Fallacies in Threat Intelligence Lead to Fault Lines in Organizational Security Postures

Organizations follow inaccurate definitions of threat intelligence leading to poorly conceived cyber threat intelligence programs. Vendors communicate threat intelligence definitions supporting their offerings propagating the fallacy that threat intelligence solves numerous security problems.

Cyber Threat Intelligence functions being built on a foundation not supported by standard intelligence tradecraft. Many programs support a fraction of the intelligence needs yet stakeholders hold unrealistic expectations based upon expenditures.

Information security capabilities marginally improve as spending skyrockets and security posture improvement is limited to after-the-fact discoveries communicated as prevention.

Continued purchases of 'threat intelligence' tools based upon the see-detect-and arrest paradigm ensures slow improvement and loss of data expansion. Intelligence program builds focused on technology capabilities repeats the historical problems of information security when firewalls and anti-virus represented the core of security programs.

Recommendations and opportunities normally located in this report position follow below in the *Changing Behaviors* section.

Access to organizations who may be more advanced presents gaps in data available for this article. We based evidence upon direct access to a number of Fortune 500 organizations, discussions during cyber intelligence training classes, and actual intelligence program build activities.

NOTE: The above format minus analytic paragraphs and alternative analysis follow standard intelligence tradecraft analytic writing.

Common Taxonomy

A general Internet search on 'threat intelligence' returns 11 million results in .36 seconds demonstrating the intentional propagation of a term intended to generate revenue. Information and cyber security vendors, well-known training organizations, and companies use the term so often it has lost any real meaning. Most vendors use the term as if intelligence is easily created, readily available. Product is sold with the expectation that threat intelligence is the panacea CISOs have sought for years. This is a general misnomer and cyclical in the regular creation and use of buzzwords and catch phrases that change annually. Vendors create years of capabilities based upon the jargon that just yesterday, no one even knew existed. One of those buzzwords is threat intelligence.

What is threat intelligence? Gartner indicates this to be:

> *Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.* (Gartner, 2013) B3

Solutionary (NTT) uses this definition from the Central Intelligence Agency:

> *Reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world around us. The prelude to decision and action by U.S. policy makers. Intelligence organizations*

provide this information in a fashion that helps consumers, either civilian leaders or military commanders, to consider alternative options and outcomes. The intelligence process involves the painstaking and generally tedious collection of facts, their analysis, quick and clear evaluations, production of intelligence assessments, and their timely dissemination to consumers. Above all, the analytical process must be rigorous, timely, and relevant to policy needs and concerns. (Security, 2016) A1 *NTT Security then goes on to say that instead of providing military or political intelligence to government stakeholders, the current focus within the information security industry is to deliver threat intelligence to an organization's stakeholders about digital threats to their enterprise systems.* (Security, 2016) B2

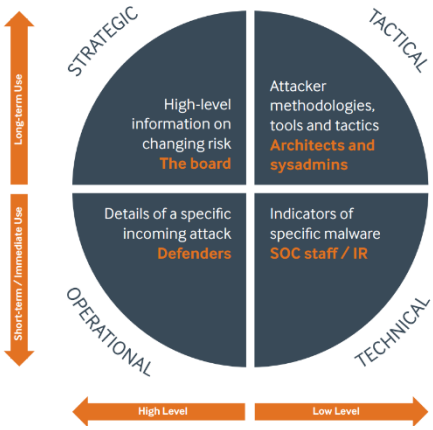

Figure 1 MWR Model of Threat Intelligence

Definitions Misunderstood

Herein lies one of the most inherent issues that vexes many organizations today. The myopic view that all that is needed is technical threat intelligence in order to protect an organization. We couple this with additional fallacies a bit later. Fallacies that create massive fault lines in our cyber security postures guaranteed that lead to unrealistic expectations and program gaps.

Definitions for intelligence range in scope and depth based upon who is using the term. We tend to stay close to traditional tradecraft definitions such as those below:

> The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning adversaries (script kiddies, novices, cybercriminals, nation-states, hacktivists, political activities, insiders, whitehat / blackhat hackers, cyber terrorists, competitors, investigative reports, academics) hostile or potentially hostile cyber elements, or areas of actual or potential operations. (Government, Joint Intelligence, 2013) A1 Also, a body of evidence and the conclusions drawn from what is acquired and furnished in response to the known or perceived requirements of consumers. It is often derived from information that is concealed or not intended to be available for use by the acquirer. (Government, 2013) A1 Alternatively, data and information that is sourced openly, and when placed through a process of decomposition, analysis, recomposition, and synthesis, becomes intelligence.

