ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Technical Research Center

Neurological & Psychological Mechanisms in Cybersecurity Engineers' Critical Thinking

Research Paper: ISAU-WP-904-2025-NPM

ISAU-TG51-2025
4-7-2025

An ISAUnited.org Published Whitepaper

Institute of Security Architecture United (ISAUnited.org)

Author or Task Group Number:

ISAU-TG51-2025

Publishing Reviewer(s):

ISAUnited Master Fellow Committee

Affiliation: ISAUnited.org

Date:

April 7, 2025

Document Registration Number:

ISAU-WP-904-2025-NPM

Assigned by the Institute Document Management Register

Neurological and Psychological Mechanisms in Cybersecurity Engineers' Critical Thinking

Abstract

Cybersecurity engineers routinely navigate complex, high-stakes situations, demanding exceptional critical and analytical thinking skills. This technical research paper explores the neurological and psychological foundations of these critical thinking abilities, specifically highlighting the roles of prefrontal cortical networks and executive cognitive functions such as working memory, attention control, and cognitive flexibility. Additionally, it examines psychological traits prevalent among cybersecurity professionals, including analytical cognitive styles, skepticism, and stress response patterns. The research provides evidence-based insights demonstrating how stress and emotional regulation significantly impact cognitive performance, emphasizing the connection between mental health and effective critical thinking. Practical recommendations are offered for cybersecurity organizations to enhance engineers' performance, resilience, and cognitive health through targeted training, collaborative strategies, and organizational support systems. Understanding these brain-behavior relationships equips technical leaders and educators with actionable strategies to bolster cybersecurity defenses by optimizing their teams' cognitive and psychological capacities.

Key words: Cybersecurity engineering, critical thinking, prefrontal cortex, decision-making, cognitive neuroscience, executive function, stress and cognition, emotion-cognition interaction, neuropsychology, analytical reasoning

Engineering the Thinking Mind

Cybersecurity engineers operate on the front lines of digital defense, confronting complex threats that demand sharp analytical and critical thinking. These professionals sift through extensive data, identify subtle patterns of malicious activity, and make quick decisions to neutralize risks. In practice, a cybersecurity analyst might investigate network logs to find anomalies or correlations that reveal a cyberattack, then deduce the attack's source and optimal response. Such tasks require technical knowledge and advanced cognitive skills in reasoning and problem-solving. Indeed, successful defense against cyber-attacks "depends on human decision making," even with many automated tools in place [1]. Cybersecurity professionals are continually interpreting ambiguous information and must draw sound conclusions under pressure. This raises the question:

What neurological and psychological mechanisms enable their high-level analytical and critical thinking?

Recent research in cognitive neuroscience provides insight into how the brains of skilled problem-solvers function during analytical tasks. Similarly, cognitive psychology and human factors studies shed light on the mental processes and traits that support (or sometimes hinder) practical critical thinking. By focusing on cybersecurity engineers—a group that exemplifies analytical reasoning in practice—we can bridge findings from neuroscience and psychology to real-world technical problem-solving. Such an interdisciplinary understanding is not just academic; it has practical implications for those who manage and support cybersecurity teams. Technical research centers (such as ISAUnited) and training departments can leverage this knowledge to design training programs, improve team collaboration dynamics, and implement support systems aligned with engineers' cognitive needs. This paper aims to educate technical staff about how cybersecurity professionals think, at both brain and mind levels, and how this understanding can translate into concrete strategies to support and enhance that thinking. We review key brain regions and networks involved in analytical reasoning, discuss cognitive functions and psychological traits relevant to cybersecurity critical thinking, and explore how these insights can inform training and support initiatives.

