CREATIVE CHOICES: DEVELOPING A THEORY OF DIVERGENCE, CONVERGENCE, AND INTUITION IN SECURITY ANALYSTS

CHRIS SANDERS
STEF RAND
APPLIED NETWORK DEFENSE

ABSTRACT

Humans lie at the heart of computer network defense. Despite the essential nature of analysts' cognition in investigations, there have been few systematic attempts to understand how security analysts think during the investigation process. In this study, we set out to develop a better understanding of the cognitive processes of information security analysts. We hypothesized that divergent and convergent thinking styles would be highly influential during the creative problem solving required to find investigative solutions successfully. We interviewed security analysts and observed their use of divergent and convergent thinking in investigation scenarios. We also measured their skill level and their metacognitive awareness. We found that intuition, ambiguity tolerance, metacognitive deficiencies, and the context of the investigation changed analysts' use of divergent and convergent thinking. We use these findings to build the ambiguity-driven convergence model for analyst thinking, as well as to suggest several practical applications to deliberately leverage divergent and convergent thought for higher quality investigations.

KEYWORDS

Information Security, Cyber Security, Digital Forensics, Incident Response, Security Operation Center, Security Analyst, Security Investigation, Divergent Thought, Convergent Thought, Creativity, Intuition, Ambiguity, Creative Problem Solving, Qualitative Research

Humans lie at the heart of computer network defense, particularly those serving in an investigative role. Through the systematic inquiry and examination of evidence, security analysts piece together anomalous events and system behaviors to build an attack timeline that represents the interaction between an intruder and organizational network assets. Using this timeline, analysts identify the scope of the attack for containment, eradication of the attacker, and eventual restoration of normal network activity.

Analysts are often first responders, diagnosticians, and rehabilitation therapists all at the same time. As the number and severity of attacks against public and private computer systems increases, so does the need for skilled analysts. In spite of growing demand, many job roles remain unfilled and universities struggle to produce job-ready graduates. Even experienced analysts actively employed in security operation centers (SOCs) are often incapable of describing how they connect the dots of an investigation.

There is an insufficient amount of research focusing on analysts' underlying cognitive processes considering society's reliance on this technical specialization. Most analyst jobs are built on a foundation of tacit knowledge passively transmitted through unstructured on-the-job training and brute force repetitive learning (Sunduramurthy et al., 2014). Failures are amplified because they can result in prolonged, meaningful compromises of sensitive information systems. Formal post-secondary and private network security education exists but is primarily centered on tools and rarely contains a cognitive component that teaches analysts how to think about their role. Typical hallmarks of well-developed and understood fields include robust mental models and peer-reviewed, research-based best practices. Information security as a discipline lacks these qualities, to the detriment of new analysts and experts alike.

In an anthropological study of SOCs Sundaramurthy et al. (2014) reported the following:

> *SOC analysts often perform sophisticated investigations where the process required to connect the dots is unclear even to the analyst. Doing the job is more art than science. (p. 5)*

> *Cybersecurity practitioners often work from hunches or intuitions. They know what to do, where to look, and how to investigate a case but often can't state this knowledge explicitly. SOC jobs such as incident response and forensic analysis have become so sophisticated and expertise-driven that understanding the process is nearly impossible without doing the job. (p. 4)*

To keep up with the growing threat landscape and societal dependence on technology, information security practitioners must better understand their own methods for defending networks. The foundation of tacit knowledge must be made more explicit so that new analysts can be identified, trained, and placed into job roles with a better chance to succeed.

With that in mind, we seek to build explicit knowledge through the exploration of successful analysts' thought patterns. We have observed the use of divergent and convergent thought by successful analysts, but no theory exists that explains how these mental constructs are applied to investigative problem-solving. The purpose of this study is to understand the cognitive processes of information security analysts and develop a theoretical framework explaining how analysts use divergent and convergent thought during the security investigation process.

BACKGROUND

Metacognition is knowledge and cognition about cognitive phenomena (Flavell, 1979). To put it more simply, metacognition is thinking about your thinking. Metacognition is further divided into two dimensions, knowledge and regulation (Hargrove & Nietfeld, 2015). Knowledge of cognition is one's explicit knowledge of declarative and procedural memory; regulation of cognition is knowledge of one's planning, self-monitoring, and self-evaluation (Hargrove & Nietfeld, 2015). Greater metacognitive awareness makes you a better learner and problem-solver. If you are aware of what you know and how well you know it, you can understand the relationship between knowing and doing, which is important for effective problem solving and meeting your cognitive goals (Hargrove & Nietfeld, 2015). Another benefit to metacognitive awareness is the ability to consciously use specific thinking styles and strategies. Two thinking styles we think are key to improved problem solving are divergent thinking and convergent thinking (Plumlee et al., 2015).

Divergent thinking starts from a single point of available information and generates multiple, varied ideas that may differ greatly from person to person (Brophy, 2001; Cropley, 2006). Convergent thinking, in contrast, starts from multiple points and seeks one conclusion that can be identified as the one which is most "true or useful" (Brophy, 2001). Convergent thinking shines in situations where an answer exists and needs to be remembered or worked out from already-held knowledge (Cropley, 2006).

Creativity, as defined by Mednick (1962), is "the forming of associative elements into new combinations which either meet specific requirements or are in some way useful. The more mutually remote the elements of the new combination, the more creative the process or solution" (1962, p. 221). Creativity is more than the cognitive activity of creating new things;

more holistically, creativity is both a behavioral action and a series of traits that lead to engaging in creative behavior (Guilford, 1950). Creativity has historically been studied as a primarily divergent process that generates novel and varied ideas (Tan, 2015). Recently in the literature there is a shift toward a broader understanding of creativity as a process that uses both divergent and convergent thinking (Cropley, 2006). Divergent thinking involves ideation, defined as the act or process of creating new ideas. Convergent thinking helps evaluate those new and novel ideas. Theoretically, divergent and convergent thinking are used in different and alternating phases of the creative process (Cropley, 2006).

