes that are seen in the Russian government. Magenta does not follow the same type of government as Russia, and in previous history wars have happened between the two separate governments. Russia was blamed for the Moonlight Maze attack, one of the first nation state sponsored cyber espionage campaigns. The theft involved a massive amount of classified information from multiple government agencies, such as the Department of Energy, NASA, and the Defense Department (DoS). North Korea could potentially be involved in Magenta's recent cyber-attacks since North Korea is a dictatorship and Magenta is a federal republic, which they may not agree with. North Korea has been responsible for many cyber-attacks in order to gain money recently. For example, in May 2018 North Korean hackers withdrew $13.5 million from a Cosmos Bank. They could potentially be involved in the Magneta attack in order to ransom the information for money. China could potentially want to cause problems in Magneta's election since it is a federal republic and China supports communism. China could be involved in this attack since they have participated in similar attacks on education. For example, in 2019 Chinese attackers were responsible for hacking 27 United States universities. China has been involved in attacks surrounding companies, universities, and governmental entities throughout the world over the last decade. It is not unreasonable to assume that China is interested in other countries' information due to the number of attacks in these areas, which means they possibly could be involved in Magnets recent attack. China could potentially have an interest in Magenta's election and be favoring a specific candidate since one of the candidates' information was exposed. China has launched cyber-attacks on other countries' prominent leaders. For example, Zirconium, which is operating from China, has targeted people in the Joe Biden for President campaign in the past.

There are many reasons that we believe that Russia is a likely candidate as the bad actor on the state of Magneta's Board of Education. The primary reason being the long history of cyber-attacks targeting the United States originating from Russia. Essentially, as long as the internet has existed, the Russians have used it as a vector of attack to disrupt the United States economy and political atmosphere. Another reason being the method of attack, where they gain their footing in a third-party that deals with government agencies, and then using that third-party: as a door to making an attack on the government. Yet another reason for attribution to be possibly attributed to Russia is the fact that the information gathered seemed to be used to disrupt the United States elections. Disrupting the Democratic process to undermine civilian confidence in the United States government would not come as a surprise as a goal of a Russian cyber-attack campaign. With these reasons behind the attack, we are certain that Russia had at least some influence on the attack on the Magneta Board of Education.

The list of reasons why we believe the cyber-attacks most likely originated from China is from growing international and economical rivalry dating back several years. From trade wars to the intense tensions over the coronavirus pandemic China and the Magneta have had a series of conflicts. Now more recently the tensions have increased due to an increase in espionage campaigns. Another reason China would be behind the attack is from their history of meddling with Magneta based companies. Specifically, their main target against Magneta is social, industrial organizations, and military information. As well as meddling with these affairs, China does have a history of disrupting the United States democratic process. With these factors in mind, we are very confident that China has had a hand in the cyber-attacks involving Magneta.

According to the evidence provided, recent attacks carried out by North Korea have been credited as social engineering attacks. Because of this, we have deemed North Korea as Not Plausible due to the fact that the scenario claimed that the attack carried out on the state's school information system was performed by highly professional attackers, those of which are likely to carry out more sophisticated attacks than socially engineered attacks. In regard to China, evidence suggests that it is Plausible for them to be responsible for an attack. When researching evidence for each country, there were noticeably fewer accounts of cyberattacks from China compared to Russia and North Korea. Furthermore, of the small amount of evidence we found for China, Chinese cyberattacks were primarily targeting foreign governments and officials and not anything along the lines of a state’s school information system. Russia on the other hand was rated Very Plausible due to multiple pieces of evidence linking up with the scenario. For example, in regard to the claim made about highly professional hackers carrying out the attack, evidence of Russian cyberattacks suggests that there are Russian hackers associated with the Russian Intelligence Service responsible for using their abilities to steal information. Furthermore, there are multiple accounts of Russia using methods regarding systems running Windows as well as through Microsoft’s cloud services. We found this interesting because an attack carried out on Magneta’s school information system likely occurred due to a vulnerability in a system capable of accessing the information as well as a possible vulnerability in a cloud service that could have been used to store the data.

Overall, out of 8 groups, 7 of them reported some sort of attribution. The attribution assessment reports indicated that the reports show a significant sign of cognitive biases. Berghel stated, *“Humans tend to be cognitive misers in that they search for the simplest explanation of events consistent with their disposition, biases, and world view.”* (The GDELT Project). It is arguable to state that the attribution is made not because of enough evidence but because of the media basis. To our surprise, one group has not attributed attacks to any country. This group stated the following: *“unsure of the adversary involved in this malicious act, due to a lack of conclusive evidence to point to a definitive source.”*. The conclusion is not supported by significant evidence.

