SOC Puppets: How Whaley's *Theory of Outs* and 'Noisy' Sock Puppets Encouraging Discovery of Network Deception Could Enhance Security Operations Center Analysis

Tim Pappa[1] and Keyur Rajyaguru
[1]Analyst1, Reston, Virginia, USA

tim.pappa@analyst1.com
kpr@umd.edu

Abstract: This practitioners' position paper suggests an unorthodox approach integrating Whaley's *Theory of Outs* and "turnabout" deception techniques to encourage an attacker's discovery of deception on a network. Although the late American deception and communication researcher Barton Whaley appeared to differentiate the categorization of deception techniques such as "turnabout" and planning for backup deception techniques if discovered or if the deception appeared to fail, we explore the integration of these approaches to deception design in a cyber context, mainly in situations where analysts in the Security Operations Center (SOC) are looking for higher fidelity alerting on anomalous events and suspected attacker activity on the network. Because attackers appear to generally demonstrate greater confidence in their network movement after discovering what they believe is deception, we visualize how 'noisy' controlled deception sock puppets inside of a network prompting optimized query returns on their content could draw attackers to later stage deception functions and effects, and more enhanced SOC analysis following alerting on those functions and effects. This practitioners' position paper suggests our unorthodox approach offers an alternative strategic and tactical approach to collaborative cyber deception design and SOC alerting, by highlighting 'noisy' deception on a network to lure and influence attackers.

Keywords: Cyber deception, Theory of outs, Turnabout, Security operations center, Cyber deception design

1. Introduction

This proposed integrated modeling is foundationally based on an increasingly practiced unorthodox operational approach to industry cyber deception, where deception is intentionally 'noisy' and staged to be discovered. Fundamentally, this idea contradicts the traditional SOC analysis approach where noisy detections are tuned out to prevent alert fatigue. However, our more recent experience in industry cyber deception operations has involved more of an organizational approach to deception functions and effects, where generally there is less direct engagement with attackers than we previously experienced when supporting law enforcement operations online. Because there is generally less direct engagement with attackers, there is often less observed attacker behaviors. Designing deception functions and effects without a baseline of behavior is arguably difficult. There must be some application of behavioral and cognitive frameworks in the absence of demonstrated attacker behaviors.

Much of the research in the past several years related to behavioral and cognitive frameworks has concentrated on cognitive vulnerabilities and attacker behaviors on a host or network when influenced by a range of cognitive biases. This research concentration on cognitive biases reflects growing efforts to explore a cognitive theory of deception, instead of what has historically been a focus on physical deception cues. Many of these same researchers concentrating on the effect of cognitive biases have encouraged a more "adaptive" cyber deception design and build, primarily based on deceptive signaling targeting attackers designed to influence changes in their attacker behaviors (Cranford et al., 2020; Cranford et al., 2021). Gonzalez et al. (2020) advocated for more dynamic forms of defense, with deception integrated into engineering design. Gonzalez et al. wrote that designing effective defense must consider the knowledge of human behaviors, namely the way people make decisions and explore a network. Incorporating these kinds of "dynamic forms of defense" in deception could result in a collection of uniquely rich attacker behaviors that demonstrate an individual attacker's reconnaissance and decision-making. That behaviorally rich collection could inform more behaviorally adaptive cyber deception operations.

Aggarwal et al. (2024) wanted to build on their findings from a prior study where participants behaving like attackers appeared to identify cognitive biases, exploring whether attackers showed any preference for targeting specific areas of a network and if attackers revealed any behavioral patterns when operating in those specific areas. Their findings suggested attackers did demonstrate cognitive biases, such as sunk cost fallacy and default effect. The goal of this follow-up research was to determine if defenders could create more dynamic