The creative process we are most interested in studying is the creative problem solving process used by analysts in information security investigations. In creative problem solving, according to Brophy (2001), problems are defined before they are studied. Solutions are generated and then chosen. This process results in creative phases similar to Cropley's theorized pattern; a back-and-forth between ideation and evaluation, divergent and convergent thinking, which helps the problem solver find the most useful conclusion (Brophy, 2001). This brings us back to metacognitive awareness and conscious use of divergent and convergent thinking to creatively solve problems. Problem solvers who received training in divergent and convergent thinking generated more explanations and better solutions (Plumlee et al., 2015).

If divergent and convergent thinking results in better solutions to problems, intentionally using these thinking styles could yield better results faster in security investigations. Establishing the patterns of divergent and convergent thinking specific to information security analysis would be useful for training new analysts and for improving the process of experienced analysts. It is a challenging prospect to measure and assess thinking styles in security analysts who have low levels of metacognitive awareness when it comes to the investigation process (Sunduramurthy et al., 2014). Studies of creativity, metacognition, and creative problem solving have determined a number o behaviors and personality traits are associated with and predictive of divergent and convergent thinking, as described below.

DIVERGENT TRAITS

One of the defining features of divergent thinking is the generation of numerous and varied ideas through ideation (Brophy, 2011). Sometimes divergent thinkers combine previously created ideas in novel ways or reinterpret prior concepts in a new or fresh way. (Kirton 1987; Martinsen, 1995; Mumford et al., 1993).

Another hallmark of divergent thought is the identification of new problems and the creation of new solutions (Brophy, 2001). Innovation is a word commonly used for these divergent processes and is a trait frequently attributed to divergent and creative thinkers.

Divergent thinking requires reason; divergent reasoning comes from a place of reflection and insight (Gough, 1979) where ideas are arranged intuitively and in parallel patterns (Brophy, 2001).

Intuition is, for the purposes of this study, defined as a vague anticipatory perception that orients creative work in a promising direction (Policastro, 1995). While intuition is not solely a divergent process, it is frequently closely associated with divergent thinking in the literature (Cropley, 2006).

Ambiguity tolerance is defined as the tendency to be comfortable with stimuli that have unclear meanings open to alternate interpretations (Brophy, 2001). Divergent thinkers have higher ambiguity tolerance (Brophy, 2001). Resisting premature closure and being comfortable having little past experience with a problem are related traits seen in divergent thinkers (Farley, 1986; Kirton, 1987; Martinsen, 1995).

CONVERGENT TRAITS

A key feature of convergent thought, when compared to divergent thought, is the almost exclusive use of previously created ideas with little to no creation of new ones. Convergent thinkers tend to adapt and re-apply the known to improve existing paradigms, problems, and solutions (Brophy, 2001; Cropley, 2006).

Convergent thinkers use reason to judge or evaluate previously created ideas according to various standards such as logic or fact (Brophy, 2001). Convergent thinkers are observant and able to see limits and weaknesses as part of the idea evaluation process when assessing idea feasibility (Cropley, 2006). Convergent thinkers also quickly recognize familiar ideas and patterns (Cropley, 2006).

Convergent thought, unlike divergent thought, is related to lower ambiguity tolerance. Convergent thinkers display a lack of comfort with unclear meanings or stimuli open to alternate interpretations (Brophy, 2001). Convergent thought is correlated with a preference for certainty and occasionally with a tendency to seek premature closure while problem solving (Gough, 1979; Isaksen et al., 1993; Puccio et al., 1995).

We theorize that these behaviors and traits can be used as observable, measurable phenomena that will give us insight into how analysts think during their investigations. Even if the analysts cannot clearly state how they are thinking about a problem, they can tell us what they are thinking, how they are feeling, and what they might do in a given situation. By asking them questions about their investigative process and observing their creative problem solving in real-time, we can begin to categorize displayed behaviors and traits based on the type of thinking they are connected to in the literature. Analyzing the frequency of divergent and convergent behaviors and noting where they take place in an investigation is the goal of this study. We can then use this data as a basis for a theoretical cognitive model of how analysts approach security investigations.

RESEARCH METHODS

We chose a primarily qualitative, grounded theory-like approach (Strauss & Corbin, 1998) due to the lack of causal and correlational knowledge of factors that make up analysts' applied thought patterns. This research design allowed us to iteratively collect and analyze data and reflexively amend our approach to best capture and understand relevant data.

We additionally used quantitative self-report measures to assess analysts' professional skill level and metacognitive awareness. This data allowed for additional insight when combined with the qualitative interview data.

Overall, this study used a mixed-method grounded theory and survey-based approach to develop a theoretical understanding of how information security analysts use divergent and convergent thinking throughout their investigations.

SAMPLING

We used purposeful, criterion-based sampling to identify and select analysts representative of the broader population (Patton, 1990). Inclusion criteria for this study were practicing security analysts in a primarily investigative role (alert/event analyst, incident responder, malware analyst, threat hunter, intelligence analyst), at least one year of security experience, and fluency with the English language. Exclusion criteria included having taken Chris Sanders Investigation Theory course, as that class teaches divergent and convergent thinking techniques and exposure may bias analysts towards specific thought processes. Theoretical sampling was used in an attempt to ensure we had a sample of participants that would allow us to explore any potential differences in thinking across a full spectrum of analyst skill levels from novice to expert.

Participants were primarily recruited through social media, semi-private chat rooms, and mailing lists. Demographic information was collected to ensure an appropriate distribution of self-reported skill levels and investigative specialties. Participants were offered a chance to win a free seat in an Applied Network Defense training course if they completed all required research tasks, with the winner drawn at random amongst all participants.