It gets quite confusing. Which definition should we follow? For pure terminology, MWR InfoSecurity in the United Kingdom seems to have a solid handle on the threat intelligence definition. MWR proposes a model that breaks down threat intelligence into four distinct categories based on consumption, strategic, operational, tactical, and technical. (InfoSecurity, 2015) B3 MWR's model (Figure 1) is well defined, detailed, and something organizations should read and recognize.

The problem with this model is the exclusive focus on threat intelligence. Threat intelligence is a subset of intelligence. Threat intelligence assumes a certain amount of collected data and information is collected creating intelligence that is then aligned to organizational threats. Threat intelligence does not always include the correct data. Most all times, the data is tactical and technical in nature leaving significant gaps. Other times that data is skewed by the inherent bias of the technologies through which it is collected and filtered. In the end, it lacks in scope, depth, breadth, including lacking tradecraft.

What is Tradecraft?

Unfortunately, most of what is produced are data and at best, information. This starts with the misunderstanding as to what data is versus information as opposed to actual intelligence. The term is a core component of sales neglecting the difficult process of creating intelligence, while presenting data and information as actionable intelligence. Creating intelligence is a process that requires hard-nosed collection, attention to detail in production, structured methods and techniques, awareness of critical thinking and cognitive bias, the use of analytic methods, and the patience and perseverance that comes with knowledge creation. For this writing, we call this tradecraft.

Let's not confuse tradecraft as being something that is military intelligence. Many believe intelligence tradecraft is military in form and function. This is not true. The intelligence tradecraft of which I speak is rooted in CIA capabilities honed over years of trial, error, mistakes, and triumphs. The writings of Sherman Kent, long held as the father of intelligence analysis, defined methods of intelligence analysis used today. Kent's analytic standards, doctrines, and practices need to be applied today within cyber threat intelligence functions. (Davis, 2007) A1 The writings of Richards J. Heuer Jr., a 45 year CIA veteran, describe issues with critical thinking, cognitive bias, and structured analytic techniques used today as well. The writings of both men are directly applicable to information security efforts to create threat intelligence. Their use enables organizations to see beyond the limited view of 'see, detect, and arrest' while progressing to data collection, analysis, and intelligence creation use to prevent and eventually predict adversary actions. In addition, tradecraft is the underlying framework for intelligence upon which military and non-military programs should be built.

Many of the fallacies we face as cyber security professionals relate to a lack of understanding of what it takes to be an intelligence professional. The two are not mutually inclusive. Security operation centers are not populated with intelligence professionals. They are not occupied by analysts skilled in the arts professed by Sherman Kent and documented by Richards Heuer. In fact, most cybersecurity professionals find tradecraft to be distasteful and a general waste of time. This conclusion is drawn from the many engagements across the globe with cybersecurity professionals. When we come onsite to help build the intelligence program, we immediately face resistance if the focus is not on low level, technical activities. Yet most do not have a grasp, respectfully, surrounding the need for a well-built intelligence program that is top-down as opposed to technically oriented, bottom-up. Most have not had training in intelligence analysis or tradecraft. Real world intelligence analysts endure rigor, structure, focused training that specializes in the craft of intelligence analysis. The core function of any intelligence organization. They learn how to think, write, and brief. They study analytic tools, counterintelligence issues, denial and deception, analysis, and warning skills. (Agency, 2007) A1

Another fallacy is that former military intelligence soldiers and National Security Agency staff are skilled in tradecraft. Not to say that they are not capable or that they have not had intelligence courses but the

courses are largely focused on physical, military action. The NSA trains collectors to collect and analysts to analyze and most times, never the twain shall meet. We have direct knowledge of these methods. The protocol is compartmentalization and separate of duties as a higher priority over continuity of effort and understanding. The intent here is to point out that their skills are very focused on many different areas associated with intelligence. Whether the type is signals based or human, the methods do not include the end-to-end scope of traditional intelligence tradecraft. What we have found is their adoption to be much faster, their understanding of the model more inclusive than cyber security professionals. In general, the ability to adapt, adopt, and incorporate the tradecraft model is not a stretch for these men and women due to their backgrounds.