responses to attackers based on linking identified cognitive biases with "behavioral patterns" observed in similar network environments. Some of these behavioral patterns appeared to reflect default effect, where attackers are more likely to choose a "preset alternative" or default when making decisions. This finding is like naturalistic decision-making research, where attacker decision makers appear to process information differently, based on their experiences making similar decisions when presented with similar information in the past (Du et al., 2023; Yuill, Denning, and Feer, 2007). Aggarwal et al. in their recent study found that attackers appeared to demonstrate this default effect most commonly in the reconnaissance phase of their attack cycle. Aggarwal et al. (2024) found other cognitive biases as well, such as availability bias or when people appear to make choices based on the information that comes to mind first, for example. Their findings in this study highlighted what they characterized as the strength of the "presence of a bias", based on whether participants behaving like attackers found a task or function on a network to be interesting or not or to what degree they found it interesting. Aggarwal et al. suggested that there are other functions that attackers may find less interesting, that may exploit other cognitive biases because of the kind of processing someone might engage in when completing some task or function considered to be mundane or expected.

Shinde and Doshi (2024) presented an approach to modeling and exploiting the cognitive biases of attackers when planning for "active deception", highlighting the cognitive biases fundamental attribution error and confirmation bias. Shinde and Doshi concentrated on human attackers, arguing that sophisticated attacks are still largely driven by human attackers, and human attackers are vulnerable to these cognitive biases. Their approach noted that even cyber deception largely developed with artificial intelligence is still based on a belief that attackers will be rational, when most attackers are not necessarily rational but vulnerable to these biases and other decision-making influences. Shinde and Doshi largely focused on the information gathering process of attackers and how they might overattribute factors in an environment to a human defender rather than assessing an environment they observe and interact with based on network and host functions. An example might be an attacker who believes a Bloodhound attack pathway is only vulnerable because defenders have nestled that pathway with decoys that alert on attackers, but perhaps in this example that attack pathway is vulnerable because defenders have overlooked vulnerabilities on that pathway because they defaulted to automated monitoring and mitigation management.

Aggarwal et al. (2025) tested approximately a half dozen cognitive biases with participants in similar studies, finding similar results like the cognitive biases studies above. But another finding was that participants' experience and knowledge did appear to limit the potential effect of attempts to induce cognitive biases in participants. While those more experienced participants may have been less affected by these tasks, they also appeared to be more willing to take risks during scenarios in this study. The findings suggested there may be a shift in risk preferences among experienced attackers that do not reflect the commonly reported findings on risk aversion.

In contrast, the information security industry's typical approach to cyber deception has largely been static and functional, however. There is a modestly growing market for commercial off-the-shelf software for deception and packaged honeypots. Those honey- prefix builds have evolved significantly in the past twenty years, but these 'turnkey' applications are generally limited and instrumental to a function on a network, rather than a function behaviorally responsive to observed attackers (Javadpour et al., 2024). These approaches are largely mitigation techniques. Lansborough et al. (2021) noted that defensive network systems are historically statically configured, generally failing to adapt to an attacker or adapt in ways that an attacker predicts or easily counters.

Strand's industry handbook on cyber deception, "The Art of Active Defense", represented almost a decade of advocating for more offensive or proactive responses to attackers. Strand (2017) wrote that network defenders should engage attackers whenever possible, essentially 'annoying' them by wasting their time and forcing them to make additional moves, which are likely to increase collection on an attacker toward some attribution. Strand often characterized cyber deception as "annoyance". Strand's handbook included a considerable number of techniques that can be applied to attackers, but these engagements would usually occur during some phase of incident response or threat hunting. These techniques were generally reactive to attackers, designed to frustrate attackers. There was limited knowledge in those moments of an attacker's behaviors or capabilities. This approach largely continues to be the standard, except when augmented with increasingly automated and curated deception software. There may be growing recognition that simply suggesting there is deception on a network is effective. There are still few organizations that appear willing to communicate that (Ferguson-Walter, 2018, 2019, 2024). We agree with this research approach into the cognitive vulnerabilities of attackers, but we also suggest that there are deception techniques or approaches that have still rarely been applied or operationalized by network defenders or cyber deception practitioners. These techniques or approaches have