Neurocognitive Basis of Analytical and Critical Thinking

Critical thinking and analytical reasoning are complex cognitive functions that engage multiple brain regions. Foremost among these is the prefrontal cortex (PFC), the brain's executive center. The PFC—particularly the frontal lobe regions—is pivotal in organizing thought, planning, and regulating other brain areas during problem-solving [1]. Evidence strongly links critical thinking abilities with the functionality of prefrontal executive networks. For example, executive functions and critical thinking performance are

associated with activity in the prefrontal cortex. This makes sense given that executive functions (such as holding information in mind, flexibly shifting attention, and inhibiting impulsive responses) are the mental tools required for reasoned, deliberate thinking. Analytical problem-solving is typically an intentional, conscious process that relies on these executive resources instead of the rapid, automatic intuitions of “fast” thinking. Neuroimaging and lesion studies help pinpoint which parts of the prefrontal cortex are most crucial for analytic reasoning. A recent lesion mapping study identified the right frontal lobe as a critical hub for reasoning and novel problem-solving ability [2]. Patients with damage to the right frontal cortex showed significantly impaired logical reasoning performance, making ~15% more errors on reasoning tests than others. This underscores that a “right frontal network” is essential for complex reasoning tasks [2]. This right-frontopolar involvement has also been linked to fluid intelligence (the capacity to solve new problems) [2], suggesting that cybersecurity engineers’ ability to tackle unfamiliar threats draws on the exact frontal-lobe mechanisms that support general problem-solving aptitude.

Analytical thinking is not localized to the prefrontal cortex alone; it emerges from interactions of frontal regions with other parts of the brain. The frontal lobes work with the parietal and subcortical structures to support critical thinking. For instance, when a person engages in deductive reasoning (deriving logical conclusions from given premises), brain imaging shows activation in a network including the anterior cingulate cortex (ACC) — involved in conflict monitoring and error detection — along with the inferior frontal gyrus and parietal regions. These areas collectively underpin the ability to hold abstract rules in mind and manipulate information, which is essential for logically working through cybersecurity problems (such as tracing an intrusion step-by-step). In contrast, reasoning that relies on recalling prior knowledge (e.g., recognizing a known malware pattern) engages memory-related regions like the hippocampus [8]. This difference indicates that analytical reasoning in novel situations leans heavily on executive and working memory networks (frontal and parietal). In contrast, familiar problem patterns can be solved by retrieving stored knowledge. Expert cybersecurity analysts likely invoke both systems: they recognize known attack signatures from memory, but when confronted with new scenarios, they shift into a more effortful analytical mode orchestrated by the PFC.

Beyond the cortex, several deeper brain structures support analytical thinking. While traditionally associated with sensory relay and motor control, the thalamus and basal ganglia contribute to cognition and critical thinking [3]. The basal ganglia, for example, help integrate information and learning from feedback (reward-related learning), which can aid in recognizing patterns or habitual sequences — helpful in spotting anomalies or repetitive attack tactics [3]. The thalamus, situated at the brain’s center, acts as a hub routing information, sustaining attention, and coordinating complex

information processing [3]. Keeping focused attention is crucial when an engineer must drill down into an incident without being distracted by irrelevant data. Meanwhile, the ACC (part of the medial frontal cortex) and related circuits monitor for conflicts or errors, alerting the person when something "doesn't add up," such as a piece of network behavior that defies expectations. Overall, practical analytical thinking emerges from a well-tuned network: the prefrontal cortex provides top-down control and working memory; the parietal cortex contributes to storing and manipulating intermediate data (a mental workspace); subcortical structures like the basal ganglia and thalamus facilitate information integration and attention; and the ACC helps maintain logical consistency and error-checking. This distributed neural network enables cybersecurity professionals to methodically work through complex problems, whether diagnosing a security incident or performing a risk analysis.