The Daily Crises

We spend countless hours preparing daily reports, responding to daily incidents, and dealing with the issue de jour. Morning standup meetings are preceded by a daily data push many call intelligence. We establish serialized reporting where each day we deliver a threat report; each week a weekly threat rollup; each month a rollup of each week and so on. We spend so much time gathering current data and fighting daily issues we never get to a point where we can actually perform intelligence-type work This is largely self-inflicted. This fallacy in our process ensures we will never have the ability to analyze data based upon historical collection. The collected data is all current. The scope for that data is immediate. The data is not arranged in such a way as to facilitate long-term analysis. Of course there needs to be a balance between the long-term analysis and the short-term reporting. The fallacy is that the short-term reporting is communicated as intelligence analysis product when it is mostly a regurgitation of open source data and vendor reports readily available.

Letting the Enemy Know What We Know

Vendor reports with cute names dot the landscape documenting the tactics, techniques, and procedures (TTPs) of adversaries. Detailed lists of adversary indicators of compromise (IoCs) populate the appendices of said reports. The reports list the capabilities of the vendors verifying their prowess at uncovering adversaries. Adversary mistakes are lauded with great swagger. The reports list many conclusions without citation, with little discussion of likelihoods, limited communication of confidence levels, and no discussion of gaps in their collection, production, or analysis. The reader is left to fully trust the report at face value. The reports positioned as absolute in their reasoning, yet the logic may be poorly crafted. Sweeping conclusions that oversimplify the problem hallmark the reports. Blanket statements used to persuade the reader repeated in the reports serve to hammer home the need to purchase services from these vendors.

Written to market and sell products and services, the reports do not discuss the potential for denial and deception. Could the data be forged or faked before vendor acquisition? Is it possible their collection methods or sensors are in error or misinterpreted? How did the vendor determine source credibility and reliability? Is there any bias in the technology used or human analysis of the data collected? Are adversaries using heuristics to lull vendors into comfort levels of consistency all the while they are deceiving vendors with traditional maskirovka, the well-honed Russian use of deception? The belief is yes; our vendors are being lulled into comfort levels. As we clearly communicate what we know about them, our adversaries adopt new methods to deny and deceive us all the while they continue to project activities that reflect old TTPs. On the contrary we seek and deception as far back as recorded time. The

Trojan horse, double agents, and tactical deception is a strategy that turns the tide of battles. (Hames, 2014) A1

The practice of deception to trigger an action is a key method of generating data that can be turned to intelligence. Triggering an action leads to the collection of data not only from the primary ripple in the so called pond, but from second and third order effects. An old USAF tactic is to circle with fighter jets near the 12-mile limit of a countries ocean border. The jets circle and circle while an RC-135 is nearby collecting data. Eventually, one or both of the jets turns on the afterburners crossing the border. Acquisition radars turn on, missile sites light up, all the while the RC-135 is collecting data. A treasure-trove of information is collected as radio chatter fills the air waves. The jets turn back and the collection slowly subsides. The intent clear. The data collected, great. Our adversaries use the same tactics in the cyber environment to determine our readiness posture, technical capabilities and methods for defense.

Is This Sedition?

The real travesty with the vendor threat reports is the fact that they are openly published. Cyber warfare is upon us. Adversaries and enemies scour blogs, forums, chat rooms and personal websites to piece together information that is used to harm the government, commercial organizations, and individuals. They utilize methods of espionage extracting sensitive data at unprecedented rates. When discovered, cyber security vendors feel a need to publish every TTP, each IoC, and their malware and individual hacker courses of action to the world. The damage done by these actions is pure negligence. Very surprising that the government does not ask the vendors to suppress the details. If one of their own were to release such data, we would be reading reports for charges of treason. The reports serve to bolster vendor sales while informing the enemy what we know about them and their TTPs. Many of these reports reference other vendor reports on the same topic providing circular reasoning that further, albeit falsely, solidifies their conclusions (demonstrated clearly in the reports on Rocket Kitten). This behavior serves to drive the enemy to increasingly creative and undetectable methods of scanning, penetration, and data exfiltration. They change these methods more frequently in light of the constant barrage of vendor reports; many timed just before or during well-known cyber security conferences. The organizations who have penetrated the enemy and adversary forums, chat rooms, and new methods of communication while using the access to learn more about them, may miss the 'frequency change' due to the vendor reports. By frequency change I refer to the old methods of rolling up on a radio frequency, learning about the enemy including alternative frequencies, and making the change to that frequency when the request is broadcast. Today the methods are much more dynamic, the communications many times encrypted, and the changes very subtle.