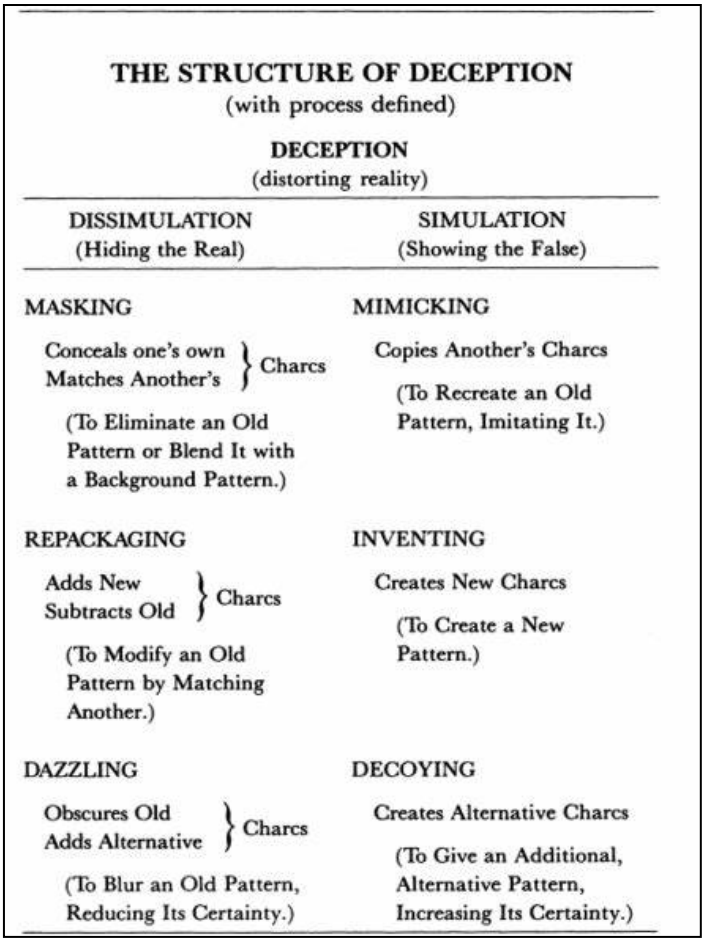
been discussed in historical military deception research and commentary, but there has been little to no known application in cyber deception and SOC contexts.

This paper is organized as follows. First, this paper will briefly discuss some of Whaley's historical work on deception. His shared framework is the foundation of the deception techniques discussed in this paper, including his *Theory of Outs* and his discussion of the "turnabout" techniques. Second, this paper will include a working characterization of the integrated approach of this theory and these lesser-known techniques in a cyber context. Third, this position paper will highlight the function of SOC across industry and organization and how Deception operations integrate within the defensive methodologies. Finally, this paper will visualize the application of this integrated approach to cyber deception to help enhance the SOC's analysis of suspected and known attacker events and incidents when incorporating 'noisy' sock puppets.

2. Related Work on Whaley's Characterizations of Deception and Misperception

The Bell-Whaley (1982, 2017) framework is the starting point for the author's cyber deception design process. This framework has been discussed extensively in literature, primarily in military deception literature (Daniel and Herbig, 1982; Martin, 2008; Whaley, 1982; Lloyd, 2003; Smith, 1992). Bell and Whaley structured this framework to demonstrate that these techniques are simultaneously *dissimulating* and *simulating*. Dissimulating in any deception scenario might include masking, or hiding the real by making it invisible, for example. Simulation might include inventing or showing the false by fabricating something.

Whaley (1974) emphasized the simultaneous dynamic of this deception framework in an early characterization where he described a scenario of burying a bag of gold coins in his backyard. He wrote that if he is burying or hiding (*dissimulating*) the golden coins to hide his wealth, he is simultaneously demonstrating or suggesting (*simulating*) that the golden coins are not at his home or that the golden coins are located somewhere else, and he is also simulating that he is not wealthy but in fact poor.