GDELT Cyber-attack Reporting: The Global Database of Events, Language, and Tone (GDELT) project is a massive, ongoing project that aims to capture, analyze, and understand global events and their patterns using natural language processing and machine learning techniques. The project collects and analyzes data from various news sources and other media outlets around the world. It was created by Kalev H. Leetaru . GDELT provides web news media monitoring from multiple countries across various languages. However, this research focuses on the GDELT reporting on cyber-attacks on Western media.

The GDELT project has many potential applications, including in academic research, journalism, business intelligence, and government policy analysis. It has been used to analyze patterns of conflict and cooperation between countries, track the spread of disease outbreaks, and monitor changes in global media coverage of various topics over time.

As can be seen from Table 5, the top four countries identified were Russia, Iran, North Korea, China. These countries are listed in the top five of the perceived attribution lists by the research participants. Compared to the public, these participants have better awareness to cyber-attacks. It shows that media-based cyber attribution has influenced even those participants who have better knowledge of cybersecurity.

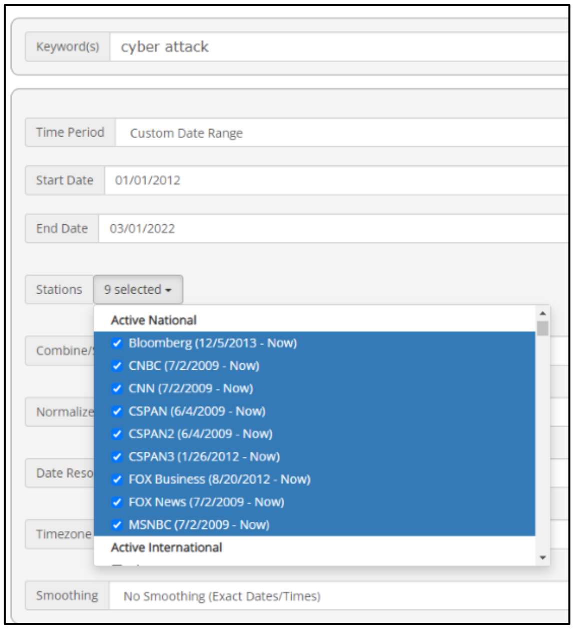
Attributed Countries	**Weighted Count**	**Ranks**
Russia	8.6811	1
Iran	8.0134	2
North Korea	5.5092	3
China	4.0067	4
USA	3.172	5
Argentina	1.5025	6

Table 5. GDELT cyber-attack reporting

Figgure 2 shows the configuration of the GDELT news event query. As can be seen from Figure 2, the query used is 'cyber-attack' the date range was 01/01/2012 to 01/01/2022. Nine national news agencies were selected for the stated query

5. DISCUSSION & CONCLUSION

Cyber-attacks have proliferated in recent years. As stated in the methodology section, a data breach is reported on a hypothetical US state was reported. This paper describes a user study to demonstrate the public bias in media-claimed cyber attribution. The paper discusses responses from participants to an attack scenario provided to them. Subsequent cyber-attack scenarios and follow-up questions were provided to eight groups of five. The participants, as a team, have come to a few conclusions regarding how the situation should be resolved in this case. As anticipated, the participants echo the media's assertions without substantial supporting evidence. For instance, while this evidence may be tenuous, in the case of attributing cyber threats to Russia, cyber threat practitioners often seek certain preliminary indicators. These include the use of Cyrillic language and Russian keyboard settings, heightened activity during times of Russian geopolitical tension, events coinciding with Russian work hours and holidays, and operations aligning with the objectives of the Russian government.



Keyword(s) cyber attack

Time Period Custom Date Range

Start Date 01/01/2012

End Date 03/01/2022

Stations 9 selected

Active National
- ✓ Bloomberg (12/5/2013 - Now)
- ✓ CNBC (7/2/2009 - Now)
- ✓ CNN (7/2/2009 - Now)
- ✓ CSPAN (6/4/2009 - Now)
- ✓ CSPAN2 (6/4/2009 - Now)
- ✓ CSPAN3 (1/26/2012 - Now)
- ✓ FOX Business (8/20/2012 - Now)
- ✓ FOX News (7/2/2009 - Now)
- ✓ MSNBC (7/2/2009 - Now)

Active International

Combine/

Normalize

Date Reso

Timezone

Smoothing No Smoothing (Exact Dates/Times)

Figure 2: GDELT query configuration

Similarly, for the attribution of Chinese-based cyber attacks, cybersecurity experts verify the consistent usage of Chinese keyboard settings and language. They also consider factors such as time zone alignment with the Chinese work period, temporal events, and the presence of IP addresses linked to government agencies.

Conversely, when attributing cyber-attacks to North Korea, basic indicators come into play. These encompass the identification of elusive IP addresses, as well as the detection of exploits and malware associated with or linked to North Korea. It's important to highlight that none of this evidence is directly embedded within the cybersecurity attack scenarios themselves.

