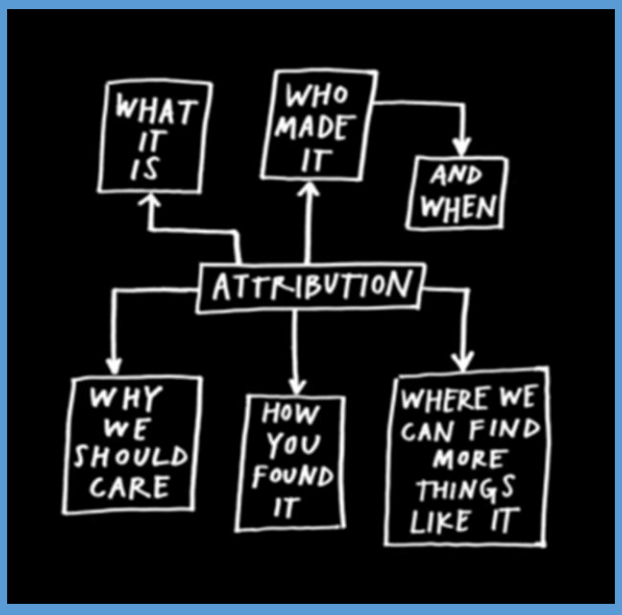
CYBER ATTRIBUTION USING UNCLASSIFIED DATA



2016 Public-Private Analytic Exchange Program Team

9 September 2016

2016
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

CYBER ATTRIBUTION USING UNCLASSIFIED DATA

Abstract

It has become almost systemic for people to immediately question, "Who did it?" when a major cyber breach occurs in the Public or Private sectors. Recent "high visibility" attacks/intrusions at many of the country's leading retail, financial and governmental institutions, has necessitated that cyber intelligence analysts gain a deeper understanding of attribution to assist in identifying their faceless attackers. Senior government officials, heads of agencies, corporate executives, investors, and others have a keen interest in findings in this area to support their decision making.

The challenge of determining, deterring, defending against and/or retaliating for such attacks – economically, politically, and/or militarily is driven by an accurate characterization and assessment of a perpetrator cloaked behind the veil of anonymity afforded by the internet. So it is extremely important to provide an accurate profile of an attacker for attribution. Organizations approach this problem in different ways, depending on their mission outcome, be it prosecutorial (law enforcement), impact to policy (intelligence community), or effect on profit (private industry). Models, such as the Diamond Model, can help these organizations follow a structured approach but they only provide a framework. It is ultimately up to the organization to decide how to analyze the situation (with appropriate methodology/tools) and whether attribution is even feasible.

A multi-disciplinary team was chartered by the Director of National Intelligence (DNI) Public/Private Analytic Exchange Program (AEP) to perform research in this area. This paper addresses several Key Intelligence Questions related to Attribution, based on interviews and panel discussions with cybersecurity experts. Focus areas include the relative importance of attribution to the Public and Private sectors, applicability of the Diamond Model, the state of

methodologies/tools. The paper concludes with the identification of areas for further research.

Introduction

In order to study attribution, we must first understand how organizations address it through their policies. Several factors can play into an organization's attribution policy (or even if they develop one at all), such as size, business domain, importance of organization information (i.e. national security or competition sensitivity), etc. Many believe that attribution is not even worth the effort, given the low probability of accurately identifying the source of an attack. So many organizations do not have a policy in place at all.

The size and business area of an organization can determine if they have the need and budget to pursue attribution, and either purchase or develop tools to that end. A DoD agency protecting sensitive/classified information, a retail corporation selling widgets, or a software firm developing the latest app may be totally different domains but their need for attribution if data is compromised is no less important to them. Depending on your perspective, the capture of state secrets can be equally as damaging as stolen PII or proprietary code.

Ultimately, it is up to the organization to decide whether they want to determine the identity of the individual/state responsible for destructive actions and pursue potential prosecution. Or they could decide that their information is not critical enough or budget cannot support attribution. For purposes of this paper, we are researching organizations that have decided to pursue attribution strategies.