THE STRUCTURE OF DECEPTION
(with process defined)

DECEPTION
(distorting reality)

DISSIMULATION (Hiding the Real)	SIMULATION (Showing the False)
MASKING	**MIMICKING**
Conceals one's own / Matches Another's } Charcs	Copies Another's Charcs
(To Eliminate an Old Pattern or Blend It with a Background Pattern.)	(To Recreate an Old Pattern, Imitating It.)
REPACKAGING	**INVENTING**
Adds New / Subtracts Old } Charcs	Creates New Charcs
(To Modify an Old Pattern by Matching Another.)	(To Create a New Pattern.)
DAZZLING	**DECOYING**
Obscures Old / Adds Alternative } Charcs	Creates Alternative Charcs
(To Blur an Old Pattern, Reducing Its Certainty.)	(To Give an Additional, Alternative Pattern, Increasing Its Certainty.)

Figure 1: The Bell-Whaley deception framework

Whaley (1980) wrote that he believed there was a "poverty of theory" about misperception of simulation and dissimulation as a foundational deception model, meaning people may generally understand surprise or how they feel to be surprised but they may not recognize the psychological underpinnings of surprise.

Whaley described misperception as both *qualitative* and *quantitative*. The qualitative depth of misperception is variety, namely that there are several ways in which someone or a system can be deceived. Someone or a system could misperceive something that is observed or communicated. Whaley wrote that the quantitative depth or dimension of misperception is intensity, namely the degree or even the frequency to which misperception occurs. Whaley (1984) added that when we consider how we characterize misperception in terms of the variety of cues, in that perception and the intensity of or degree of that misperception, we could think of players on a baseball team as a characterization of strength in the context of misperception.

Whaley wrote that while we can count each player on a team in terms of numbers to represent strength, we also can and should consider how each player has qualitatively differentiated roles and positions on a team. Whaley noted that each of those players individually may be better or worse than each other and may be better or worse than other players on other teams. Whaley wrote that "we tend to think we know who the players are", but that can change depending on which baseball teams are playing against each other and how those players on each team are performing and how they chose to perform.

3. A Working Characterization of Integrated "Turnabout" and "Outs" Deception Planning

The purpose of this paper is to explore how someone like an attacker might respond behaviorally and cognitively to deception, especially when an attacker believes they have discovered deception. Whaley characterized "turnabout" as a context where deception appears to have been discovered, and there is an opportunity to respond with deception. "Turnabout" was a historical and practiced technique in military deception, but Whaley found that planning for "turnabout" in contemporary deception operations in the military appeared to be considerably rare in contrast to the practice of "turnabout" in historical military examples.

Whaley shared an example of "turnabout" in a plot by Soviet intelligence to add laxatives to the saltshakers in the Radio Free Europe cafeteria in Prague. The Soviet asset directed to add the laxatives confessed to security personnel and then American intelligence the plot before any saltshakers were compromised, but American intelligence allowed this plot to be revealed publicly to expose this attempt by Soviet intelligence to frighten Radio Free Europe personnel and locals working for this American government news media organization. American intelligence allowed this plot to proceed for a while before exposing it.

Whaley wrote about what has been called a "Let's Double Back trick" or a "double back" as another representation of "turnabout". This generally means someone has 'doubled back' to a starting point in an ongoing deception, whether that deception was planned or not. The audience or target of that deception may presume that someone in some pattern is following a sequence of activity that will lead to an anticipated outcome, rather than returning to a starting point. The "double back" is surprising, then. But deception planners planned for it.

Whaley referred to a deception operation in the 1970s where the Central Intelligence Agency had been collecting imagery of the Soviet Union from their KH-11 "Keyhole" satellite, searching for potential SALT agreement violations related to missile production. Because the Soviets were aware of this collection, they would often relocate or hide missile infrastructure. When the CIA later incorporated an unknown new design feature in the KH-11 satellite, where collection was transferred to another satellite and then transmitted to the ground rather than directly from the KH-11 to ground, the Soviets could no longer detect any data imagery transmissions from the KH-11 to ground. The Soviets' conclusion appeared to be that the satellite was "dead".