DATA COLLECTION

Quantitative

Participants completed a self-assessment questionnaire comprised of three parts:

- Expertise: Participants were asked to self-rank their level of expertise on a 3-point scale as Junior (1), Intermediate (2), or Senior (3).
- Analyst Skill Inventory (ASI): As no prior measure of security analyst skill exists in the literature, we created a measure to more precisely assess analysts' self-reported skill level. Respondents were asked to report their level of agreement with a 5-point Likert scale, with 1 being “strongly disagree” and 5 being “strongly agree,” across 23 items measuring aptitude for using various security tools, investigation heuristics, reflexive behavior, and comfort with different types of evidence.
- The Metacognitive Awareness Inventory (MAI): We chose the MAI to measure metacognition, as adapted by Harrison & Vallin (2017). Respondents were asked to report their level of agreement with a 5-point Likert scale, with 1 being “strongly disagree” and 5 being “strongly agree,” across 19 items organized into two subscales measuring knowledge of cognition and regulation of cognition.

The participants completed the quantitative portion of the study using Survey Monkey, an online assessment tool. The results were downloaded as Excel spreadsheets for analysis. Quantitative data analysis was performed by the co-investigator and reviewed by the principal investigator.

Qualitative

We conducted online audio/video interviews using web conference software following participants’ completion of the quantitative surveys. Interviews were semi-structured using pre-written questions but were flexible enough to permit more in-depth exploration of new ideas or themes. The interviews began with an information security related problem-solving scenario which we asked the analysts to walk us through, followed by a series of questions about their general investigation process. Interviews ended with a second information security problem-solving scenario. We added, modified, and removed questions as needed to support research goals based on preliminary data analysis. The interviews were conducted by the principal researcher. Interviews were recorded with the permission of the participants and transcribed verbatim. The transcribed interviews were entered into the Atlas.TI program for qualitative data analysis. The lead investigator performed open, axial, and selective coding.

SAMPLE SIZE

The criterion for sample size in grounded theory studies is theoretical saturation (Strauss & Corbin, 1998). According to theoretical saturation, data should be collected until each theme of the study has been saturated, constituting a representative sample.

Forty-nine security analysts volunteered to participate in the study. Of those 49, 20 were selected to form an initial pool of participants, and 16 completed the study. Four participants did not complete all portions of the study.

Using theoretical saturation, we examined our interviews to determine the need for further sampling. Based on the quality of the information provided by the analysts and the clear patterns which emerged across most or all of the participants, sampling was completed with 16 participants. The demographic characteristics of the participants are included in Table 1. Four of the analysts were women, and 12 were men. The average number of years of information security experience across all participants was 6.3 years (range: 0.5-19, SD = 5.4). The average number of years spent in an investigative role was 3.9 years (range: 0.5-10, SD = 3.4) and the average number of total years spent in information technology was 11.2 (range: 0.5-28, SD = 7.4). Incident response was the most frequent self-reported job role (6 participants).

TABLE 1: Participant Characteristics (sorted by years of information security experience)

		Years of experience:			
Age range	**Gender**	**Infosec**	**Investigative**	**Total IT**	**Job Role**
45 to 54	Female	19	10	28	Incident Response
35 to 44	Male	13	2	15	Event/Alert/SOC Analyst
45 to 54	Female	12	10	12	Threat Intelligence
35 to 44	Male	11	4	14	Other (SIEM Developer)
35 to 44	Female	10	10	22	Incident Response
35 to 44	Male	8	7	18	Threat Hunting
25 to 34	Male	7	2.5	7	Security Generalist
25 to 34	Male	5	3	6	Threat Hunting
25 to 34	Female	4	4	4	Incident Response
25 to 34	Male	3.5	2	8	Incident Response
25 to 34	Male	2	2	16	Security Generalist
25 to 34	Male	2	2	2	Event/Alert/SOC Analyst
25 to 34	Male	2	2	11	Event/Alert/SOC Analyst
25 to 34	Male	1	1	10	Incident Response
35 to 44	Male	1	1	6	Other (Digital Forensics)
25 to 34	Male	0.5	0.5	0.5	Incident Response

DATA ANALYSIS

Qualitative

The principles of grounded theory data analysis guided qualitative data analysis for this study (Strauss & Corbin, 1998). After a thorough literature review to ensure no essential traits or behaviors associated with divergent or convergent thinking were overlooked, we created aggregated trait categories made up of the most commonly associated traits. Traits were grouped based upon conceptual similarity, resulting in 9 divergent codes and 7 convergent codes. Codes were also added for general convergent or divergent responses, as well as the quality of investigative responses for scenario-based questions. Appendix A shows the list of traits that primarily comprised our codebook. After all of the interviews had been coded, the most frequent traits and behavioral patterns were selected as the basis for our theoretical framework.

Quantitative

To offset analysts' lack of metacognitive awareness regarding their skill level (McIntosh et al., 2019, Sundaramurthy et al., 2014), the principal investigator ranked participants' skill level using the 3-point Expertise scale. It became clear early in the study that more nuance was needed. An additional 1-5 point Expertise scale was created, with 1 being Novice and 5 being Expert. The three Expertise scores were combined to create a Primary Skill score (PS). The PS score was used to stratify participants into three skill groups. The top third, designated the expert skill group, had five participants with a mean PS score of 9 (range: 8-10, SD = 0.70). The middle third, designated the intermediate skill group, had six participants with a mean PS score of 7 (range: 6-7, SD = 0.52). The bottom third, designated the beginner skill group, had five participants with a mean PS score of 4 (range 3-5, SD = 0.84).

The Analyst Skill Inventory (ASI) had a mean score of 82 out of 115 (range: 48-103, SD = 12.68) across the sample. The mean, range, and standard deviation were calculated for all three of the PS score-stratified skill groups.

The Metacognitive Awareness Inventory (MAI) had a mean score of 71 out of 95 (range: 59-86, SD = 8.63) across the sample. The mean score on the knowledge of cognition subscale was 32 (range: 26-38, SD = 4.03), and the mean score on the regulation of cognition subscale was 39 (range: 32-49, SD = 5.16). The mean, range, and standard deviation were calculated for all three of the PS score-stratified skill groups. Pearson correlations were run for the ASI and MSI score, by PS score skill group.

