Bias in Analysis 2.0: Let Sleeping Dogs Lie

Brian Myers

Center for Development of Security Excellence

ED 520 01 SP21

Professor Jackson & Professor Gentle

April 18, 2021

Summary

In the past 20 or 30 years, large-scale events have brought into question the analytical rigor of the Intelligence Community. Brian Myers' essay argues that a major challenge to combatting Insider Threats is the tendency of individuals to bring their own biases into threat analysis. He begins with a history of cognitive biases of intelligence analysis in the early years of the Central Intelligence Agency (CIA) and strides within the intelligence community (IC) that led to the birth of different tools, including the Analysis of Competing Hypotheses (ACH) and the Rating Scale. However, despite these strides forward, he cites hubris within the IC as a barrier to fully overcoming cognitive biases. To prevent bias in the Counter Insider Threat community, Myers recommends Insider Threat Programs (InTPs) use a myriad of training resources and awareness campaigns to build critical thinking skills and to increase community understanding of such programs so that there is an added layer of accountability on such programs. He also provides a set of accessible analytical aids and techniques to combat cognitive biases and to elevate the severity of this issue among InTPs.

Bias in Analysis 2.0

Since time immemorial, there has existed analytical bias that at best yielded an oracle-like approach to analysis. At worst, a reliance on coincidental and anecdotal events served to confirm biases. This is especially the case when there is a paradigm shift or a revisited science that gives the false sense that none of the old is needed in this brave new world. The same goes for the new archetype of insider threat versus the Intelligence Community's (IC) dated modus operandi of analytical products. Nevertheless, the IC has enjoyed a renaissance of sorts regarding unbiased analytical products (Heuer, 2020). This writer seeks to show the most comprehensive multidisciplinary approach to insider threat will likely nullify if the human tendency of analytical bias is not adequately addressed. In other words, let the sleeping dogs of cognitive biases lie and

instead let loose the cats of Structured Analytical Techniques (SAT) with their nine lives of critical thinking skills.

History of Analysis

While it could be more beneficial to perform a more exhaustive historical context of analysis, this paper will have as its starting point in the early days of the Central Intelligence Agency. Moreover, within the CIA, Sherman Kent's trailblazing contributions to the analytical profession will be the most relevant (Heuer, 2020). Kent, a professor at Yale, worked in the Research and Analysis Branch of the CIA's predecessor, the Office of Strategic Services. It is said he "advocated application of the techniques of 'scientific' study of the past to analysis of complex ongoing situations and estimates of likely future events" (Heuer, 2020). However, in his championing the cause of impartial and scientific analytic products, it was not until Robert Gates served as the Deputy Director for Intelligence (DDI) in 1982-1986 that the most significant positive impact was made to CIA analysis. DDI Gates was adamant about the separation of fact from opinion by his analysts. He has identified the need for outsiders or expertise in academia and in the policy arena to help "present alternate future scenarios" (Heuer, 2020). Then Doug MacEachin, the DDI from 1993 to 1996 and an economics major who spent a lot of time in a "policymaking office," took on a different but helpful perspective to analysis. He promoted a methodology to structured argumentation that played on semantics to get more buy-in from analysts. For example, he used "drivers" instead of "key variables," and important drivers in a "hypotheses" became 'lynchpins.' DDI MacEaching made an important stride when his "standards for analysis was incorporated into a new training course, 'Tradecraft 2000'" (Heuer, 2020).

Once the Sherman Kent School for Intelligence Analysis in 2000 was created, John McLaughlin, the then CIA Deputy Director for Intelligence, placed a high emphasis on the consolidation of techniques for alternative analysis. This "red-team" analysis was taught as the Advanced Analytic Tools and Techniques Workshop (Heuer & Pherson, 2021). In 2005, the Kent School formally approved the updating of training materials from "alternative analysis" to Randy Pherson's "Structured Analytic Techniques" (Heuer & Pherson, 2021).