The Soviets stopped hiding their missiles during these flyovers because they believed the satellite was not collecting imagery. But the CIA continued collection and transmission, until the Soviets later discovered from an asset that the CIA had modified the satellite.

Whaley referred to another example of "double back" from an operation known as MOONSHINE from World War II. The British had begun distorting German radar detection by using older models of radar emulation technology. When the British began 'doubling back' or reintroducing older versions of their radar technology, the Germans struggled to accurately detect enemy aircraft. The number or scale of approaching British aircraft was distorted because the Germans had configured their detection systems to look for more advanced British radar hardware. The Germans eventually discovered this "double back" and adjusted their detection efforts. About a year after that discovery, the British reintroduced this early version of their radar emulation of an older

model again, which again distorted German detection efforts because they expected to see more advanced versions.

Whaley differentiated his *Theory of Outs* as planning for "alternative goals" for a deception if that deception is discovered or if the deception appears to have failed. Whaley wrote that deception rarely fails because there is generally some effect because of deception where the target is influenced in some manner, but deception planners in his experience consistently did not include options in their deception operations for accomplishing the deception or influence goal in some other way if the deception was discovered.

There are situations he wrote where a strategic goal of deception may appear to have failed, but a tactical goal of the same deception succeeds.

Whaley wrote about the "Delayed Message Trick" where the true operational plans are transmitted on a channel the target is monitoring, but the transmission is slowed or delayed in a manner where the target will be unable to react effectively. Whaley wrote that this approach is rare and should be used sparingly, but this is an example of planning for an "out" by managing the transmission of the operational plans but perhaps keeping those plans vague and making it appear there are technical issues with the target's monitoring infrastructure. There is still flexibility in this deception design to hold the target's attention and influence them, but to control the transmission or communication of that deception content.

Whaley referred to failed airborne parachute drops in Normandy in 1944 as an example of what appeared to be failed deception, but the deception was still effective. The goal of Allied airborne drops in Normandy was to slow or block the responding German reinforcements until the beachhead was secured. There were also "diversionary drops" of fake or dummy paratroop units. Whaley wrote that the Germans were immediately aware of the scattered airborne drops, but they assumed those scattered drops were deliberate rather than a mistake.

The Germans missed an opportunity to destroy or ignore those scattered and lightly armed parachute units and proceed directly to the beachhead, but instead because the Germans believed it was deliberate they allocated reinforcements to engage each of those scattered units slowly and cautiously. Whaley wrote that the unplanned failed airborne drops and scattered units appeared to have a better effect than the planned version because it still achieved the objective of slowing the Germans' response. Whaley emphasized the need for deception planners incorporating "outs" in their deception operation to consider how the target might misperceive deception it discovers or believes it has discovered.

This paper characterizes a working approach to deception planning or deception design integrating "turnabout" and this theory of "outs", where planners include the discovery of the deception into their design.

Whaley may have intended these approaches or techniques in deception to be separate given the context or situation, but the author suggests that in a naturalistic offline and online network attack environment there should be an integration of these techniques and layered deception design.

4. Role of the Security Operations Center (SOC) in Cyber Defense and how "Turnabout" Deception Strengthens Defensive Mechanisms

A Cyber Security Operations Center (SOC) is a unit within an organization responsible for monitoring and responding to cyber threats in real time. Generally, a team of cybersecurity analysts operates 24/7 to investigate alerts, determine their severity, and take necessary actions.

Deception operations can be integrated into alert pipelines. Some of the most common deception artifacts include false credentials stored in documents, or fake confidential documents, for example. Any alert from the honeypots enhances SOC operations by providing context about the attacker or insider threat behavior, objectives and methods leveraged. A fake but strategically placed honeytoken when accessed gives the SOC insights into what data types are targeted by the attackers.