RESULTS

THE AMBIGUITY-DRIVEN CONVERGENCE MODEL

Participants' rich and thoughtful descriptions of their mental processes provide the basis for the Ambiguity-Driven Convergence (ADC) model. Our model provides a visual representation of this theory and illustrates when analysts are likely to use divergent and convergent thought (see Figure 1). In summary, the model shows that analysts are likely to rely on intuition first in an investigation. When their intuition leads them into a high stakes situation, the analysts' tendency toward lower ambiguity tolerance results in the use of convergent and divergent thought processes to advance the investigation.

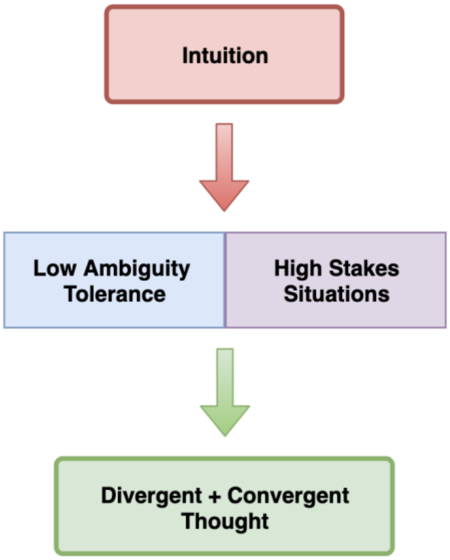

Figure 1: The Ambiguity-Driven Convergence Model

INTUITION IS RELIED ON, BUT OFTEN WRONG

The difference between convergent thought and intuition was highlighted when discussing investigative workflows and scenarios. Convergent thinking occurred when the analysts evaluated multiple ideas or questions and chose one starting point, usually by adapting known solutions and reasoning. When approaching scenarios, analysts commonly used intuition to pursue the first investigative path that came to mind:

> *"So I would say I usually start with the first thing that comes to mind and then table all the others."*

> *"Normally I will go with my gut. Which...I know that I shouldn't do. So I guess I spend enough time knowing that that's not what I should do."*

> *"I go with…the first thing that comes to mind. As I'm chasing that I'll make a list of other potentials. But it's so much just from your gut, what you think it might be. Even if I start with something else, I would be drawn back to whatever that first thought was. So I'd go with that."*

Intuition can play a role in divergent thought and the creation of potential investigation paths. In scenario-based interviews with analysts, we found that the quality of divergently-created lists started low, but increased as the analyst spent more time building the list. We saw evidence of this when examining the investigation path that the analysts chose to pursue in the convergent portion of the exercise.

Among high-quality convergent responses, only 10% were the first item in the analyst's divergently-created list, and most were found in the latter half. However, 95% of the high-quality convergent responses were present on the divergently-created lists. The analysts almost always came up with a good investigation path to pursue, but it wasn't until they listed several other ideas first. Most analysts recited the first few items in their investigation path lists immediately and without hesitation, while they were much slower and more thoughtful with responses comprising the middle and latter portions of their lists.

We suggest that the low quality of the early list items is because they were formed intuitively, and without adequate reasoning and evaluation. Exhausting the initial pool of intuitive ideas forces more deliberate thought, which leads to higher quality investigative paths.

Divergent thinking is correlated with creativity. Some analysts may need to exhaust their initial intuitive thoughts before they engage their creative problem solving skills and push toward more meaningful investigative paths. Stating or writing down intuitive thoughts provides the opportunity to evaluate them, develop connections between them, and build a foundation for additional reasoning. Although more deliberate reasoning may be a more desirable goal, the path there may be just as important as the destination.

LOWER AMBIGUITY TOLERANCE

Participants exhibited signs of lower ambiguity tolerance more frequently than any other trait we measured, with 79 significant statements exhibiting characteristics of this trait. Further examination of these statements groups them into two primary source categories that explain their utility.

First, lower ambiguity tolerance is a trait used automatically and out of functional necessity. When met with incomplete timelines and unanswered questions, analysts must be less tolerant of ambiguity or they are likely to skip important details, close a case prematurely, or make judgments based on incomplete information. Analysts' desire to avoid ambiguity motivates them to pursue additional investigative paths and relevant evidence. In this form, recognizing ambiguity propels the analyst to move the investigation forward.

Second, lower ambiguity tolerance is a trait used deliberately for completeness. Skilled analysts recognize the limitations of their tools and data. These potential weaknesses in their conclusions compel them to seek additional perspectives in the form of more evidence, third-party opinions, or previously unexplored hypotheses. In this form, recognizing ambiguity calls on the analyst to reflect and look back over the path they've taken and the conclusions they've made to ensure rigor or to consider their next move thoughtfully.

In both source categories, a lower tolerance for ambiguity appears as a consistently identified trait among analysts. The nature of investigative work would dictate that lower ambiguity tolerance is a desired trait in most situations. This goes a step further when you consider how analysts with low ambiguity tolerance handle high stakes situations.

HIGH STAKES SITUATIONS LEAD TO DIVERGENT AND CONVERGENT THOUGHT

Our research revealed three high stakes scenarios encountered by analysts which often preceded divergent and convergent thought. A high stakes scenario has the potential to cause anxiety and stress for the analyst or increases the potential to miss a crucial investigative finding. An analyst's tendency toward low ambiguity tolerance is likely to produce convergent and divergent thought when they encounter one of the following high stakes scenarios we identified.

Scenario 1: Unfamiliar or Vague Situations

An investigation scenario is unfamiliar when it contains evidence or inputs that the analyst hasn't encountered before. Similarly, an investigation scenario is vague when the provided context lacks enough useful information to propel the analyst forward toward meaningful findings that help build the attack timeline. In either scenario, analysts are more likely to make poor decisions resulting in a greater potential for missed network attacks.