Milestones

Thinking about Thinking

It was not until a retired former head of the methodology unit in the Directorate of Intelligence's political analysis office, Richards Heuer, that a momentous paradigm shift took place. Dick Heuer, in his effort to expose the cognitive challenges or biases of intelligence analysts, developed some groundbreaking yet straightforward tools. He posited that "alternative hypothesis need to be carefully considered especially those that cannot be disproved on the basis of available information," and thus, his "Analysis of Competing Hypotheses" (ACH) was born (Heuer, 2020). This Structured Analytic Technique is currently part of a pantheon of tools that include exploration, diagnostic, reframing, foresight, and decision support techniques that are available to the analyst (Heuer & Pherson, 2021).

Analytic Standardization

The Intelligence Community Directive 203 (ICD 203) is perhaps one of the most notable milestones in the Intelligence Community that came as a result of the pursuit of improvement and standardization of analysis. Born from the National Security Act of 1947, the Intelligence Reform and Terrorism Prevention Act of 2004 (ODNI, n.d.), and Executive Order 12333, the ICD 203's purpose is to "serve as a common IC foundation for developing education and

training in analytic skills" (McConnell, 2007). ICD 203 also has primary Standards of objectivity, independence from political considerations, and the nine Analytic Tradecraft Standards implementation and exhibition. While an excellent approach to mitigating cognitive biases was found in the analytical community, the most readily available rubric was the Rating Scale (McConnell, 2007). Developed by the Office of the Director of National Intelligence's Analytic Integrity and Standards (AIS) Group, it provides a tool that contains rating levels and also "describes the process raters should use in evaluating a report" (McConnell, 2007).

Bias in Analysis 1.0

In the past 20 or 30 years, large-scale events have brought into question the analytical rigor of the Intelligence Community. Arguably the largest event was the intelligence failures of the 9/11 attacks that were owed mainly to the inherent siloing of information within the United States intelligence apparatus (Harknett & Stever, 2011). The investigation that ensued by the 9/11 Commission that culminated with a 585-page report was quite transparent on this lack of unity within the IC (Harknett & Stever, 2011). Nevertheless, it was not long before the implementation of intelligence reform that another intelligence blunder was to highlight the Intelligence Community's "new clothes": The 2003 invasion of Iraq. The years that followed the war have highlighted the lack of objectivity and were fraught with political considerations that the White House imposed on the entire IC (Hammond, 2020). Also, the Department of State's Bureau of Intelligence and Research (INR) and the Department of Energy were the only ones with a dissenting opinion of Iraq's Weapons of Mass Destruction (WMD) capabilities (Hammond, 2020). If there was still any possible doubt about Iraq's WMD program or lack thereof, the main informant, code-named Curveball, admitted that it was a complete fabrication (Risen, 2011).

Restating the Problem

While it is easy to look back at these events and criticize both the decision-makers and the intelligence analysts for their cognitive biases, it is not beneficial, especially as case studies. In fact, one would be falling into a cognitive trap, a variation of a confirmation or even hindsight bias that ignores any evidence to the contrary. Heuristics also play a role since they are experientially based and are able to yield fast answers but can sometimes be wrong (Heuer & Pherson, 2021). These traps highlight the need for checking these biases at the door. So, while the IC is apparently addressing these sleeping dog biases in everyone, there is a risk of the insider threat community running a raging bull into the middle of the analytical china shop. With so many subject matter experts likely found within a Fully Operational Capable (FOC) Insider Threat Program (InTP) Hub, it can cause the same hubris that went unchecked in the IC.

It would be easy to look at a highly trained, fully staffed, and full-time InTP Hub with its security, cyber, legal, human resources, personnel security, counterintelligence, law enforcement, and behavior science pillars (Morgan & Ransdell, 2020) and think that cognitive biases cannot exist. However, groupthink or a false consensus effect thrives in such environments (Cherry, 2021). A focus can be so centered on the insider threat that one could miss one's own insider threat to objective analysis. Incidentally, as seen with the intelligence blunder of the Iraqi War, the vulnerability to bias in the analysis was not just limited to analysts; it was found with the decision-makers and customers as well (Risen, 2011).