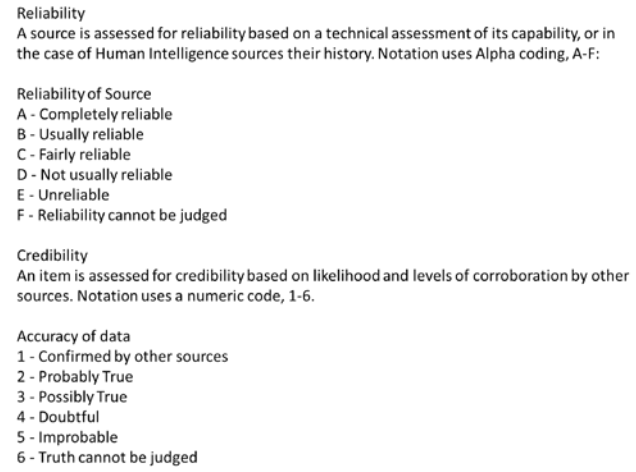

Figure 2 Admiralty Code - Hansen

Fallacies that Create Fault Lines

As discussed above, we believe the fallacies in threat intelligence stem from a lack of agreed upon glossary and taxonomy, the industries acceptance of vendor solutions to provide actual intelligence, vendor reports taken at face value without source validation or citation, organizational placement of intelligence within information security many times incident response, inaccurate understanding of what an intelligence professional is, and the inability of organizations to see beyond purely defensive measures for information security. These fallacies, understood to be non-inclusive, create inherent fault lines in our security programs.

Changing Behaviors

What can we do to rectify the path of fallacies we continually choose to follow?

First (in no specific prioritized order) we must educate everyone in information technology, information security, and the C-Suite on the standard taxonomy of intelligence. This provides a shared understanding and baseline glossary upon which to build communication.

Secondly, we must treat each vendor report as nothing more than another source of data. Data that must be evaluated for credibility, reliability, and relevance. To do so, we can use the NATO Admiralty Code (Figure 2). (Hanson, 2015) A1 used throughout this article to rate sources in the format of (A1, B2, B3, etc.). The code helps organizations evaluate sources of data and the credibility of the information provided by that source. Evaluate each vendor report using this code while documenting ease of data extraction, relevance to your organizational issues, and value in solving your security problems.

TITLE: Use the title to introduce your findings

BLUF:

- What –
- Why now –
- So what –
- Impact so far -
- What next / outlook -
- Implications
- Supervisory Action (actions to be taken based upon data/information/analysis)
  - Recommendations and Opportunities (actions to be taken based upon data/information/analysis)
  - Could be strengths and/or threats converted to be opportunities.
  - Recommended courses of action. Could be strengths and/or weaknesses that can be converted to strengths.

SUMMARY PARAGRAPHS:

Most important point topic sentence (could be most diagnostic piece of evidence)
Explanation / elaboration
Fact / example / illustration # 1 supporting 'Most important point' topic sentence
Fact / example / illustration # 2 supporting 'Most important point' topic sentence
Analysis (answers the question "so what?")

Next most important point topic sentence (could be most diagnostic piece of evidence)
Explanation / elaboration
Fact / example / illustration # 1 supporting 'Next most important point' topic sentence
Fact / example / illustration # 2 supporting 'Next most important point' topic sentence
Analysis (answers the question "so what?")

Third most important point topic sentence (could be most diagnostic piece of evidence)
Explanation / elaboration
Fact / example / illustration # 1 supporting 'Third most important point' topic sentence
Fact / example / illustration # 2 supporting 'Third most important point' topic sentence
Analysis (answers the question "so what?")