In unfamiliar or vague situations, analysts must contend with more unknown variables than a typical scenario. While they are likely to select an initial investigation path to pursue based on intuition, the additional variables often require a more rigorous level of reasoning applied to the situation. In this case, analysts invoke creative problem solving, using divergent thought to ideate and convergent thought to choose a path forward:

> *"If it's really something completely new that's not very documented I would...try the first thing out...then try another one until I find something."*

> *"It changes a little bit when I encounter something I haven't seen before and I try what I've usually tried. And if what I try doesn't work then I have to step back and re-evaluate."*

> *"I would say go with the first thing in mind, start there. And then depending on what happens I build a list or other things to look for."*

These situations are more common for inexperienced analysts because their lack of evidentiary and heuristic knowledge dictates they will experience more unfamiliar situations and interpret more scenarios as vague.

Scenario 2: Investigative Roadblocks

All analysts will, at some time, experience the feeling of coming to a roadblock in an investigation. Often described as being "stuck" or "hitting a brick wall," this is a point in an investigation where progress halts and no additional findings are added to the attack timeline.

Analysts report recognizing that they're stuck through a few common occurrences:

- Spending too much time reviewing the same data source without new findings
- Repeating the same analytic actions without new findings
- The passage of a significant amount of time with no new findings
- Exhausting all possible evidence sources
- Exhausting all possible questions leading to investigative actions

When encountering investigative roadblocks, the analyst has already found interesting leads that they've deemed worthy of pursuit. If they are unable to get past the roadblock, those anomalies will remain unsolved and may result in the delayed discovery of an attack.

When conscious of the blocked investigative state, most analysts report physically separating themselves from the investigation. During this process, they usually generate ideas about different ways to approach the investigation, a hallmark of divergent thought. When they re-engage, they often report a new sense of clarity around the problem and converge on a single path forward:

> *"So I think like stepping away completely, washing my hands of it for a little bit, and then just explaining start to finish where I'm at...I'd say almost every time I kinda come up with something."*

> *"It's easy to get focused on one thing and get hung up on that. And then I'm always like let's take a step back. Or go for a walk and take your mind off it for a little bit...for me that works. Where I'll just go for a walk and think about other things. Either for that investigation or just outside. And things just pop up. Like oh, I didn't look at this, or I didn't try this, or whatnot."*

> *"And I've learned in the past from a lot of other jobs that when I start spinning my wheels, that's when I need to reset and kind of just step back and, and take a look at it. Either go to somebody else, ask for help, or take a break. You know, walk away from it 15, 20 minutes, take a lunch,*

> *something like that. Maybe I'm hungry. Things like that. Turn on some music, that sort of thing."*

Inexperienced analysts hit investigative roadblocks more frequently because they lack a large library of investigative heuristics or evidentiary knowledge that allow them to ask additional investigative questions or manipulate data in meaningful ways.

Scenario 3: Social Conditions

While not all analysts will work in investigations as part of a team, those who do report heightened concern about expressing their findings to other team members because the burden of proof is higher. Twelve of the sixteen participants reported that being part of a team changes their investigative approach.

Social conditions may occur during large coordinated investigations, peer review, managerial review, reporting, case management, tabletop exercises, or during general office chatter. Each of these situations exerts added pressure on the analyst to be more confident in their findings:

> *"I think that when you work in a team environment that there's a little bit more polish that goes into it. I think that...the overall reception of what you're producing is going to be...inspected by additional folks and that they need to be able to work off of it."*

> *"Being a junior I think you're always going to be a little bit nervous trying to present things to people knowing that they already have experience. You don't want to make yourself look like a fool or whatever."*

Because of additional pressure in social situations, analysts often revisit what they've concluded and ask additional questions. They ask, in one form or another, "How could I be wrong?" Divergent and convergent thought are at the center of this type of reconsideration:

> *"I don't present findings...unless I have run down every path that I can identify and think needs to be investigated. I don't give findings when there's still investigation to do."*

We acknowledge that the scenarios presented in our interviews for the present study constitute a social condition. Many analysts reported that they rely on intuition more than divergent and convergent thought; however, they still took a divergent/convergent path when presented with scenarios during the interviews. This was anticipated and fit within the construct of the research focus.

The prevalence of divergent and convergent thought in higher stakes scenarios underscores their importance as effective mechanisms for reaching accurate conclusions.

ANALYSTS POSSESS A LACK OF OVERALL METACOGNITIVE AWARENESS

Throughout the interviews, a lack of metacognitive awareness was prevalent among analyst participants. In every interview, analysts were unable to describe their investigative methods and processes clearly:

> *"It's hard to put into words."*

> *"It's interesting to think about. Usually this is a process with a lot of shortcuts where you don't necessarily have to systematically think through it...I'm used to the pathways enough that I don't question myself as much as I should."*

While most analysts were able to respond to specific investigative scenarios reasonably, they could not extrapolate on a structured or deliberate investigation process without referencing real-world scenarios. Analysts were able to apply heuristics they had previously developed to the scenarios indicating inductive reasoning had been at work to create "rules of thumb," while deductive reasoning was used to apply them to the current scenario. There were no signs that analysts recognized these processes were occurring. However, five analysts specifically mentioned the development of playbooks to standardize investigative processes, demonstrating a desire to regulate cognition even if they were unable to demonstrate knowledge of cognition at the time.

Within the context of specific scenarios, analysts were asked to assert their level of confidence in their answers for the first investigative path they would pursue. Those with high-quality responses assessed their confidence in their response as 3.8 (out of 5.0) on average. For analysts with low-quality responses, their average confidence assessment was also 3.8. They were equally confident they were making the right decision to move the investigation forward, even though they weren't.

Overconfidence in cognitive abilities is an example of the Dunning-Kruger effect; the poorest performers overestimate their ability, while top performers have more accurate self-assessments (McIntosh et al., 2019). Analysts with low metacognitive awareness are more likely to believe they are more capable than they are and that their decisions are more often correct than reality supports.