Countering Counter-InTP Bias

Training

While rigorous research contributions from organizations like Carnegie Mellon University's Software Engineering Institute (SEI) and the Defense Personnel and Security

Research Center's (PERSEREC) Threat Lab have yielded a veritable boon of information on countering the insider threat, there does not seem to be a huge emphasis on the behavior of InTP Hub representatives. While the IC has expended a great deal of time and energy towards countering analytical bias, with the exception of the Center of Development of Security Excellence's (CDSE) Critical Thinking for Insider Threat Analysts course (INT 250.16), it is difficult to find any such focus anywhere else.

Fortunately, U.S. Government (USG) departments and agencies can access most courses that are offered to intelligence analysts. Courses like those found within the CDSE have excellent unclassified online offerings for anyone and not just USG departments and agencies. There is also the National Intelligence University, located in Bethesda, Maryland, and the Naval Postgraduate School located in Monterey, California, with their many certifications and intelligence degrees that would likely prepare anyone desirous of honing and developing their analytical skills. However, these are out of reach for most and require a great deal of commitment and time that most Insider Threat professionals do not have.

Another training resource that is offered online, accessible to anyone, and offers the same Structured Analysis Techniques within the Intelligence Community is called Globalytica (Pherson, 2018). Founded by a married couple, Katherine and Randolph Pherson, who retired from the CIA with a combined 50 years of experience as analysts, also pioneered and developed Structured Analytical Techniques. Mr. Pherson collaborated with Dick Heuer in launching the Analysis of Competing Hypotheses or ACHs (Pherson, 2018).

Awareness

The awareness of cognitive pitfalls has to be thorough. In other words, it should not be limited to the analytical cadre but should be inclusive of the decision-makers and the rest of the

workforce. Even though this kind of buy-in is more challenging, it would be more rewarding. However, insider threat awareness training could take a month to dedicate it to the critical-thinking aspect of insider threat. It could be a type of bring-a-kid to work day, but more of a bring-an-employee to workday instead. For example, one could take National Insider Threat Awareness Month and use it as a day to learn about what the InTP Hub does, turn the month into an InTP Fair of sorts, or bring out the games that challenge people to use critical-thinking skills while giving an appreciation for the pillars represented in the InTP Hub.

At the core of any awareness campaign, the idea is to have the participants see segues of insider threat in everything they do. All InT programs' raison d'être is the safety and security of its insiders. However, if the workforce does not participate in the program, the department or agency will likely be blind to the internal threats. In other words, the insiders are the perimeter sensors to the insider threat.

Biased on Biases

There is a saying that "if it ain't broken, don't fix it!" Perhaps the InTP Hub is not in any danger of bias in analysis, or at least not enough that it cannot be overcome, for example, with a comprehensive standard operating procedure. After all, Insider Threat Programs are rarely identical. From an enterprise-level and fully staffed DITMAC, or a one-man show at a small NT-50 agency, the squeeze might not be worth the juice to get everyone trained as an analyst. In fact, some might conclude that since counterintelligence is part of the IC and has been handling insider threats, let them also be in charge of countering the cognitive pitfalls for the group. Even dedicated analysts in some InTP Hubs can act as the gatekeeper for all things analytical.

Due to the availability of redacted IC case studies, insider threat professionals have plenty of examples that should be sufficient in the prevention of those same analytical pitfalls. Perhaps

that like the IC, “the fundamental problem, still unrecognized by most members of the general public and all too many government officials, is that intelligence can never be right all the time, even on the most important issues on which it concentrates the bulk of its resources” (Beebe & Pherson, 2014). It appears that for various reasons, the customers’ expectations are not being managed. It is possible that a plethora of analysts, or InTP Hubs for that matter, are over just promising and under-delivering.

History Repeating

While there are undoubtedly many fronts to the insider threat problem, one should not dismiss cognitive biases as one of them. These cognitive pitfalls should be addressed in the insider threat-scape just as definitively as it has been in the IC. Furthermore, if the Intelligence Community saw it as a problem that needed to be addressed, it should be the same for every InTP Hub. Insider Threat professionals should focus on tapping into as many available resources on the issue. Thankfully, the IC has perfectly done much of the legwork that should be assimilated and applicable to an InTP Hub. One should seek not to repeat the history of mistakes in the IC and instead duplicate their best and most appropriate responses.