Learning attacker techniques is a much-needed part of proactive and reactive cyber defense. These techniques become more useful when they are observed in the infrastructure the SOC is trying to protect. Since these activities are performed in an environment where we have full control, it becomes an attractive investment to put in some time and extract intelligence compared to the generic intelligence available about various attacker groups. deception alerts are inherently different from other SOC alerts. Generally, SOC alerts focus on anomalies in the network and user behavior to catch them. These anomalies can be in different forms like time of activity, length of engagement, nature of user performing actions, number of attempts made to access artifacts, and so

on. In deception alerts, those honeytokens are placed strategically where no one would attempt to access for their daily operations, only the ones with "extra curious" mindset or someone with intention of gaining unauthorized access to the confidential details would access it. The alerts become even more helpful when the tokens are placed further into the campaign from the entry point of the lure. Many times, people will stop progressing if they sense that they are not supposed to access this information. An attacker would not stop because that is exactly what they are after. A noisy deception environment would make an attacker more interested in advancing the attack even if they sense deception because they believe they can laterally move, and they have a strong foothold in the infrastructure. Some attackers may keep advancing just because of a great reconnaissance opportunity as they want to collect intelligence about the victim to use it later in other attack campaigns. This is where SOC can leverage "turnabout" deception techniques to study attacker behavior. These learnings can be funneled back to the detection logic and can be mapped elsewhere in the infrastructure. Feedback from SOC to a cyber deception team will also help to create more honey content that works. There are always some traces that attackers leave behind, even behaviors that bypass traditional rules or signature-based attack methodologies. Mapping those Indicators of Behavior within the enterprise network would improve security posture. SOC can leverage the use of MITRE ATT&CK framework to demonstrate how deception helps catalog attacker Techniques, Tactics, and Procedures (TTPs) before they can target valuable systems. These insights allow SOC to modify existing detections.

5. Visualizing a 'Noisy' Sock Puppet Deception Approach Integrating "Turnabout" and "Outs" Modeling

This cyber deception practitioner's position paper visualizes a scenario in which a controlled sock puppet account that appears to be demonstrably affiliated with a company has been consistently posting content on a social media platform about his or her infrastructure development work. This sock puppet by design has been making mostly generalized references to his or her projects, but there are also keywords in the content in blogs and posts that may be of interest to attackers who are also interested in targeting this company. This might include references to unique tools or projects that appear to be developmental, and involving access to company data considered to be sensitive or valuable if an attacker stole that data to sell it on a market.

Even if the attacker in this scenario obtains unauthorized access to this company's network simply by obtaining basic user account credentials, there will likely be some effort inside the network to verify whether the sock puppet account is a company employee or not and if that employee is posting or sharing content inside the network about similar projects. That kind of consistency in content creation and sharing over time by the same controlled sock puppet account is what makes that deception storyline plausible.

When the attacker in this scenario begins to query certain terms or keywords associated with this sock puppets projects and the area of interest to the attacker, there should be optimization of this sock puppet's content because of the consistent and considerable content creation internally by the sock puppet. This is the 'noisy' sock puppet content. While these are internal platforms, there are similar approaches to optimizing search content. Because there has been consistent content sharing by this sock puppet, there may have been prior false positives from other company employees curious about these projects or employees questioning the content he or she is posting. This is what makes this sock puppet content 'noisy'.

Network defenders in this scenario may have also placed simple decoys along this possible attack pathway for an attacker, so that the attacker will avoid what appear to be oddly placed honey files with likely alerting and perhaps obvious naming conventions on the files, such as "sensitive data_confidential_Q1". The author recognizes that this kind of naming convention may still appeal to attackers who will try to access this kind of honey file because of the naming convention or description of the data in the file in the title, however, this kind of approach would still represent the author's proposed integrated modeling of "turnabout" and "outs" deception planning. Network defenders want the attacker in this scenario to believe he or she has discovered these honey files in a plausible attack pathway, so that they will either trip those decoys and return with other credentials in the future or they will avoid these honey files and continue their movement, perhaps confident they have detected this deception.