The Dunning-Kruger effect is also reflected in our participants' scores on the Metacognitive Awareness Inventory (MAI). The expert-level group had a mean MAI score of 71 (range: 64-79, SD = 8.04) and the correlation between MAI score and skill level was high ($r = 0.63$, $p < 0.01$). In short, higher self-reported skill level was related to significantly higher MAI scores in analysts observed to have a high level of investigative skill. The intermediate-level group had a mean MAI score of 68 (range: 59-74, SD = 5.72). The low-level skill group had a mean MAI score of 74 (range: 63-88, SD = 9.58), which is higher than the expert-level skill group. Analysts observed to have lower skill levels believed their metacognitive awareness to be, on average, higher than the expert-level group.

DISCUSSION AND PRACTICAL IMPLICATION

Based upon our observations, much of analysts' day-to-day work appears to be intuition-based. This is disconcerting because intuition-based decisions are often low quality. Even for experienced analysts, "going with your gut" can be a recipe for wasted time and missed leads. If we can't rely on intuition, should we seek to remove it from the investigation process altogether? Absolutely not; analysts need to make quick decisions to rapidly pivot through evidence. However, we can decrease the absolute reliance on intuition while also increasing its utility by applying practical lessons from the present research based on observing divergent and convergent thought.

Analysts of all skill levels unconsciously resort to divergent and convergent thought when the stakes are high, but these ways of thinking have potential uses elsewhere in the investigative process. Divergent and convergent thought are powerful tools in the analysts' arsenal if they can learn to leverage them deliberately. Doing so provides an opportunity to raise metacognitive awareness by increasing recognition of cognitive processes and providing a mechanism for regulating cognition more efficiently.

One potentially effective strategy is to employ divergent and convergent thought exercises in the training and daily practice of analysts. This has been tried in other fields, such as accounting, where auditors received training in divergent and convergent thinking. When given a set of data that included anomalies, the trained auditors had a greater likelihood of coming up with and choosing the correct explanation for the situation based on the evidence they were given (Plumlee et al., 2015). A similar type of organized training or skill practice could be used by security analysts. Rather than intuitively jumping into every situation and pursuing the first investigative lead that comes to mind, the analyst intentionally pauses and creates a list of investigative questions to ask or evidence sources to pursue. Once they've brainstormed for a short while, they evaluate their list and choose the best investigative path to pursue. After the investigation is complete, they can evaluate the quality of their list and subsequent decisions, perhaps as part of a group. Each iteration of this process serves to increase the analyst's heuristic skills and metacognitive awareness. Eventually, the analyst should be able to trust their intuition more because of the accumulation of experience gained through repetition and reflection.

Divergent and convergent thought exercises have great potential to benefit playbook development. As an example of how this may work within a given SOC, analysts can identify common investigative scenarios and create categories of investigations. From there, they would gather a series of examples (hypothetical or based on real cases) within each category. The analysts complete the same divergent and convergent exercises previously mentioned, then they collectively evaluate the utility of each investigative step and rank them accordingly. This ordinal list provides a basis for their playbook. A series of these playbooks reduces the reliance on intuition and offers high-quality, peer-reviewed investigation paths analysts can pursue based on the nature of the investigation scenario at hand. While prescriptive, these playbooks should not be so strict that they prevent analysts from manipulating and evaluating additional ideas outside the scope of the playbooks when warranted by the evidence.

These applied divergent and convergent problem-solving techniques can provide value for analysts during their daily workflow, while also providing a foundation for analyst education in post-secondary or professional learning environments. Without intentional development and improved metacognitive awareness, intuition can lead analysts astray. The conscious and deliberate use of divergent and convergent thinking provides a mechanism for strengthening the quality of intuitive decisions while also reducing reliance on them.

STUDY LIMITATIONS

There are three primary limitations to this study: the chosen methodology, the sample, and a lack of participant metacognitive awareness.

Grounded theory studies are based on verbal data collected through interviews between researchers and participants. It is possible that different researchers and participants could yield different findings even though measures were put in place to ensure reliability and rigor.

We sought to collect perspectives from many levels of expertise so that our sample would reflect the broader security analyst population and provide an opportunity to study the differences between novices and experts. While we were able to identify some differences, the ranking of analysts was primarily based on self-reported data combined with researcher evaluation during qualitative interviews. A more rigorous analyst skill evaluation mechanism would better define the stratification between analyst skill levels and ensure a more representative sample.

Finally, the evidence that analysts lack metacognitive awareness could limit the validity of their responses during the self-assessment and qualitative interviews.

FUTURE WORK

The nature of our research was primarily qualitative for the explicit purpose of exploring human experience and gaining a better understanding of underlying cognitive processes. While we created a theory surrounding divergent and convergent thought, further validation of the Ambiguity-Driven Convergence model using experimental or quantitative measures could further confirm our observations.

In addition, we made several direct observations about deficiencies in metacognitive awareness among analysts. Additional qualitative research could further clarify this issue, while experimental research could be leveraged to identify interventions that increase metacognitive awareness.

CONCLUSION

The successful defense of information systems revolves around the human analyst's ability to perform investigations. Even though facets of information security are becoming increasingly automated, the human remains at the center of the process for the foreseeable future. It's critically important that the industry seeks to understand and enhance the discipline of network security analysis.

We studied how analysts use divergent and convergent thinking to solve problems creatively during the investigation process. We propose the ambiguity-driven convergence model as a framework to help explain these processes. By understanding this theory and improving it with further research, analysts and educators can improve knowledge of cognition and advance the field with increased metacognitive awareness and more effective investigations.

REFERENCES

Brophy, D. R. (2001). Comparing the Attributes, Activities, and Performance of Divergent, Convergent, and Combination Thinkers. *Creativity Research Journal*, 13(3/4), 439–455.

Chamorro-Premuzic, T., & Reichenbacher, L. (2008). Effects of Personality and Threat of Evaluation on Divergent and Convergent Thinking. *Journal of Research in Personality*, 42(4), 1095–1101.

Cropley, A. (2006). In Praise of Convergent Thinking. *Creativity Research Journal*, 18(3), 391–404.

Farley, F. (1986, May). The Big T in Personality. *Psychology Today*, 44–52.