Under this DNI project, the "Cyber Attribution" team will consider the full panoply of actors known and suspected of targeting critical infrastructure and key resources throughout the United States using "unclassified data." The goal of this project is to research technical and non-technical areas related to assigning responsibility for cyber-attacks/intrusions and provide guidance and/or areas for further research.

Research Team

A team of experienced cyber personnel was assembled from both government and private industry to address the chosen topic. Each member brought expertise in different areas to support and shape our research.

Name	Organization
Ernie Chambers (co-champion)	DHS/Treasury
Steve Choma (co-champion)	USSS
James Harris	Aflac
Kyle Pellegrino	Ernst Young
Christopher P.	DHS
Becky Selzer	United
Steve Sloan	Lockheed Martin

The team also solicited inputs from various experts in the field (organizations/representatives cited later in the paper) and we would like to acknowledge their assistance.

Methodology

The team was established in January 2016 and setup weekly teleconferences to discuss project plans and status. Our first task was to decide what form our final product would take. It was agreed to develop a symposium with a panel of experts to discuss various topics as our main approach. A field trip would also be conducted over the course of the project to further our research. The final product deliverable would be a summary of our field trip interviews and the symposium, resulting in this paper.

In order to properly address our topic, we determined that we needed to focus on specific key cyber attribution questions to be answered. The team developed a series of key intelligence questions that were refined into a set to be researched.

Key Intelligence Questions

- Is attribution important to private sector cyber security differently than public sector? How does attribution best fit within a cyber security risk framework?
- Does the Diamond Model properly describe the information needed to perform attribution?
- What is the state of cyber attribution tools/processes?
- Invariably, attacks/intrusions originate from within the borders of a nation state. Should cyber attribution be used to assign accountability to a nation state? Should they be held accountable for investigating, prosecuting, etc. based on cyber attribution?

There are many possible responses to each of these questions, depending on the perspective of who is evaluating it. To address these questions from varying viewpoints, we wanted to solicit inputs from as many cybersecurity experts as we could, within the limitations of our project timeline. We decided that to maximize inputs, we would plan a field trip to interview experts in person, as well as conducting a symposium with panelists to discuss/debate the questions.

Interviews

The team had the opportunity to conduct a field trip in support of this effort at an appropriate location. The Pittsburgh PA area was chosen for its proximity to several organizations, including CERT (Computer Emergency Response Team) at Carnegie Mellon University and the National Cyber-Forensics & Training Alliance (NCFTA).

CERT Division is a national asset in the field of cybersecurity that is recognized as a trusted, authoritative organization dedicated to improving the security and resilience of computer systems and networks. Because of its operationally relevant cybersecurity research, innovative and timely responses to cybersecurity challenges, and broad transition to our stakeholder communities, the CERT Division develops, executes, and evolves a technical agenda that brings unique solutions to cybersecurity challenges that measurably improve the security of the cyber environment.

The NCFTA is a non-profit corporation founded in 2002, which focuses on identifying, mitigating, and neutralizing cybercrime threats globally. The NCFTA operates by conducting real time information sharing and analysis with Subject Matter Experts (SME) in the public, private, and academic sectors. Through these partnerships, the NCFTA proactively identifies cyber threats in order to help partners take preventive measures to mitigate those threats. The NCFTA has a proven track record and has long been identified as the model for private/public partnerships. Collaboration with partners has resulted in countless criminal and civil investigations having been initiated, that otherwise may not have been addressed. To date, the NCFTA has provided intelligence which has aided in the successful prosecution of hundreds of cyber criminals worldwide.