SATs

At the risk of bringing back the terrible memories of college entrance exams, this writer seeks to focus on the step-by-step process that externalizes the analyst’s thinking: Structured Analytical Techniques or SATs. The reason for such a focus stems from its applicability as an analytical tool that masterfully incorporates both critical thinking and analytical thinking skills. The previously mentioned collaboration between retired CIA analysts Dick Heuer and Randolph Pherson, has since expanded into a veritable pantheon of accessible analytical aids. These techniques start with the basics of getting organized: “checklists, sorting, ranking and organizing

your data" (Heuer & Pherson, 2021). Then the SATs are broken down into the following categories:

Exploration Techniques. The nine techniques include several types of brainstorming, including Circleboarding, Starbursting, and Cluster Brainstorming.

Diagnostic Techniques. The eleven techniques covered involve widely used ones such as Key-Assumptions Check and Chronologies and Timelines. The Cross-Impact matrix and several techniques that fall in the domain of hypothesis generation and testing to include Analysis of Competing Hypothesis ACH.

Reframing Techniques. The sixteen techniques in this family help analysts break away from established mental models by using Outside-In Thinking, Structured Analogies, Red Hat Analysis, Quadrant Crunching, and the Delphi Method to reframe an issue or imagine a situation from a different perspective.

Foresight techniques. This family of 12 techniques include 4 new techniques for identifying key drivers, analyzing contrasting narratives, and engaging in counter factual reasoning.

Decision Support Techniques. The ten techniques in this family include three new Decision Support Techniques: Opportunities Incubator, Bow Tie Analysis, and Critical Path Analysis (Heuer & Pherson, 2021).

Precursor

A crucial point that has to be made is that preparation of sorts has to be done before the application of these tools. In other words, one has to understand that critical thinking skills are the precursor to a robust analytic capability (Morgan & Ransdell, 2020). Moreover, with this solid analytical capability, one can begin to wield the techniques mentioned above. It is also

essential to understand that there is also a need for empirical and quasi-quantitative analysis that is usually found within the Cyber/IT pillar where the User Activity Monitoring (UAM) and the Security Information and Event Management (SIEM) reside (Cappelli et al., 2012).

Another very important consideration is that "unfortunately for analysts, these biases, heuristics, and traps are quick to form and extremely hard to correct" (Heuer & Pherson, 2021). This means that all the preparation and pinpoint matching of Structured Analytic Techniques might not be as helpful.

Matchmaking

Perhaps it would be of more significant benefit at this point to actually match the cognitive limitation to the structured technique, much like the second day of the National Insider Threat Task Force Hub Ops course when one starts to get hands-on with the case studies and go from theory to practice. For example, if the cognitive bias is Confirmation or Evidence Acceptance bias, then the SAT that would most likely apply is the Diagnostic, which helps the analyst overcome relying on first impressions and ignoring inconsistent evidence. If one suspects the InTP Hub of Groupthink or Premature Closure, one or more of the 10 Decision Support Techniques would help avoid the intuitive trap of overrating behavior factors and overestimating probability (Heuer & Pherson, 2021).

Wheel Reinventing

The idea behind adopting Structured Analytic Techniques into the insider threat-scape is not to reinvent the wheel but to make a better mousetrap. In other words, it is to structure how one thinks about thinking and to be as transparent as possible in the process but not to create a new way of doing things. Just as every InTP Hub's mission is to deter, detect, and mitigate the insider threat, it is the same goal when it comes to cognitive biases. Just as risk cannot be entirely

avoided, one cannot expect with 100% certainty that the insider threat professional has not fallen into one or more of these traps.

However, if one hones critical thinking skills, follows analytical tradecraft standards, and employs Structured Analytic Techniques, a high degree of confidence can be placed on the mitigation efforts of any incident. This individual effort quickly becomes synergistic when all who are supporting the InTP Hub have the same approach. If one looks at "structured techniques as "thinking tools," analysts can use them to instill more rigor, structure, and imagination in the analysis" (Heuer & Pherson, 2021); then one can understand its benefit.