Notably, the brain's emotional centers interface with this cognitive network, highlighting the interplay between emotion and critical thinking. While we often imagine analytical thinking as purely rational, neuroscience shows that emotion can modulate cognitive processing. The amygdala and limbic system (which process emotions like fear or stress) connect to the prefrontal cortex and can influence decision-making. Moderate levels of negative emotion or skepticism may boost critical analysis, making a person more vigilant and detail-oriented. In contrast, an overly optimistic mood might lead to complacency or reliance on mental shortcuts [3]. Studies suggest that people in a mildly negative mood tend to engage in more systematic, effortful information processing. In contrast, happy individuals are more prone to use heuristic or biased thinking [3]. In cybersecurity, a healthy dose of wariness (for example, not taking things at face value and being alert to anomalies) can be beneficial, as it triggers a more critical evaluation of information. On the other hand, excessive stress or fear can be detrimental: high stress levels impair prefrontal cortex function and executive abilities [4]. Chronic stress, such as the pressure of handling continuous cyber incidents without relief, can degrade working memory, attention, and cognitive flexibility [6], all needed for agile thinking. Thus, there is a balance to strike — some emotional arousal (like urgency or skepticism) may sharpen critical thinking, but too much stress can overwhelm the brain's executive capacity. Cybersecurity engineers often work in high-pressure situations (e.g., during an active breach), so managing stress is essential to maintain optimal cognitive function. When needed, techniques to regulate stress responses (deep breathing, tactical pauses, or mindfulness practices) could help preserve the prefrontal executive networks' integrity.

In summary, neuroscience reveals that a coalition of brain regions, with the prefrontal cortex at the helm, supports analytical and critical thinking. This "analytical brain network" enables cybersecurity engineers to work through unfamiliar problems logically, hold multiple pieces of information in mind, and remain vigilant to

inconsistencies. It also underscores why individuals vary in analytic ability: factors like frontal lobe integrity, working memory capacity, and mood can influence critical thinking performance. These neurocognitive insights set the stage for understanding the minds of cybersecurity professionals and point to ways we might enhance their cognitive performance through training and supportive interventions.

Cognitive Processes and Psychological Traits in Cybersecurity Professionals

High-level analytical thinking in cybersecurity engineers has a neural basis corresponding to measurable cognitive skills and psychological characteristics. One key set of mental skills is the executive functions, which include working memory (the ability to hold and update information), inhibitory control (the ability to suppress irrelevant impulses or distractions), and cognitive flexibility (the ability to switch between tasks or mental sets). Research indicates these executive functions strongly predict critical thinking performance [8]. In an extensive study of young adults, individuals with better working memory updating and inhibitory control scored higher on essential thinking tasks, even after controlling for general intelligence [8]. This suggests that, regardless of raw IQ or knowledge, the efficiency of one's executive processes can make the difference in how well they reason through complex problems. In practical terms, a cybersecurity analyst with a robust working memory can juggle multiple pieces of an investigation (IP addresses, timelines, hypotheses) without losing track, and strong inhibitory control helps them ignore misleading cues or snap judgments (for example, not jumping to conclude an alert is a false positive before deeper analysis). Another study using neural measures found that high-level critical thinkers showed different brain response patterns than low-level critical thinkers, consistent with more efficient processing. Specifically, brainwave (ERP) data indicated that those who performed better on critical thinking had smaller P3 amplitudes (an indicator of attentional resource allocation) than poorer performers [9]. This was interpreted as evidence that proficient critical thinkers rely on fast, automatic updating and inhibition processes (requiring less overt effort). In contrast, less proficient thinkers expend more effort (higher P3) to achieve the same ends [8]. With practice and skill, specific analytical processes become more automatic; experts can swiftly recognize what is relevant, update their mental model, and filter out noise, solving problems more efficiently.

Besides these cognitive capacities, thinking style and cognitive approach play a role. Some people are naturally more analytical, preferring methodical, step-by-step problem solving, whereas others rely on insight or intuition. Cybersecurity work tends to attract and reward those with a strong analytical bent. Neuroscience studies on problem-solving styles show that self-identified "analytical thinkers" exhibit distinct brain activity patterns, such as higher frontal lobe engagement during task-solving, compared

to more “intuitive” thinkers [1]. As noted earlier, analytical thinkers engage frontal executive circuits to work through puzzles, aligning with cybersecurity analysis demands methodically. They may also possess a high need for cognition – a psychological trait describing one’s inclination to engage in and enjoy effortful cognitive activities. A cybersecurity engineer must often concentrate intensely and think deeply about abstract problems; enjoying this mental challenge is almost a prerequisite. Another relevant concept is metacognition – thinking about one’s thinking. Skilled analysts are often very reflective about their reasoning process: they may pause to question their assumptions, double-check inferences, and consider alternative explanations (e.g., could this network anomaly be an internal error rather than an attack?). Such metacognitive habits correlate with better critical thinking, as they guard against overconfidence and cognitive biases. In cybersecurity, where deceptive tactics and false leads are common, the best professionals maintain a healthy skepticism and continuously evaluate whether their current theory fits the evidence.