The field trip was conducted during the week of 20 June 2016 to meet with industry experts and discuss our chosen research topics (their responses were recorded and will be summarized later). The team met with representatives from:

- CERT (including their Penetration Testing team)
- NCTFA
- USSS

The interview responses can be summarized as follows:

Importance of Attribution to the "Public vs. Private" Sectors

- Our research has shown us that there are at least 3 distinct communities that are impacted by the issue of attribution:
    i. Law Enforcement / Operational Investigations with arrest authorities who are interested in prosecution of the attributed party as the outcome.
    ii. US Intelligence Community (IC) (Title 50 Community) with operational aspects and investigations under the Espionage Act who are interested in Economic, Military, Political policy changes as the outcome.
    iii. Industry / Commercial-Private Sector Business community who are impacted by attribution from an economic perspective, with business decisions and remediation efforts to maintain business operations.

- Private sector attribution efforts are impacted by a reliance on information sharing efforts between organizations through Information Sharing and Analysis Centers (ISACs) and with government partners.

The DIAMOND Model

- We learned that this model was not used for attribution as prevalently as we originally believed and serves more as a guideline, with perceived benefits on what information can be helpful in determining attribution. Using the Diamond Model as a structured approach compared to other suggested approaches lends itself to further analysis.

The State of Tools

- We learned that while there are many tools used in this space, most are not standardized across the identified communities. Law enforcement has their prescribed set of tools, which are often less than stellar but functional and often require customization (in STEPs CERT and MITRE or any of the other National Labs). The FBI and USSS both have great cases to exemplify such use cases.

Assigning Accountability to Specific Actor Sets

- The USSS has had some success in working with nation states where cyber criminals initiated criminal cyber activity against US based cyber systems. We found that there is a benefit to accurate attribution leading to nation states accepting accountability by working with the US to investigate, collect additional evidence, arrest, extradite, etc. criminals.

Summary

- Each of the organizations/communities approaches attribution based on their particular and designed mission outcome, which effectively are Prosecutorial, Policy or Profit.

Symposium

A group of distinguished panelists was chosen to convene for a symposium on our research area, discussing specific topics and interacting with each other and symposium attendees. The symposium was conducted in Arlington VA on 13 July 2016. Invitations were sent out to interested parties and many participants attended either in person or via teleconference/web sharing (Adobe Connect).

The distinguished panelists for the symposium were:

Name	Organization
Sam Liles	DHS (Moderator)
Michael Jacobs	CERT, SEI/Carnegie Mellon
Andy Prendergast	ThreatConnect
Rich Barger	ThreatConnect
David Johnson	NCFTA
Deana Schick	CERT, SEI/Carnegie Mellon

The symposium was structured to include an overview of the state of attribution and two sessions with specific focus areas. The moderator opened with a discussion of cyber attribution, including several different types (political, technical, forensic), an overview of the Diamond Model, and attribution as a process. Questions were formulated by the moderator prior to the symposium (listed below each session) and additional questions were also solicited from the audience.

Session 1 - Cyber Attribution & the Cybersecurity Risk Framework

- Anton Chauvakin of Gartner has talked about tri-team model of cybersecurity where you have a security team, an incident response team, and a threat "something" team. How do you think these pieces fit into the attribution puzzle?**[1]**
- Thomas Rid and Ben Buchanan state that technical details of attribution can overwhelm decision makers with a false sense of precision. Can we answer that criticism or can we alleviate the concern of false precision? **[2]**
- The Diamond Model is based on a set of technical indicators and uses the "Cyber Kill Chain" to define stages of an attack. Is there a technical bias to the Diamond Model? Does the "Cyber Kill Chain" create a bias to attribution? **[3]**
- Earl Boebert said that attribution has a technical dimension and a human dimension. The end of the discussion being that attribution is hard. Is it attribution worth the effort? **[4]**

Session 2 - Attribution, Accountability, Privacy & First Amendment Concerns

- Given that adversaries infrastructure changes rapidly how do we assure correct attribution within the cyber domain? **[5]**
- Intelligence agencies have authorities that allow for collection on foreign entities, but infrastructure can be hosted anywhere including domestically. How do we insure legal, proper, and still quality attribution of foreign adversaries operating from domestic information assets? **[5]**
- The capability demonstrated by an adversary is likely going to be only that which accomplishes the job. When untangling the difference between cybercrime and nation state espionage how do you differentiate them? If the tools are similar or the same? **[6]**
- How do we protect privacy and civil liberties from false attribution claims?