Feldman, D. H. (1988). Creativity: Dreams, insights, and transformations. In R. J. Sternberg (Ed.), *The nature of creativity* (pp. 271–297). Cambridge, England: Cambridge University Press.

Flavell, J. H. (1979). Metacognition and Cognitive Monitoring: A New Area of Cognitive-Developmental Inquiry. *American Psychologist*, *34*(10), 906–911.

Gough, H. G. (1979). A creative personality scale for the Adjective Check List. *Journal of Personality and Social Psychology*, 37, 1398-1405.

Guilford, J. P. (1950). Creativity. *American Psychologist*, *5*(9), 444–454.

Hargrove, R. A., & Nietfeld, J. L. (2015). The Impact of Metacognitive Instruction on Creative Problem Solving. *Journal of Experimental Education*, *83*(3), 291–318.

Harrison, G. M., & Vallin, L. M. (2018). Evaluating the metacognitive awareness inventory using empirical factor-structure evidence. *Metacognition and Learning*, *13*(1), 15–38.

Isaksen, S. G., Puccio, G. J., & Treffinger, D. J. (1993). An ecological approach to creativity research: Profiling for creative problem solving. *Journal of Creative Behavior*, 27, 149–170.

Kirton, M. (1987). Adaptors and innovators: Cognitive style and personality. In S.G.Isaksen (Ed.), *Frontiers of creativity research: Beyond the basics* (pp. 282–304). Buffalo, NY: Bearly Limited.

Martinsen, O. (1995). Cognitive styles and experience in solving insight problems: Replication and extension. *Creativity Research Journal*, 8, 291–298.

Martinsen, O. L., Arnulf, J. K., Furnham, A., & Lang-Ree, O. C. (2019). Narcissism and creativity. *Personality and Individual Differences*, 142, 166–171.

Mednick, S. A. (1962). The associative basis of the creative process. *Psychological Review*, 69, 220–232.

McCrae, R. R. (1987). Creativity, divergent thinking, and openness to experience. *Journal of Personality and Social Psychology*, 52(6), 1258–1265.

McIntosh, R. D., Fowler, E. A., Lyu, T., & Della Sala, S. (2019). Wise up: Clarifying the role of metacognition in the Dunning-Kruger effect. *Journal of Experimental Psychology: General*.

Mumford, M. D., Costanza, D. P., Threlfall, K. V., Baughman, W. A., & Reiter-Palmon, R. (1993). Personality variables and problem-construction activities: An exploratory investigation. *Creativity Research Journal*, 8, 365–389.

Myszkowski, N., Storme, M., Davila, A., & Lubart, T. (2015). Managerial creative problem solving and the Big Five personality traits: Distinguishing divergent and convergent abilities. *The Journal of Management Development*, 34(6), 674–684.

Patton, M. (1990). Qualitative evaluation and research methods (2nd ed.). Newbury Park, CA: Sage.

Plumlee, R. D., Rixom, B. A., & Rosman, A. J. (2015). Training Auditors to Perform Analytical Procedures Using Metacognitive Skills. *Accounting Review*, *90*(1), 351–369.

Puccio, G. J., Treffinger, D. J., & Talbot, R. J. (1995). Exploratory examination of relationships between creativity styles and creative products. *Creativity Research Journa*l, 8, 157–172.

Strauss, A., & Corbin, J. (1998). Basics of qualitative research: Techniques and procedures for developing grounded theory. Thousand Oaks, CA: Sage.

Sundaramurthy, S. C., McHugh, J., Ou, X. S., Rajagopalan, S. R., & Wesch, M. (2014). An Anthropological Approach to Studying CSIRTs. *IEEE Security & Privacy*, *12*(5), 52–60.

Tan, A.-G. (2015). Convergent Creativity: From Arthur Cropley (1935-) Onwards. *Creativity Research Journal*, *27*(3), 271–280.

Tardif, T. Z., & Sternberg, R. J. (1988). What do we know about creativity? In R. J. Sternberg (Ed.), *The nature of creativity* (pp. 429–440). Cambridge, England: Cambridge University Press.

AUTHOR BIOGRAPHIES

Chris Sanders is the founder of Applied Network Defense, an information security training company. He is also the Director of the Rural Technology Fund, a non-profit organization that donates scholarships and technology education equipment to public schools to further computer science education in rural and high poverty areas. He is the author of Applied Network Security Monitoring and Practical Packet Analysis.

Chris is an EdD candidate at Baylor University. He holds the GSE, GCIA, GCIH, GREM, GPEN, GSEC, CISSP, and Security+ designations. His current research focus is on the intersection of cyber security, cognitive psychology, and education to enhance the field of information security investigative disciplines through a better understanding of the human thought and learning processes.

Chris blogs at https://chrissanders.org and is on Twitter @chrissanders88.

Stef Rand is a research intern at Applied Network Defense and will complete her Bachelor of Science in Information Technology with a concentration in cyber security from Augusta University in December of 2019. Stef earned a Master of Science in Clinical Psychology at Augusta State University in 2012. Her research focus was on undergraduate student attrition and retention. Her clinical focus was on mild traumatic brain injury diagnosis, management, and treatment in veterans.

Stef is a board member for the STEM Club of America and a volunteer mentor for The Girls Engineering and Coding Organization.