Personality and dispositional traits have also been studied in relation to cybersecurity professionals’ mindsets. Intriguingly, recent research suggests that those drawn to security roles differ in personality profile from other IT professionals. A master’s thesis comparing personality traits found that cybersecurity specialists scored significantly higher on Openness to Experience (particularly the “Intellect” facet, reflecting curiosity and love of ideas) and markedly lower on Agreeableness than their peers in other IT fields. Higher Openness is consistent with the curiosity and inventiveness needed for cybersecurity work—engineers must be willing to explore new technologies, question assumptions, and think outside the box to anticipate attackers. Lower Agreeableness (especially lower trust and higher skepticism) also makes sense in a security context: being naturally skeptical can be advantageous when one’s job is to find hidden threats and not take information at face value. These professionals may have a more questioning, even cynical mindset, which helps scrutinize systems for weaknesses. They might also be quite independent and assertive (traits noted in the same study), which can aid in pressing forward with investigations or challenging the status quo when security is at stake. However, these traits can be double-edged swords; for example, low agreeableness might challenge team coordination or communication if not recognized and managed. Technical research center staff should know that the cybersecurity workforce could be cognitively and personality-wise “wired” differently from other groups. This suggests tailoring management and support accordingly (e.g., fostering an environment that respects independent thinking and skepticism while also training on teamwork and communication skills).

Another psychological factor to consider is the presence of cognitive biases in decision-making. No matter how analytic a person is, human cognition is prone to systematic biases, and cybersecurity professionals are not immune. Studies have

shown that experienced security decision-makers can fall prey to the same biases as everyone else, sometimes exacerbated by their confidence in expertise [10]. For instance, overconfidence bias has been observed among security professionals, who express high confidence in risk estimates even with limited information [10]. This can be dangerous if it leads an analyst to dismiss the possibility of an unusual attack because it hasn't been seen before, or to underestimate the likelihood of a breach due to unwarranted confidence in their defenses. Confirmation bias is another concern: an analyst might fixate on an initial hypothesis (say, that a specific malware is to blame) and interpret evidence selectively to support that belief, overlooking signs that point to a different reality. In fast-paced security operations, there is a tendency to rely on "System 1" thinking (rapid, experience-based judgments) for efficiency, but this needs to be checked by "System 2" thinking (slow, logical analysis) to avoid mistakes [10]. The best cybersecurity thinkers strike a balance — they use intuition built from experience to recognize patterns quickly. Yet, they are ready to slow down and reason carefully when faced with novel or high-impact situations. Bringing multiple perspectives is also a known debiasing technique; diverse teams can counteract individual biases by hashing out different views [10]. This is one reason why collaborative analysis (e.g., peer review of an incident report) is encouraged in security operations: it forces analysts to justify their reasoning and consider alternatives, thereby reducing bias and error.

In summary, cybersecurity engineers' minds are characterized by strong executive cognitive capacities, an analytical thinking style bolstered by traits like curiosity and skepticism, and a continuous battle to manage biases and emotions. Their working memory and attention control enable them to sift complex technical information; their traits drive them to question and learn relentlessly; and their awareness of cognitive pitfalls helps them maintain objectivity. Recognizing this profile allows us to appreciate why specific individuals thrive in cybersecurity roles and points to areas where even experts need support (for example, coping with stress or mitigating overconfidence). The following section translates these insights into practical training, collaboration, and support recommendations to align organizational practices with how cybersecurity professionals think and function best.

Implications for Training, Collaboration, and Support

Understanding cybersecurity engineers' neurocognitive and psychological makeup provides valuable guidance on how to support them. Technical research centers and employers can use these insights to design training programs, teamwork structures, and support systems that enhance strengths and address analytical and critical thinking weaknesses.