Research Results

The following is a summarization of the inputs collected from both interviews and the symposium in support of answering these key intelligence questions:

Is attribution important to private sector cyber security differently than public sector? What elements of attribution are important to private sector cyber security? Public sector?

Attribution in cyber-attacks is certainly interesting to any information security organization in both government and private industry. However, our research hypothesized that the goals of this attribution vary between organizations. Our research questions for this topic focused on how attribution matters differently to private sector compared to the public sector. We wanted to find out what elements of attribution are important to private sector cyber security compared to the public sector, and how much specificity on attribution was needed for each group.

One other area we looked to research was the differences in tactical attribution for remediation in comparison to strategic attribution for the long term goals between public and private sector organizations. Our research focuses only on attribution from unclassified data, so we also wanted to cover how attribution for law enforcement and prosecution varies between public and private sector in the unclassified space.

We initially identified groups of interest in the following categories:

- The C-suite in private sector organizations
- Lawmakers in public sector organizations
- Intelligence analysts in public sector organizations
- Incident response roles in private sector organizations
- Threat intelligence roles in private sector organizations

After performing our interviews, we narrowed the scope of our research down to the following distinct communities:

- Law Enforcement
- United States Intelligence Community
- Private Sector Businesses

Each of these groups are interested in attribution for many reasons, some of which overlap. All three are interested at some level of the tactical attribution of cyber-attacks – the information which allows each group to remediate the threat or to prevent similar threats in the future.

From the law enforcement perspective, we found through our research that the main focus of attribution is, unsurprisingly, prosecution. Law enforcement is interested in finding out who was behind a particular attack and being able to present enough evidence to support the attribution. In this arena, specific information and names can be useful when working with law enforcement in other countries or regions. This level of specificity may be less useful to our other identified communities.

The Intelligence Community appears to be most interested in attribution to inform policymakers to help them make informed policy decisions in regards to offending countries in the cyber arena. This group is tasked with operational aspects and investigations under various authorities. Our research only covered unclassified attribution efforts, so we were not able to obtain the largest amount of information on this community – only visibility at a high level. From our interviews, our research suggested that economic, military, and political policy changes were the most likely to be affected by attribution information. The more operational efforts in the Intelligence Community were not covered by this report since many of those are classified.

The final group we saw placing an importance on attribution was the industry and commercial private sector business community. Private sector businesses are impacted by attribution in determining how to make business decisions and keep their operations running to maintain or increase their profit margins. Tactical attribution information at the private sector level allows technical experts of a

business to remediate or prevent attacks. Since attribution in these areas is done primarily through purchased sources and other intelligence gathering that is all unclassified, these companies rely on the partnerships created through information sharing efforts. One way these information sharing efforts are used is through sector-based Information Sharing and Analysis Centers (ISACs) and through partnerships with government parties. When dealing with reporting of an incident to authorities for potential prosecution, private sector organizations are asked to provide as much detail as possible.

The tactical groups in the private sector exchange indicators of compromise, which can assist in attribution and remediation efforts. From a tactical perspective, knowing specific names and organizations can be less important to these analysts unless being sent to law enforcement for action. When the more technical groups report to their leadership, their executive team is interested in how the attacks affect their business. Executive teams could be interested in attribution information to decide where to open a new facility and if to make a certain business transaction.

Attribution is approached slightly different by each of our identified communities based on their missions, which can be summarized as prosecution, policy, or profit.

Does the Diamond Model properly describe the information needed to perform attribution?

The Diamond Model is designed to break each cyber event into four vertices or nodes: Adversary, Infrastructure, Capability and Victim. The connections between the vertices form a diamond shape. This framework can be utilized to provide a filter for malicious cyber events. It has been suggested that the Diamond Model could be used to assist in cyber attribution. This model is being utilized by some organizations to assist them in determining who is performing or has performed a specific cyber event.