You can learn more about Stef at www.stefrand.com or on Twitter @techieStef

APPENDIX A: QUALITATIVE DIVERGENT AND CONVERGENT TRAITS

Table 2: Divergent Traits

Trait Category	Description
Manipulate Ideas	ideation; combine ideas; generate diverse ideas; reorganize/rearrange ideas; reinterpretation of ideas & concepts (Brophy, 2011; Kirton 1987; Martinsen, 1995; Mumford et al 1993)
Innovative	original; create new solutions; identify new problems; imaginative; question norms; intellectually curious; inventive; resourceful; unconventional; comfortable with higher level of risk (Brophy, 2001; Chamorro-Premuzic & Reichenbacher, 2008; Gough, 1979; Isaksen et al 1993; McCrae,1987; Puccio et al, 1995)
Higher Ambiguity Tolerance	comfortable with unclear meanings; comfortable having little past experience with a problem; resist premature closure (Brophy, 2001; Farley, 1986; Kirton, 1987; Martinsen, 1995)
Intuition	intuitive; arrange ideas in parallel patterns; reflective; insightful (Brophy, 2001; Gough, 1979)
Greater Field Independence	associates more meanings with specific information; organize information from separate categories/sources in multiple ways; capable of shifting contexts; flexible (Brophy, 2001; Cropley, 2006)
Assertive	justify ideas; need for control; confident/overconfident (Brophy, 2001; Chamorro-Premuzic & Reichenbacher, 2008; Gough, 1979)
Less Agreeable	lower levels of cooperation; high need for control; snobbish (Gough, 1979; Myszkowski et al, 2015; Martinsen et al, 2019)
Extraverted	sociable; positive/optimistic outlook; energetic/active; humorous; informal; expressive (Chamorro-Premuzic & Reichenbacher, 2008; Gough, 1979)

Manipulate Ideas	ideation; combine ideas; generate diverse ideas; reorganize/rearrange ideas; reinterpretation of ideas & concepts (Brophy, 2011; Kirton 1987; Martinsen, 1995; Mumford et al 1993)
Innovative	original; create new solutions; identify new problems; imaginative; question norms; intellectually curious; inventive; resourceful; unconventional; comfortable with higher level of risk (Brophy, 2001; Chamorro-Premuzic & Reichenbacher, 2008; Gough, 1979; Isaksen et al 1993; McCrae,1987; Puccio et al, 1995)
Higher Ambiguity Tolerance	comfortable with unclear meanings; comfortable having little past experience with a problem; resist premature closure (Brophy, 2001; Farley, 1986; Kirton, 1987; Martinsen, 1995)
Intuition	intuitive; arrange ideas in parallel patterns; reflective; insightful(Brophy, 2001; Gough, 1979)
Greater Field Independence	associates more meanings with specific information; organize information from separate categories/sources in multiple ways; capable of shifting contexts; flexible (Brophy, 2001; Cropley, 2006)
Assertive	justify ideas; need for control; confident/overconfident (Brophy, 2001; Chamorro-Premuzic & Reichenbacher, 2008; Gough, 1979)
Less Agreeable	lower levels of cooperation; high need for control; snobbish (Gough, 1979; Myszkowski et al, 2015; Martinsen et al, 2019)
Extraverted	sociable; positive/optimistic outlook; energetic/active; humorous; informal; expressive (Chamorro-Premuzic & Reichenbacher, 2008; Gough, 1979)

Table 3: Convergent Traits

Trait Category	Description
Adaptive	adapt; reapply the known; improve existing paradigms, problems, and solutions; accept paradigms but use in new ways; avoid risk; stick to rules (Brophy, 2001; Cropley, 2006; Feldman, 1988; Kirton, 1987; Tardif & Sternberg, 1988)
Evaluate Ideas	evaluate; recognize familiar things quickly; recognize both possible and workable solutions; seek simplicity; gather facts; remember accurately (Cropley, 2006)
Reasoning	judge ideas according to logic, fact, or value standards; arrange ideas in a linear fashion; aware of weaknesses; see limits; observant; fast information processing; assess idea feasibility (Brophy, 2001; Cropley, 2006)
Lower Ambiguity Tolerance	uncomfortable with unclear meanings; seek closure even if premature; prefer certainty; prefer narrow job tasks (Brophy, 2001; Gough, 1979; Isaksen et al 1993; Puccio et al, 1995)
Lower Field Independence	challenged by shifting contexts; less flexible (Brophy, 2001)
Agreeable	agreeable; cooperative; preference for group work and consensus (Feldman, 1988; Kirton, 1987; Myszkowski et al, 2015; Tardif & Sternberg, 1988)
Adaptive	adapt; reapply the known; improve existing paradigms, problems, and solutions; accept paradigms but use in new ways; avoid risk; stick to rules (Brophy, 2001; Cropley, 2006; Feldman, 1988; Kirton, 1987; Tardif & Sternberg, 1988)
Evaluate Ideas	evaluate; recognize familiar things quickly; recognize both possible and workable solutions; seek simplicity; gather facts; remember accurately (Cropley, 2006)

Reasoning	judge ideas according to logic, fact, or value standards; arrange ideas in a linear fashion; aware of weaknesses; see limits; observant; fast information processing; assess idea feasibility (Brophy, 2001; Cropley, 2006)
Lower Ambiguity Tolerance	uncomfortable with unclear meanings; seek closure even if premature; prefer certainty; prefer narrow job tasks (Brophy, 2001; Gough, 1979; Isaksen et al 1993; Puccio et al, 1995)
Lower Field Independence	challenged by shifting contexts; less flexible (Brophy, 2001)
Agreeable	agreeable; cooperative; preference for group work and consensus (Feldman, 1988; Kirton, 1987; Myszkowski et al, 2015; Tardif & Sternberg, 1988)
Adaptive	adapt; reapply the known; improve existing paradigms, problems, and solutions; accept paradigms but use in new ways; avoid risk; stick to rules (Brophy, 2001; Cropley, 2006; Feldman, 1988; Kirton, 1987; Tardif & Sternberg, 1988)
Evaluate Ideas	evaluate; recognize familiar things quickly; recognize both possible and workable solutions; seek simplicity; gather facts; remember accurately (Cropley, 2006)
Reasoning	judge ideas according to logic, fact, or value standards; arrange ideas in a linear fashion; aware of weaknesses; see limits; observant; fast information processing; assess idea feasibility (Brophy, 2001; Cropley, 2006)
Lower Ambiguity Tolerance	uncomfortable with unclear meanings; seek closure even if premature; prefer certainty; prefer narrow job tasks (Brophy, 2001; Gough, 1979; Isaksen et al 1993; Puccio et al, 1995)