1. Cognitive Training and Skill Development: Given that executive functions like working memory and inhibition underlie critical thinking success, training programs can incorporate exercises to strengthen these abilities. This might include complex problem-solving drills, memory games, and “red team/blue team” simulations that challenge analysts to juggle multiple information streams and resist quick assumptions. For example, scenario-based exercises where trainees must investigate a mock cyber incident can help develop their ability to update hypotheses as new evidence comes in and inhibit the impulse to rush to judgment. Such exercises should be designed to progressively increase complexity, expanding the individual’s mental “RAM” (working memory capacity) over time. Additionally, encouraging metacognitive practices can be beneficial: training analysts to pause and reflect on their reasoning, question their assumptions, and consider alternative outcomes. This can be done through after-action reviews of exercises, where participants discuss not just what they concluded, but *how* they arrived at their conclusions and whether they missed any cues due to bias or oversight. Research has shown that critical thinking skills can indeed be improved through targeted training interventions, even leading to measurable changes in brain function. For instance, mindfulness meditation training has enhanced critical thinking and increased functional connectivity in prefrontal brain networks. Incorporating short mindfulness or focus training sessions into the work routine might help engineers sharpen their attention and emotional regulation, keeping their brains primed for analytic work. Over the long term, an organizational commitment to cognitive skills training and continuous learning will improve individual performance and nurture a culture of thoughtful, evidence-based decision-making in the cybersecurity team.

2. Collaboration and Team Strategies: The psychological profile of cybersecurity professionals (analytical, high curiosity, lower agreeableness, etc.) suggests that traditional team-building approaches may need adjustment. Team collaboration should be structured to leverage their strengths, such as independent thinking and skepticism, while mitigating potential friction or blind spots. One strategy is to implement peer review and collaborative analysis as standard practice. The organization ensures that multiple viewpoints are considered by having analysts routinely double-check each other’s findings or work in pairs on complex incidents. This aligns with the recommendation to “bring in different points of view to make more informed, rational decisions” in security contexts [10]. A colleague might spot an oversight or challenge a biased assumption that the primary investigator missed. Such processes capitalize on personal biases, but a well-functioning team can collectively be more objective.

Another approach is cognitive diversity within teams. Individuals vary in cognitive styles; some are highly analytical, others may be more intuitive or creative. You can cover more bases by composing teams with a mix of these styles. For example, an intuitive thinker might generate a novel hypothesis for an attacker's motive that a purely analytical thinker did not consider. In contrast, the analytical thinker can systematically validate that hypothesis. Technical leaders should cultivate an environment where debate and questioning are welcome (fitting the skeptically minded culture of security folks) and where there is respect and psychological safety so that lower agreeableness traits (like bluntness or impatience) do not devolve into conflict. Clear communication protocols and role definitions during incident response can help; if each team member knows their specific focus (one person digging into network logs, another examining malware behavior, etc.), they can work semi-autonomously (appealing to their independence) while contributing to a collective picture. Regular team debriefs allow the independent threads to be woven together, and each expert can present their findings for group scrutiny. In essence, the goal is to harness the power of many analytical minds without the process becoming disjointed – structure and shared goals are key.

Furthermore, leadership should know the potential for overconfidence in seasoned experts and encourage humility and continuous learning. One way to do this is to rotate roles occasionally or have team members present analyses to external experts for feedback. This practice keeps even veteran analysts on their toes and reminds them that there is always more to learn. Mentorship programs can pair less experienced analysts with veterans, which benefits both: the novice gains skills and the veteran is kept accountable in explaining their reasoning (often revealing tacit knowledge or assumptions that can be examined). The net effect is a collaborative culture where critical thinking is a shared responsibility and learning is ongoing.