Based on our interviews and discussions with our experts, the Diamond Model is having minimal impact in assisting them with the cyber attribution effort and is being used by them sporadically, if at all. Other organizations that we are aware of have had success utilizing the Diamond Model in cyber attribution, for example, anyone using the ThreatConnect Threat Intelligence Platform (TIP) uses the Diamond Model (as the TIP is based on it), but the experts we interviewed are not consistently using the Diamond Model. There are multiple cyber attribution models being utilized today, including but not limited to the, Director of National Intelligence Threat Framework, the Q model, as well as the Cyber Kill Chain and it is up to each organization to determine which model fits their specific needs. Each model has their advantages and disadvantages and comparing and contrasting them is not the purpose of this paper, however as there are many different models, what we did find, is there is little standardization of cyber attribution models across our experts with each using the model that they like the best or are most comfortable with. This can lead to inconsistencies in the cyber attribution results.

More in-depth and specialized research is needed and should be focused on each major group of organizations that is performing attribution. For example law enforcement has different needs for cyber attribution than civilian government, DOD, IC and commercial entities. Different attribution models may be more effective for these specific organizations than the Diamond Model. Going forward

research should be performed to assist these entities in formalizing the process for the collection, aggregation and analysis of cyber attribution data points, for ensuring that the language is consistent for cyber attribution and developing and leveraging existing models in a unique but agreed upon practice for each major group.

What is the state of cyber attribution tools/processes?

Attribution for cyber-attacks is a concern for any organization, whether it be government or private industry. The difficulty is clearly identifying perpetrators, considering the ability of skilled hackers to hide their trails and avoid detection. As attacks become even more sophisticated, quicker methods to identify and prevent them must be developed. Tools enhance an analyst's work in identifying attackers and sharing that information throughout the community. Some tools are available to support this process but there is still work to be done as attacks become more sophisticated. Continued progress must be made in this area in order to keep up with the bad guys.

Attribution is the process of building a story describing how an attacker has managed to infiltrate an organization's infrastructure, hacked a website, or performed some other destructive / malicious act. As many analysts have discovered, this is not an exact science, and has become more of an art. It takes experience and the help of tools to put all of the pieces together and solve the puzzle.

Smaller organizations certainly cannot afford to dedicate IT personnel to tracking down attackers on a full-time basis, and even some larger organizations do not want to expend these resources in what some say is a fool's errand. So the need for tools to make the job more efficient/cost-effective is a necessity for proper attribution.

If the decision is to pursue attribution, there are multiple methods that can be chosen, from using basic operating system commands to analyze system logs to more sophisticated tools to mine data or alert administrators to attacks real-time. The choice of method comes down to the organization's policy, which are typically based on cost and/or criticality of data protection to the organization.

Basic auditing of system logs by Incident Response (IR) teams can provide a path to pursue yield some results from unsophisticated attacks but they do not typically provide the level of detail to accurately point the finger at possible perpetrators. While this method cost little and requires no specialized tools, since

the commands used are part of the OS, the process can be very labor intensive and potentially yield no results.

Attacks can be detected as they happen (near real-time) or be found much later through system auditing. Both areas require attention and a different toolset to support them. Detecting threats as they are occurring allows system administrators to shut them down and minimize damage, while tools to analyze attack patterns can be used to develop defense strategies to prevent future attacks.

Tools are being developed to cover different areas of the attribution problem, from near real-time activity tracking, to pattern analysis for behavior prediction, to data fusion/sharing. Several government/non-profit organizations, and commercial developers are at the forefront of tool development. Other organizations have also decided to develop their own custom toolsets to meet their needs (and budget).