Conclusion

Perhaps one of the greatest of humanity's conundrums is the apparent inability to learn from history. Moreover, this could very well be due to complete disregard for addressing one's cognitive biases. It is as if human beings do not focus enough on questioning or at least investigating their thinking about thinking. However, the insider threat professional cannot afford to not reflect on their own bias and thought patterns. Not only does he or she have to contend with the thinking and behavior of the insider threat, but with their own thinking as well. The critical thinking skills that are needed to analyze such a complex and rapidly evolving insider threat-scape properly are in some ways daunting, so much so that technological advances in quantum computing (Coleman, 2020) and artificial intelligence will undoubtedly be needed to deal with the moving targets of insider threats.

For this reason, it is all the more important that one adopts the hard lessons learned by the forerunners of the Insider Threat Community. The Intelligence Community, and in particular the counterintelligence components, have been deterring, detecting, and mitigating for quite some time. They have also had their shares of intelligence failures that came mainly in part due to the

unseen enemy of biases in analyses. The IC appears to be making great strides in addressing this persistent foe of objective analysis, and the Insider Threat Program Hubs must take advantage of this.

Only time will tell if the Insider Threat Community will rise above the persistent threat of bias in analysis and mitigate them in the most prejudicial manner. If not, the most comprehensive multidisciplinary approach to insider threat will likely nullify if the human tendency of analytical bias is not adequately addressed. In other words, let the sleeping dogs of cognitive biases lie and instead let loose the cats of Structured Analytical Techniques (SAT) with their nine lives of critical thinking skills.

References

Beebe S. M., & Pherson R. H. (2014). *Cases in Intelligence Analysis: Structured Analytic Techniques in Action*. [Liberty University Online Bookshelf]. Retrieved from https://libertyonline.vitalsource.com/#/books/9781483340142/

Cappelli, D., Moore, A., & Trzeciak, R. (2012). *The Cert guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud)*. Addison-Wesley.

Cherry, K. (2021, January 20). *Types of Cognitive Biases That Distort How You Think*. Verywell Mind. https://www.verywellmind.com/cognitive-biases-distort-thinking-2794763.

Coleman, K. (2020, June 8). *The Security Implications of Quantum Technology*. Security Magazine RSS. https://www.securitymagazine.com/articles/92545-the-security-implications-of-quantum-technology.

Hammond, J. R. (2020, March 19). *The Lies that Led to the Iraq War and the Myth of 'Intelligence Failure'*. Foreign Policy Journal. https://www.foreignpolicyjournal.com/2012/09/08/the-lies-that-led-to-the-iraq-war-and-the-persistent-myth-of-intelligence-failure/.

Harknett, R.J. and Stever, J.A. (2011), The Struggle to Reform Intelligence after 9/11. Public Administration Review, 71: 700-706. https://doi-org.ezproxy.liberty.edu/10.1111/j.1540-6210.2011.02409.x

Heuer, R. J. (2020). *Psychology of intelligence analysis*. ProQuest Ebook Central http://ebookcentral.proquest.com

Heuer, R. J., & Pherson, R. H. (2021). *Structured analytic techniques for intelligence analysis*. SAGE/CQ Press.

McConnell, M. (2007, June 21). *Intelligence Community Directive Number 203: Analytic Standards (Effective June 21, 2007)*. Homeland Security Digital Library. https://www.hsdl.org/?abstract&did=479263.

Morgan, R. & Ransdell, S. (2020). Foundations of Insider Threat Management [PowerPoint slides].Center for Developing Security Excellence, Defense Counter Intelligence and Security Agency. https://sakai.cdse.edu/access/content/group/2df5604a-22c2-4312-91eb-a8cd73537e88/Power%20Point%20Presentations%202020/Lesson%204%20-%20A%20New%20Paradigm%2C%2020201103%2C%20Narration%20for%20Sakai.ppsx

ODNI Home. Intelligence Reform and Terrorism Prevention Act of 2004*. (n.d.). https://www.dni.gov/index.php/ic-legal-reference-book/intelligence-reform-and-terrorism-prevention-act-of-2004

Pherson. (2018, November 1). Globalytica. http://www.globalytica.com/about/founders/.

Risen, J. (2011, February 16). *Iraqi Says He Made Up Tale of Biological Weapons Before War*. The New York Times. https://www.nytimes.com/2011/02/16/world/middleeast/16curveball.html.