

How to Win at Cyber-Chess: Leveraging Neuro Analytics in Your Cyberspace

by:

Dr. Alenka Brown
Senior Managing Member
McClure, Brown, & Associates LLC

Jason Christman
MS, CISSP, PMP
McClure, Brown, & Associates LLC



The cyber domain presents limitless opportunities for cyber threat actors while causing significant challenges for cybersecurity professionals. While our current time might be construed by historians as the golden age of cybercrime, it is also an age that offers new ways and means to counter these crimes. Neuro-behavior forensics is such a means, permitting the extraction of analog indicators¹ to identify an intruder's internal thought process – more specifically, the neurocognitive 'decision' pattern that aligns with the system or network behavior. This is possible because cyber intruders leave behind cognitive fingerprints with neuro psychometric markers² that can be translated into cognitive patterns.³ Neuro cyber analytics deciphers these indicators, of analog or digital origin,⁴ into a cognitive print (Cogni-print®)⁵, or signature, in order to make sense of how the intruder thinks in the context of committing a cybercrime. Neuro cyber analytics unravels the footprint of cyber intruders using an engineering system approach in order to help professionals 'protect, detect, respond, and recover'⁶ from unwarranted or unexpected cyber acts.

Neuro cyber analytics is a process by which cues are translated into neurocognitive patterns, and from which expected behaviors, biases, and beliefs could be determined.

Neurocognitive Patterns

Cyber threat is derived from an individual or a collective group making calculated decisions. These decisions exhibit behaviors based on a person's neurosensory experience – how they see, hear, and feel within a given context. As a person processes information from their environment, they unconsciously show neuropsychometric indicators that are embedded within their verbal and nonverbal behavior.

These cues, or tells, reveal how people sort, order, and sequence their thoughts into distinct neurocognitive 'decision' patterns. These tells are found in various forms in cyber domains: videos, audio, photographs, social media postings, website layout, emails, keystrokes, and so forth. They are key in determining the internal strategies at play of how people establish a preferred neurocognitive pattern, and when the cognitive pattern changes depending upon context and their state of mind.

Neuro cyber analytics is a process by which cues are translated into neurocognitive patterns, and from which expected behaviors, biases, and beliefs can be determined. Neuro cyber analytics tell us whether a person's behavior is based on their preferred cognitive pattern, such as deceptiveness within a specific context. As in a polygraph, a baseline is first obtained by establishing a person's preferred or 'normal' behavioral responses to stimuli and is then monitored for changes. Significant changes in behavioral responses for a given context indicate a shift in the baseline that may warrant further investigation. The same holds true for people operating within cyber-ecosystems. A baseline Cogni-print® is collected when a user is first authenticated and granted access to the information systems. This baseline is then used to continuously monitor for significant shifts in the user's behaviors, correlated to various network behaviors. This is especially useful for detecting possible insider threats to an individual or organization, anomalies in system behaviors, falsified identities, or time-sensitive or critical courses of action.

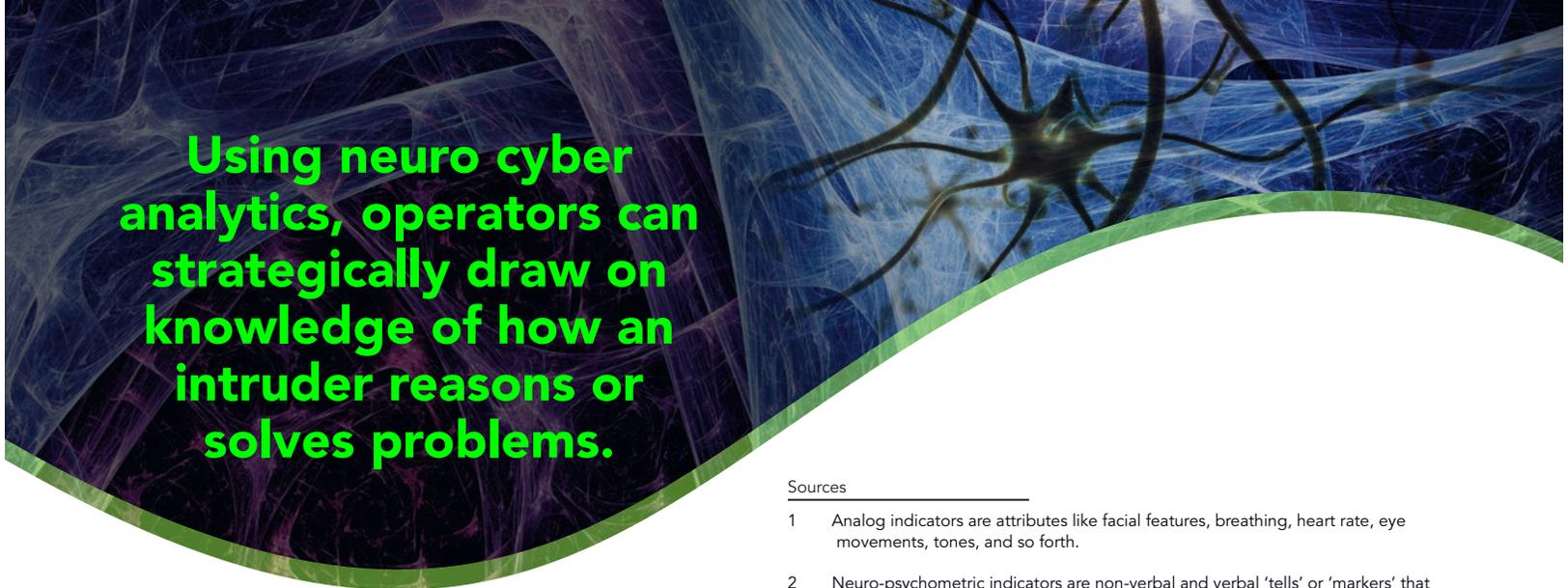
Convergence of Digital and Analog (Human) Forensics