Alternative Analysis

Figure 3 Intelligence Analysis Format - SAMPLE

Thirdly, begin to grow and expand your intelligence program functions. Learning methods of anonymity, open source data collection, collection management and planning, production management of intelligence functions, analysis, and analytic writing and dissemination adds immediate value to your organization. Understand that

intelligence is not the same as incident response or a core component of the security operations center. These skills are unique and must be shared but to bury them within these areas is a mistake. We faced this for years (and still do) putting information security under information technology treating it as a solely technical issue. We should not make the same mistake with intelligence. Intelligence functions need direct access to organizational stakeholders.

Fourth, create standard processes to seek out malicious actions within your information technology environment. Use adversary TTPs to drive your 'hunt and detect' but understand that albeit a valuable capability, is not a proactive function. They are already inside the wire and must be removed. Organizations need to do this for proper hygiene.

Fifth, develop methods within your organizational risk model to collect open source data regularly. Like our third point above, we must grow this function so we collection data and information, and develop intelligence that is pertinent to our stakeholders and our organization. Capture priority intelligence requirements, create information requirements prioritized and vetted focusing on all sources of data including open source collection. Devise methods for mission management that drives targeting for passive collection.

> Make note that many vendor report subscriptions provide generalized and generic data and information. Periodically, intelligence is part of the report. Occasionally, something relevant to your organization is included. Most time the reports are of a create once, distribute many format.

Sixth, create a model of your adversaries and their capabilities that are target centric. Expand your collection to include all areas concerning your adversary. The only way to fully understand what threatens your organization is to fully understand the enemy, their motivations, their competence, and their skills. Otherwise, organizations will continue to play a basketball game on defense, never crossing the half-court line. A recipe for assured loss.

Seventh, write in intelligence analysis format. Stakeholders have little time. Making them hunt for the answers ensures failure. Use the guide in Figure 3 to assist in your writing, Intelligence Analysis Format.

Eighth, create a strategic plan followed by a program plan for intelligence in your organization. Define what it is and is not. Author a vision and mission along with guiding principles. Develop a series of goals with three to four objectives determining how to achieve those goals. Gain acceptance and follow the plans.

Ninth, set up a listening tour of your lines of business and corporate stakeholders. Gain permission to attend their meetings with the understanding that you are there to listen and learn. Do not offer your services and listen to digest and gain knowledge of your stakeholders. Do not listen to prepare a response. Gather this information and take it back to your organization to help your program move forward. You may believe you know your company but knowing your professor ensures and 'A.'

Tenth, give your organization time to implement an intelligence function. Determine what makes sense for your organization as to what that timeframe is. Institutionalize lesson-learning as process of performance improvement, not assessing blame. (Gabbard, 2008) B1 Give your intelligence organization time to learn. Making mistakes in the early stages of maturity is expected. Just do not make the same mistakes repeatedly. Give your intelligence organization the authority to make decisions and the access to stakeholders to learn requirements and communicate capabilities. Establish goals and objectives that

are actually reachable and practical. Stretch goals when first building a function can lead to unnecessary failures. Leadership and the right level of leadership is required to manage analysts. Find the right level for your organization. When you add an intelligence function to an organization that has never had one, manage expectations. Eventually, a properly staff, trained, and led group can delivery significant value to the organization.

Lastly, although non-inclusively, prepare your organization for the next steps. Those next steps involve counterintelligence. Although now seen as a high-risk area for organizations, my belief is that we will eventually adopt certain principles associated with this tradecraft. In fact, several organizations already employ methods associated with counterintelligence, both passive and active. In 2011, we adapted the Ten Commandments of Counterintelligence into a list focused on cyber. They are:

1. Be offensive
    a. Do not be afraid to anonymously collect information on your adversaries. In many cases, they are hiding in plain sight. You just need to know where to look.
    b. Cyber intelligence is the basis for cyber counterintelligence. Learning your adversary prepares an organization for counter denial and counter deception.
2. Honor your profession
    a. Learn about intelligence analysis. Leave your security comfort zone.
    b. Take classes in critical thinking. It is never too late.
3. Own the street
    a. Establish a presence on the same sites of your adversaries.
    b. Create multiple personas when doing so.
4. Know your history
    a. The old adage of 'know your history or be destined to repeat it' is in effect.
    b. Know what your adversaries have done in order to determine what they may do.
5. Do not ignore analysis
    a. Analysis is not grown from a server but resides in human skill.
    b. Until such time as artificial intelligence is truly with us, the human mind serves as the best solution for intelligence analysis (if properly trained).
6. Do not be parochial
    a. Share data even if you must do this via back channels. We do not advocate break corporate rules by sharing sensitive data.
    b. Quid pro quo sharing is required.
7. Train your people
    a. Understand your needs, understand the timing of those needs, and drive for increased training budgets.
    b. The best investment you can make is in yourselves.
8. Do not be shoved aside
    a. Gently push your way into business meetings establishing a 'listening tour.'
    b. Clarify what intelligence is and is not.
9. Do not stay too long
    a. Fully document your actions while periodically shifting targeting assignments to stay fresh.
    b. Rotate assignments to learn every facet of the intelligence game.

10. Never give up (Bardin, 2011) B2
    a. Perseverance and patience are required.
    b. Our adversaries do not operate under the same rules of engagement that hampers our actions.

Much like information security a short 15 years ago, cyber intelligence is in its infancy and largely misunderstood. We are rife with fallacies, inaccurate definitions, and terminology usage. The profession of intelligence should not be confused with security and should not be clouded by poor and biased reporting. The only way to change the problems inherent in intelligence today is to drive that change internally while forcing the market to shift. The CIA realized this years ago striving to create the 'profession of intelligence analysis.' The framework of intelligence can and should be the underlying standard for strategic intelligence planning and program builds.

This comes with frequent constructive criticism of vendor delivered products and services. I have always said the best investment you can make in life is in yourself. Organizations should consider doing the same. Educate your staff. Plan your program. Drive the change from the inside.

For a summary of this article, see the first section.

Jeff Bardin
Treadstone 71

Agency, C. I. (2007, April 25). *Offices of the CIA*. Retrieved from Central Intelligence Agency - Training Resources: https://www.cia.gov/offices-of-cia/intelligence-analysis/training-resources.html

Bardin, J. (2011). *The Ten Commandments of Cyber Counterintelligence.* Boston: CSO Online.

Davis, J. (2007, April 21). *Sherman Kent and the Profession of Intelligence Analysis*. Retrieved from CIA Library: https://www.cia.gov/library/kent-center-occasional-papers/vol1no5.htm

Gabbard, T. a. (2008). *Assessing the Tradecraft of Intelligence Analysis.* Retrieved from Rand Corporation Published Research: https://www.rand.org/content/dam/rand/pubs/technical_reports/2008/RAND_TR293.pdf

Gartner. (2013, May 13). *Threat Intelligence*. Retrieved from Gartner Definition: Threat Intelligence: https://www.gartner.com/doc/2487216/definition-threat-intelligence

Government, U. (2013, October 22). *Joint Intelligence*. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf

Government, U. (2013, February 21). *Office of the Director National Intelligence*. Retrieved from www.dni.gov

Hames, J. (2014, September). *Strategic Trickery: The U.S. Army's Use of Tactical Deceoption*. Retrieved from Soldiers - The Official U.S. Army Magazine: http://soldiers.dodlive.mil/2014/09/strategic-trickery-the-u-s-armys-use-of-tactical-deception/

Hanson, J. (2015). *The Admiralty Code - A Cognitive Tool for Self-Directed Learning.* Sydney: JM Hanson. Retrieved from www.ijlter.org/index.php/ijlter/article/download/494/234

InfoSecurity, M. (2015). *Threat Intelligence: Collecting, Analysing, Evaluating.* London: MWR InfoSecurity. Retrieved from https://www.mwrinfosecurity.com/assets/Whitepapers/Threat-Intelligence-Whitepaper.pdf

Security, N. (2016, September 9). *Threat Intelligence Defined - 1260wp.* Retrieved from Threat Intelligence Defined - Solutionary: https://www.solutionary.com/_assets/pdf/white-papers/threat-intelligence-defined-1260wp.pdf