In this scenario, once the attacker finds content of interest from his or her queries of keywords or terms of interest and the search return includes the sock puppet's content, the attacker may scrutinize this content less because he or she is familiar with this deception storyline, but unaware this is deceptive. The indexed content may include a hyperlink to another site on the network that suggests access to the data the attacker is seeking. When the attacker clicks on this link, he or she is transferred to a site where he or she can enter his or her stolen

user credentials. That access attempt will be successful, but there will be alerts. Then the attacker will be transferred to another controlled portal with further warning on that site regarding confidential access. When the attacker attempts to sign into this portal with the same credentials, the SOC will be alerted immediately. This incremental sequence of deception effects and function limits the number of false positives, discouraging employees from attempting to explore and access these sites and content. This sequence of deception functions also allows the SOC to observe a user's intent and to capture a high-fidelity alert.

6. Discussion

This visualized scenario demonstrates how a 'noisy' sock puppet's content creation inside and outside a network can not only gain the attention of an attacker and influence that attacker's cognitive and behavioral decision making throughout his or her attack cycle but mitigate and manage the behaviors of false positives or other employees who may also become interested in this 'noisy' content.

The visualized scenario applied the design framework proposed in this position paper. The attacker was presented with simple deception decoys along plausible attack pathways so that he or she would find that deception easily or avoid that deception and continue moving. We believed this might increase the attacker's confidence and suggested that the company's attempt at deception had been discovered and had failed.

Because the attacker may believe he or she has discovered this failed deception, he or she may scrutinize the remainder of files and data sites on the network. The sock puppet's content creation outside the network on a social media platform may have been surprising, but once the attacker quickly determines that this sock puppet appears to be a real employee at this company, the attacker again may scrutinize the sock puppet's content less. The attacker's belief that he or she has easily discovered attempts at deception and that he or she has successfully found a pathway to the data of interest associated with the sock puppet could have surprised or violated the attacker's expectations, but the author argues that the true violation of the attacker's expectations will occur when the attacker is transferred to controlled infrastructure and alerted on each of his or her attempts. The attacker will be quickly mitigated or will exit the network promptly when he or she realizes that the controlled portal and sock puppet content was also a deception, but much more material and influential.

Even in this relatively brief interaction and deception effect and function between an attacker and this controlled 'noisy' sock puppet content and deception, network defenders have demonstrably surprised or violated the attacker's expectations of network defense and deception capability. We argue that this is not only a reputational deterrence, but a strategic and tactical change in this company's interactions with this attacker and likely future attackers. This kind of cyber deception design modeling and application could enhance the SOC's confidence in their collection and analysis of these high-fidelity alerts based on 'noisy' sock puppets.

Ethics Declaration: Ethics clearance was not required for this paper.

AI Declaration: There was no use of AI in the development or at any other stage of this paper.

References

Aggarwal, P., Venkatesan, S., Youzwak, J., Chadha, R. and Gonzalez, C., 2024. Discovering Cognitive Biases in Cyber Attackers' Network Exploitation Activities: A Case Study. In *Human factors in cybersecurity. AHFE (2024) International conference*.

Aggarwal, P., Rubaiyet Nowmi, S., Du, Y. and Gonzalez, C., 2024. Evidence of Cognitive Biases in Cyber Attackers from An Empirical Study.

Aggarwal, A., Ferreria, Maria J., Aggarwal, P., Rajivan, P., and Gonzalez, C., 2025. Cognitive Biases in Cyber Attacker Decision Making: Translating Behavioral Insights into Cybersecurity. In 10th IEEE European Symposium on Security & Privacy Workshops, 4th Active Defense & Deception Workshop, Proceedings.

Bell, J.B. and Whaley, B., 2017. *Cheating and deception*. Routledge.

Bell, J.B. and Whaley, B., 1982. *Cheating: deception in war & magic, games & sports, sex & religion, business & con games, politics & espionage, art & science*. St Martin's Press.