Since cyber intruders leave residual Cogni-prints® within cyber-ecosystems they exploit, these prints are potential forensic evidence. The use of Cogni-prints® as e-discovery evidence, aligned with digital forensics, offers cyber operators or analysts a powerful new tradecraft (neuro cyber analytics) for solving and outmaneuvering cyber incursions.

We know digital forensics produces valuable information that is used by cybersecurity professionals to track and monitor system-network behaviors. By adding analog forensics, neuro cyber analytics can draw further conclusions for cyber investigators about strategies used by intruders in setting up and performing intrusions. The ability to form Cogni-prints® from analog or digital forensics to assess and monitor incongruent behaviors is essential for continuous authentication and attribution of an individual actor or collective of cyber actors. This integrated approach to forensics paves the way for an automated Cogni-print® engine that would enable intrusion prevention by dynamically defending the system at network speed, adapting to an adversary's decision processes. This provides a more effective way to hunt cyber-intruders as one's Cogni-print® is extremely difficult to conceal.

These patterns identify behaviors one can expect to see of intruders and the cyber professionals who hunt them, in addition to their strengths and weaknesses when moving through a particular cyber act. Consequently, neuro cyber analytics, whether employed as a tradecraft or as an automated capability, can help frontline cyber operators and analysts gain a human-dimensional edge against the onslaught of current and future cyber threats.





Using neuro cyber analytics, operators can strategically draw on knowledge of how an intruder reasons or solves problems.

Operationalized

As part of an overall cyber risk management strategy, neuro cyber analytics has a role to play in every phase of deploying, operating, maintaining, and defending a networked technology infrastructure, be it a commercial enterprise, industrial control system, or military weapons system. Network and system security administrators can implement Cogni-print® active authentication as another factor in their identity and access management strategy. External cyber intruders or insider threat actors would find gaining authenticated access to networks challenging, since it would be quite difficult to impersonate the cognitive patterns of a legitimate user. Cyber hunters would use neuro cyber analytics to continuously monitor the user's neuro cybermetrics for user-system behavior anomalies, flagging incongruent behaviors linked to a set of cyber personae for attribution.

Using neuro cyber analytics, operators can strategically draw on knowledge of how an intruder reasons or solves problems. Thus, they can become more proactive in mitigating security risks. Cyber analysts, operators, and planners can become more proficient strategists with the ability to move pieces in positions of influence for an ultimate checkmate.

Acknowledgement

We wish to acknowledge Dr. Joe McClure VanHoozer, Senior Managing Member of McClure, Brown, & Associates LLC, and leading expert in neuro analytics, neurolinguistics, and Cogni-print for his generous time in reviewing and editing this article.

Sources

- 1 Analog indicators are attributes like facial features, breathing, heart rate, eye movements, tones, and so forth.
- 2 Neuro-psychometric indicators are non-verbal and verbal 'tells' or 'markers' that translate to one of our five senses.
- 3 Cognitive patterns are the repetitive process that humans use for mapping their reality in making decisions.
- 4 Digital indicators (in this article) are verbal indications, like words and phrases.
- 5 Cogni-print® is a registered trademark of McClure, Brown, and Associates LLC.
- 6 Core activities to achieve specific cybersecurity outcomes outlined in the NIST Cybersecurity Framework. National Institute of Standards and Technology: "Framework for Improving Critical Infrastructure Cybersecurity." February 2014. <<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>>

About the Authors

Dr. Alenka Brown is a Senior Managing Member of McClure, Brown, & Associates LLC. She is a leading expert in neuro cyber analytics and Cogni-print®. She has a diverse background encompassing applied research, system integration, policy, energy, intelligence, special operations, and cognitive autonomous systems. She is currently a member of NIST's working group for cloud overlay and security reference architecture, cloud forensics, and continuous monitoring. She is also a member of OSSI's Strategic Planning working group and NCOIC's Cybersecurity Integrated Project Team and cloud computing working group.

Jason Christman, MS, CISSP, PMP is an industry leader and domain expert in cyber operations planning and execution, threat intelligence analysis, and human decision analytics. His strategic planning, mission management, and technology development background spans the homeland defense, intelligence, special operations, and commercial telecommunication business arenas. Jason is an ardent supporter of human-centered computing and is a proponent for the convergence of neurocognitive technology and cyber ecosystems.