3. Support Systems and Organizational Practices: To support the cognitive well-being of cybersecurity engineers, organizations should address factors like cognitive load, stress management, and workspace design. Cybersecurity work can be mentally taxing – the sheer volume of alerts, information sources, and the need for constant vigilance can lead to cognitive overload. To alleviate this, provide tools and user interfaces that streamline information. For instance, a centralized dashboard correlating data from multiple monitoring systems into one coherent view can reduce an analyst's working memory load. If engineers currently must mentally integrate data from separate screens or reports, that extraneous load can be offloaded to better software design. Investing in decision support systems (potentially AI-driven) that highlight anomalies or suggest

probable causes could assist the human analyst. However, care must be taken that such systems are explainable and do not encourage blind trust. The aim is to let humans focus their cognitive energy on the tough reasoning tasks, rather than on attention-consuming but straightforward chores that computers can handle. This concept aligns with treating a person's mental capacity as a precious resource, akin to CPU cycles or RAM in a computer, that should be optimized.

Stress is another aspect that must be managed proactively. As discussed, chronic stress impairs the cognitive functions (attention, memory, flexibility) that cybersecurity professionals rely on. Technical research centers can institute policies and resources for mental health and stress relief. This could include regular breaks during intense operations, access to counseling or stress management workshops, and ensuring on-call rotations are humane (to prevent burnout). Encouraging a culture where taking a brief step back to clear one's head is seen as smart rather than weak can pay dividends. A short break or a good night's rest can often restore the prefrontal cortex's capacity to solve a problem that seemed intractable under fatigue. Additionally, training staff in emotional regulation techniques (some teams practice breathing exercises or quick mindfulness moments before high-pressure tasks) can help maintain composure and clarity of thought during cyber crises. Cybersecurity incidents can sometimes carry significant emotional weight; responding to a major breach is akin to emergency responders at a fire, complete with adrenaline. Having team rituals for after-action debriefs and emotional check-ins can help individuals process the stress and learn from the experience without undue cognitive strain lingering.

Lastly, supporting continuous education and intellectual growth will motivate these inherently curious professionals. Because cybersecurity threats evolve rapidly, engineers must constantly learn and adapt – a process their high Openness predisposes them to enjoy. Employers should provide research opportunities, attend conferences, and experiment with new technologies. This satisfies their intellectual curiosity and exercises their analytical muscles in novel ways, fostering neuroplasticity. It's analogous to cross-training an athlete's muscle groups; engaging with new problems (like a different domain of cybersecurity or a complex puzzle competition) can strengthen the brain's problem-solving networks. Moreover, allowing cybersecurity teams to pursue creative projects (like developing tools or conducting "red team" hacking experiments) can activate more creative, insight-driven thinking to complement their analytical skills. Such initiatives keep the team's collective cognitive toolkit sharp and diverse.

In implementing these support measures, technical research center staff and managers should continually seek feedback from the cybersecurity engineers. These individuals can often articulate what helps or hinders their thinking processes. By treating the analysts as partners in optimizing their cognitive work environment, an organization can fine-tune its approaches (adjusting shift schedules, tweaking a SIEM interface, or adding a whiteboard space for brainstorming) to best support critical thinking. The ultimate objective is to create an ecosystem where the sophisticated reasoning brains of cybersecurity professionals can operate at peak performance with minimal friction. When analytical minds are well-supported, they are more likely to catch that subtle anomaly, solve that thorny problem, and innovate new security solutions – outcomes that benefit the entire enterprise.

Final Insights and Applications

Analytical and critical thinking in cybersecurity engineers arises from a complex interplay of neural circuits and mental processes. The prefrontal cortex and network enable focused, logical reasoning to dissect security problems. At the same time, robust executive functions and certain personality traits equip these professionals to analyze deeply and remain skeptical of easy answers. At the same time, human factors like stress and cognitive biases can impair judgment, even for experts, if not properly managed. Organizations gain a powerful perspective on supporting these invaluable thinkers by understanding how cybersecurity engineers think, which brain regions light up, which cognitive skills come into play, and what personal dispositions are common.

Technical research centers and cybersecurity team managers can apply this knowledge to cultivate training programs that strengthen the neural and cognitive foundations of critical thinking, such as exercises that boost working memory or scenario drills that practice bias awareness. They can design collaboration frameworks that play to analytical strengths while ensuring diverse perspectives and mutual critique to guard against errors. They can also implement support systems that respect the limits of the human brain: reducing unnecessary cognitive load, providing tools that align with cognitive workflows, and promoting a healthy work environment that keeps stress manageable. The result of these efforts is twofold. First, cybersecurity professionals can perform better, making more accurate decisions, faster problem resolution, and creative solutions to emerging threats. Second, these professionals can sustain their performance over the long term, with a lower risk of burnout or cognitive fatigue, thanks to an environment that acknowledges their psychological needs.