Cranford, E.A., Gonzalez, C., Aggarwal, P., Tambe, M., Cooney, S. and Lebiere, C., 2021. Towards a cognitive theory of cyber deception. *Cognitive Science*, *45*(7), p.e13013.

Cranford, E., Gonzalez, C., Aggarwal, P., Cooney, S., Tambe, M. and Lebiere, C., 2020. Adaptive cyber deception: Cognitively informed signaling for cyber defense.

Daniel, D.C. and Herbig, K.L., 1982. Propositions on military deception. *The Journal of Strategic Studies*, *5*(1), pp.155-177.

Du, Y., Prébot, B., Xi, X. and Gonzalez, C., 2023, January. A Cyber-War Between Bots: Human-Like Attackers are More Challenging for Defenders than Deterministic Attackers. In *HICSS* (pp. 856-865).

Ferguson-Walter, K., Shade, T., Rogers, A., Trumbo, M.C.S., Nauer, K.S., Divis, K.M., Jones, A., Combs, A. and Abbott, R.G., 2018. *The Tularosa Study: An Experimental Design and Implementation to Quantify the Effectiveness of Cyber Deception* (No. SAND2018-5870C). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

Ferguson-Walter, K., Shade, T.B., Rogers, A.V., Niedbala, E., Trumbo, M., Nauer, K., Divis, K., Jones, A., Combs, A. and Abbott, R., 2019. *Appendix to the Tularosa study: an experimental design and implementation to quantify the effectiveness of cyber deception* [online]

Ferguson-Walter, K.J., 2024. An empirical assessment of the effectiveness of deception for cyber defense.

Gonzalez, C., Aggarwal, P., Cranford, E.A. and Lebiere, C., 1825, January. Design of dynamic and personalized deception: A research framework and new insights for cyberdefense. In *Proceedings of the 53rd hawaii international conference on system sciences* (Vol. 1834).

Javadpour, A., Ja'fari, F., Taleb, T., Shojafar, M. and Benzaïd, C., 2024. A comprehensive survey on cyber deception techniques to improve honeypot performance. *Computers & Security*, p.103792.

Kambow, N. and Passi, L.K., 2014. Honeypots: The need of network security. *International Journal of Computer Science and Information Technologies*, *5*(5), pp.6098-6101.

Landsborough, J., Carpenter, L., Coronado, B., Fugate, S., Ferguson-Walter, K. and Van Bruggen, D., 2021, January. Towards Self-Adaptive Cyber Deception for Defense. In *HICSS* (pp. 1-10).

Lloyd, M., 2003. *The art of military deception*. Pen and Sword.

Martin, C.L., 2008. *Military deception reconsidered* (Doctoral dissertation, Monterey, California. Naval Postgraduate School).

Mokube, I. and Adams, M., 2007, March. Honeypots: concepts, approaches, and challenges. In *Proceedings of the 45th annual southeast regional conference* (pp. 321-326).

Shinde, A. and Doshi, P., 2024, May. Modeling cognitive biases in decision-theoretic planning for active cyber deception. In *Proceedings of the 23rd International Conference on Autonomous Agents and Multiagent Systems* (pp. 1718-1726).

Smith, D.V., 1992. Military Deception and Operational Art.

Strand, J., Asadoorian, P., Robish, E. and Donnelly, B., 2013. *Offensive Countermeasures: The Art of Active Defense*. CreateSpace Independent Publishing Platform.

Whaley, B., 1982. Toward a general theory of deception. *The Journal of Strategic Studies*, *5*(1), pp.178-192.

Whaley, B., 1980. A Typology of Misperception or The Ways We Can Be Wrong. *Unpublished manuscript draft*.

Whaley, B., 1974. Deception: Its Decline and Revival in International Conflict. *Unpublished manuscript draft*.

Whaley, B., 2016. *Turnabout and Deception: Crafting the Double-cross and the Theory of Outs*. Naval Institute Press.

Yuill, J., Denning, D. and Feer, F., 2007, January. Psychological vulnerabilities to deception, for use in computer security. In *DoD Cyber Crime Conference* (Vol. 2007).