One area that the panelists agreed on was the need to better share data among the cyber community. Analysts utilize internal data logs/tools to mine for results that can benefit in protecting their organization. But for various reasons, those results are typically kept internal when they could benefit others in the community. Corporations have proprietary/competitive concerns with sharing their data, while government organizations may just determine not to share due to bureaucratic policy. So ultimately, it comes down to a matter of trust between organizations, which can be hard to build.

Data sharing can also be difficult because the results from different organization may not be compatible with others, because of data formatting and/or levels of analysis. This would require that the data be translated into some common form/lexicon to be useful to other analysts. Whatever the reason, it allows attackers to launch similar attacks against multiple organizations which could be prevented if the community had a shared resource of attack campaigns. Initiatives like DHS/MITRE's Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) are helping to bridge that gap, but require that all organizations adopt the standard to be fully effective.

Invariably, attacks/intrusions originate from within the borders of a nation state. Should cyber attribution be used to assign accountability to a nation state? Should they be held accountable for investigating, prosecuting, etc. based on cyber attribution?

Assigning accountability to a nation state has proven to be productive on numerous occasions. To explain what we mean by holding a nation state accountable or assigning accountability to a nation state, we mean a nation state being held to taking action to stop ongoing cyber-criminal activity, investigate cyber-criminal activity, make arrests of those involved in cyber-criminal activity, work with the targeted nation states involving the cyber-criminal activity, patch/secure infrastructure to prevent future activity, etc. Although some nation states have the resources or expertise to accomplish any one of these, we should keep in mind that not all nation states have the proper resources or expertise to accomplish some of these.

A few examples of accountability being used successfully would be the Peter Romar case [7] and the Eric Donys Simeu case [8]. Regarding Peter Romar, the extradition shows that authorities in Germany were willing to make the arrest and to review the US's request for extradition. For Eric Donys Simeu, the investigation involved multiple international law enforcement partners. Ultimately, the suspect was apprehended in France and later brought to the US. Those are by no means all, but we can see from those examples that accountability can be used successfully.

For law enforcement, assigning accountability has, at times, been productive. We see in the news that US law enforcement has worked with some nation states to investigate, track down, arrest, and extradite cyber criminals. The previous examples show that other nations can be cooperative and that some nations accept that they have a responsibility to help or cooperate with other nations when cyber criminals are within their borders.

In the intelligence community (IC), accountability may be used in an attempt to encourage a nation state to put a stop to malicious or criminal cyber activity. The IC can use accountability, among other things, in an attempt to bring an end to

ongoing malicious cyber activity or criminal cyber activity. In Jason Healey's Atlantic Council's Issue Brief – Beyond Attribution: Seeking National Responsibility for Cyber Attacks from January 2012 [9], he makes reference to the US Secretary of State Hillary Clinton's speech where she holds the Chinese government accountable regarding attacks on Google's networks.

"We look to Chinese authorities to conduct a thorough investigation of the cyber intrusions that led Google to make this announcement […]. We also look for that investigation and its results to be transparent." [9]

Secretary Clinton may or may not have expected arrests to come from that, but this is an example of a government representative applying accountability to a nation state. Attribution that lead to this came from Google and experts in the cyber threat intelligence community. This indicates that attribution performed by the IC could also be used to assist policy makers in assigning accountability.

For corporations, at times, it is important to them to enable law enforcement or policy makers to use accountability. Attribution efforts by companies can help law enforcement and policy makers with this. In the example of Secretary Clinton, her use of accountability had the potential to help not only Google, but any US company who has or will have a presence in China. In the Peter Romar case, US business were among the targets of his extortion schemes.

Conclusion

We see that attribution is performed by 3 distinct communities (IC, Law Enforcement, and Corporations/Private Businesses). At times, law enforcement will reach out to the private sector by way of organizations such as the ISACs, NCFTA, etc. to see if members of the private sector have additional information that may relate to law enforcement investigations. If law enforcement were to have a system, such as a Threat Intelligence Platform (TIP) and were to have information sharing agreements in place with members of the public and private sectors, the need to reach out to the ISACs and other organizations would be reduced and in some cases not necessary. The same would apply to DHS/ODNI.