In essence, bridging neuroscience and psychology with cybersecurity practice is an emerging frontier that benefits individuals and organizations. As this paper has

discussed, insights from brain science and cognitive research are not esoteric; they directly translate to practical actions like teaching analytical strategies, adjusting team communication, or encouraging brief mindfulness exercises. Cybersecurity is ultimately a human endeavor as much as a technological one. By investing in the human mind – understanding its workings and supporting its development – technical research centers can amplify the capabilities of their cybersecurity engineers. This leads to more innovative defense mechanisms and a more resilient security posture. In a field where adversaries are constantly innovating, leveraging every advantage is critical; knowledge of the neurological and psychological mechanisms of thought is a potent advantage that can elevate cybersecurity training and operations to new heights. The brain is, after all, the most advanced security tool we have – and by caring for and honing this tool, we empower those who protect our digital world.

References

1. Kounios, J. (2019, February 13). *What makes some people creative thinkers and others analytical?* Drexel University. Retrieved April 22, 2025, from https://drexel.edu/news/archive/2019/february/cognitive-styles-of-creative-and-analytical-thinkersDrexel Home+7Drexel Home+7Drexel Home+7
2. GEN Staff. (2025, April 16). *Brain regions essential for logical thinking and problem solving in humans identified*. Genetic Engineering & Biotechnology News. Retrieved April 22, 2025, from https://www.genengnews.com/topics/translational-medicine/brain-regions-essential-for-logical-thinking-and-problem-solving-identified/GEN
3. NeuroSearches. (n.d.). *Neural basis of critical thinking*. Retrieved April 22, 2025, from https://neurosearches.com/post/critical-thinkingneurosearches.com
4. Girotti, M., Adler, S. M., Bulin, S. E., Fucich, E. A., Paredes, D., & Morilak, D. A. (2017). Prefrontal cortex executive processes affected by stress in health and disease. *Progress in Neuro-Psychopharmacology and Biological Psychiatry, 85*, 161–179. https://doi.org/10.1016/j.pnpbp.2017.07.004
5. Schuster, D. (n.d.). *Cognitive factors in cybersecurity*. VECTR Lab at San José State University. Retrieved April 22, 2025, from https://www.vectrlab.net/research.php?area=cybersecurity
6. University College London. (2025, April 16). *Brain areas necessary for reasoning identified*. UCL News. Retrieved April 22, 2025, from https://www.ucl.ac.uk/news/2025/apr/brain-areas-necessary-reasoning-identified
7. Arnsten, A. F. T., Paspalas, C. D., Gamo, N. J., Yang, Y., & Wang, M. (2017). Prefrontal cortex executive processes affected by stress in health and disease. *Progress in Neuro-Psychopharmacology and Biological Psychiatry, 85*, 161–177. https://doi.org/10.1016/j.pnpbp.2017.07.005
8. Luo, J., Tang, X., Zhang, E., & Stupple, E. J. N. (2014). The neural correlates of belief-bias inhibition: The impact of logic training. *Biological Psychology, 106*, 1–7. https://doi.org/10.1016/j.biopsycho.2014.09.010
9. Li, Shuangshuang & Ren, Xuezhu & Schweizer, Karl & Brinthaupt, Thomas & Wang, Tengfei. (2021). Executive functions as predictors of critical thinking: Behavioral and neural evidence. Learning and Instruction. 71. 101376. 10.1016/j.learninstruc.2020.101376.
10. de Wit, J., & Meyer, C. (2022, May 1). Uncovering cognitive biases in security decision making. *Security Management Magazine*. ASIS International. Retrieved

April 22, 2025, from https://www.asisonline.org/security-management-magazine/articles/2022/05/uncovering-cognitive-biases-in-security-decision-making/

End of Document.

IO.