The paper describes and discusses responses from students to an attack scenario provided to them. The questions posed to the students (deliberately) omit many details that require the respondents to "fill the gaps". The answers to all questions depend on how missing pieces of information were added, to answer the questions. The answers that are discussed in the result section provide some interesting insights to the respondents' perceptions of the situation. This research hopes to provide contribution to our understanding of perceptions around security. It is interesting to note that the researchers selected state actors. As a future work, we would like to explore how that would have changed if ransomware attacks were chosen (where motive could have been financial).

Attribution is a difficult task in digital forensics, and even experts may struggle with it. A recent study has shown that even students of digital forensics, who might be expected to be cautious about attribution, can be overconfident. This has important implications, as incorrect attribution can have serious consequences. The study suggests that cybersecurity practitioners should educate the public about the complexities of cyber attribution, and that educators should include cyber breach investigation and effective incident handling processes in their curriculum. In other words, it's important to include the difficulties of cyber attribution as part of educational curricula. Exploring real-life examples through case studies is crucial in helping people understand the importance of correctly identifying the sources of cyber activities. This approach underscores the vital role accurate cyber attribution plays in the larger field of cybersecurity. The paper concludes with a call to action for educators to address this issue.

The field of digital forensics has long acknowledged that attribution is a challenging task. While one might assume that digital forensics students would approach attribution with caution, a recent study has shown that this is not always the case. The study's findings are concerning, as incorrect attribution can have severe consequences. To address this issue, the research recommends that cybersecurity practitioners educate the public about the complexities of cyber attribution and that cybersecurity educators include cyber breach investigation and effective incident handling processes in their curriculum. This paper is a call to action for educators to take responsibility for addressing this issue.

The difficulty of attribution is a well-known challenge in digital forensics. Despite this, a recent study has shown that even students of digital forensics may be overly confident in their ability to attribute attacks. This has serious implications, as incorrect attribution can lead to significant consequences. To address this issue, the research recommends that cybersecurity practitioners educate the public about the complexities of cyber attribution and that cybersecurity educators incorporate cyber breach investigation and effective incident handling processes into their teaching. This paper aims to inspire action from educators to address this important issue. It is important to include the difficulties of cyber attribution as part of educational curricula. Exploring real-life examples through case studies is crucial in helping people understand the importance of correctly identifying the sources of cyber activities. This approach underscores the vital role accurate cyber attribution plays in the larger field of cybersecurity.

6. REFERENCES

Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., & Disso, J. (2016, August). Cyber-attack modeling analysis techniques: An overview. *In 2016 IEEE 4th international conference on future internet of things and cloud workshops* (FiCloudW) (pp. 69-76). IEEE.

Banks, W. C. (2019). The Bumpy Road to a Meaningful International Law of Cyber Attribution*. American Journal of International Law,* 113, 191-196.

Berghel, H. (2017). On the Problem of (Cyber) *Attribution. Computer*, 50(3), 84-89)

Caltagirone, S., Pendergast, A., & Betz, C. (2013). The diamond model of intrusion analysis. Center *For Cyber Intelligence Analysis and Threat Research Hanover* Md.

Carr, J. (2016). Faith-based Attribution?

Edwards, B., Furnas, A., Forrest, S., & Axelrod, R. (2017). Strategic aspects of cyberattack, attribution, and blame. *Proceedings of the National Academy of Sciences*, 114(11), 2825-283

Garvey, T. D., & Lunt, T. F. (1991, October). Model-based intrusion detection. *In Proceedings of the 14th national computer security conference* (Vol. 17).

GDELT "The GDELT Project"https://www.gdeltprojec

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in *Information Warfare & Security Research*, 1(1), 80.

Khan, A., Ullah, M., Rehman, F., & Ghani, A. (2017). Cyber Attacks in International Law: *From Atomic War to Computer War*. Available at SSRN 3064787.

Kuang, F., Xu, W., & Zhang, S. (2014). A novel hybrid KPCA and SVM with GA model for intrusion detection. *Applied Soft Computin*g, 18, 178-184

Rosencrance, Linda. "What Is Cyber Attribution? Definition from Whatis.com."*SearchSecurity, TechTarget*, 31 Oct.

Ratnam, Gopal. "Congress May Require Some Companies to Report Cyber Attacks." GovTech, GovTech, https://www.govtech.com/security/congress-may-require-some-companies-to-report-cyber-attacks.

Tannery, C. (2019, April 17). Cyber attribution: Essential component of incident response or optional extra. Exabeam. Retrieved October 24, 2021, from

EBSCOhost, doi:10.1093/ejil/chaa057.

https://www.exabeam.com/incident-response/cyber-attribution-essential-component-of-incident.

Tran, D. (2018) "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack,"20 Yale J. L. and Tech. 378

Tsagourias, Nicholas, and Michael Farrell. "Cyber Attribution: Technical and Legal Approaches and Challenges." European Journal of International Law, vol. 31, no. 3,. 2020, pp.941–967.