NCFTA attempts to promote collaboration among its public and private sector members and, therefore, can act as an example of bringing together information sharing from the private and public sectors. The lack of use of systems supporting a standard like STIX/TAXII and the lack of use of TIPs seem to be some of the biggest issues with information sharing.

The Diamond Model is one of several established frameworks that can be used to analyze the attribution problem set. There is currently no structured approach being universally followed but that is a function of which industry is using them. Different models work better for certain analysts/organizations, although most share some common features. Combining the best features of these frameworks into a more standardized approach could benefit the cyber community.

Recent examples prove that when a nation is targeted by a cyber-attack and then assigns accountability to another nation state, it can better facilitate the identification of the perpetrator within that nation. Governments (and potentially the private sector) can cooperate/share resources to more efficiently and accurately track down attackers. Not all nation states are willing partners and sometimes political pressure is required to make those nations work together. In other cases, nations are just not able, due to resources/expertise, to accept that responsibility. Ultimately, assigning accountability can be another tool to be used to help solve the attribution problem.

Areas for Future Research

At this time, DHS I&A is looking into standing up a cyber threat attribution capability. DHS I&A should consider how they will enable the sharing of information among the 3 sectors (IC, Law Enforcement, and Private sector). Whatever TIP is used to support this should have bidirectional information sharing capabilities. Our research has indicated to us that one of the major problems in the area of attribution is that at times attribution efforts in one sector are duplicated in others due to lack of information sharing. Another problem is the quality or accuracy of attribution information. DHS I&A will need to account for this issue in whatever system supports their attribution capability. In addition, DHS and ODNI should consider working with law enforcement and the private sector to formulate a plan to enable better sharing of cyber threat attribution information. The use of accountability has had positive results. DHS and ODNI should consider whether or not to use information from attribution efforts to enable policy makers and law enforcement to hold nation states accountable.

Further research/development in the area of attribution data sharing could help to reduce the number of attacks, if shared results can be quickly and efficiently disseminated to potential target analysts. Continued development and acceptance of a common lexicon and data standard would allow analysts from disparate organizations to speak the same language and benefit from each other's hard work. Sensitivity would have to be exercised with the data, based on the originating system's classification or propriety, but through proper policy and sanitization, useful data could still be collected. Data mining tools could then be developed to take advantage of the larger amounts of data to better identify patterns/trends and allow organizations to more quickly establish defenses.

Another follow up point for this group would be to determine which structured approaches the three main communities are deploying, and it would be pertinent to address the perceived benefits of a structured approach (like the Diamond Model) versus other suggested approaches.

References

1. http://blogs.gartner.com/anton-chuvakin/2016/07/07/about-the-tri-team-model-of-soc-cirt-threat-something/
2. Rid, Thomas; Buchanan, Ben "Attributing Cyber Attacks" The Journal of Strategic Studies, Vol 38, 1-2, 4-37
3. Catagirone; Pendergast; Betz "The Diamond Model", DoD Document released 2013
4. Boebert, Earl "A survey of challenges in attribution" Proceedings of a workshop on deterring cyber-attacks: Informing strategies and developing options for U.S. policy, National Academies Press, 2010
5. Clark, David; Landau, Susan, "Untangling Attribution", Proceedings of a workshop on deterring cyber-attacks: Informing strategies and developing options for U.S. policy, National Academies Press, 2010
6. Confirmation bias (https://en.wikipedia.org/wiki/Confirmation_bias)
7. http://www.federaltimes.com/story/government/cybersecurity/2016/05/11/syrian-hacker-romar-extradited/84231020/
8. https://www.justice.gov/usao-ndga/pr/computer-hacker-extradited-france
9. https://www.fbiic.gov/public/2012/mar/National_Responsibility_for_CyberAttacks,_2012.pdf

All judgments and assessments are solely based on unclassified sources and are the product of joint public and USG efforts.