Reflexive Control Theory in Cyber Operations

Sheyla Gyles
Computer Science Department
Hampton University
Hampton, VA

Abstract – This report will discuss and explore the concept of reflexive control theory (RCT) in the context of day-to-day cybersecurity operations. Specifically, this study aims to investigate and emphasize the influential role of this trend in cyberspace while simultaneously examining the manipulative tactics employed by adversaries and RCT's effect on the public. This report will further explain the concept of RCT and aims to promote awareness to educate the public about this topic. In the realm of cybersecurity, reflexive control serves as a potent weapon, used to allow adversaries to be able to exploit vulnerabilities, influence decision-making and essentially predict their target's actions. This research will focus on three key concepts within reflexive control theory: Behavioral Analysis, Threat Detection and Perception Management. Furthermore, this report examines the ethical dimensions and potential risks associated with the reflexive control theory technique. These findings are intended to raise awareness and propose strategies to enhance resilience against these manipulative tactics. By meticulously synthesizing existing literature, research studies, and user surveys, this report provides a comprehensive analysis of the reflexive control theory in cyber operations.

Figure 14: Reflexive Control

I. Introduction

Historically, the concept of manipulating individuals for personal gain or espionage predates the digital age. From the 'Trojan Horse' of ancient times to the sophisticated misinformation campaigns of the Cold War, the manipulation of human behavior has been one of the only constants in the realm of conflict. However, the creation of the internet and its allowance for the interconnectedness of modern society have exponentially expanded the avenues through which social engineering can be employed. What makes social engineering particularly insidious is its ability to exploit not only technological vulnerabilities but also the inherent cognitive biases and emotional responses of individuals. In this modern time, it has become increasingly evident that manipulating people has always been an

accessible and potent tool in the cyber adversary's arsenal. Through this reflexive control theory was formed.

In cybersecurity, reflexive control theory refers to the manipulation of an adversary's decision-making process through the use of information and psychological techniques. In simpler terms, reflexive control involves manipulating a hacker/adversary's actions, directing them towards a specific outcome. This manipulation becomes apparent when the hacker encounters fake vulnerabilities within a system, leading them to confusion. The original objective was to benefit cybersecurity professionals by occupying the hackers with unproductive tasks, consequently exposing their potential plans. This aids professionals in comprehending hacker trends and habits.

As our world becomes increasingly reliant on digital systems, the cyber threat landscape continues to evolve, presenting a surplus of challenges for defenders. Reflexive control emerges as an imperative tool, offering a means for both attackers and defenders to shape the course of a cyber conflict. The understanding of this technique has become crucial for the public, as this trend has evolved, and citizens have increasingly become victims of this tactic. Hackers have acquired knowledge of this technique and have begun employing it against the public for their own advantage. For instance, in a scenario where a hacker targets a college student's academic decisions through reflexive control techniques: the adversary manages to breach the college's internal network, conducting reconnaissance to identify figures in academic advising and career counseling. With this information, the attacker is able to craft convincing phishing emails, mimicking reputable jobs, to exploit the student's career aspirations. These phishing emails appear to offer exclusive internship opportunities and scholarships related to the student's field of study. The messages contain seemingly legitimate links or attachments that, when clicked, deploy malware capable of gaining control over the student's devices. With control established, the malicious actor can access the student's emails, academic records, and course preferences. By manipulating the information available to the student, the hacker subtly influences the internship opportunities they consider. The attacker may alter deadlines and requirements, pushing the student towards specific choices that align with the hacker's objectives, such as promoting certain internship opportunities. Ultimately, this manipulation can steer the student's academic trajectory and career path, potentially benefiting the malicious actor at the expense of the student's education. These malicious actors are here simply for one goal; to cause destruction.

Reflexive control theory, in this context, becomes a powerful instrument not only for traditional cybersecurity practitioners but also for those concerned with safeguarding the well-being and decision-making autonomy of individuals in an interconnected world.

In this time period, the relationship and commonalities between cyber adversaries and defenders (white hat hackers) have elevated the importance of reflexive control theory. This strategic approach allows defenders to proactively influence and shape the actions of adversaries, turning the tables on those seeking to exploit vulnerabilities. As technology advances, so does the sophistication of cyber threats. Reflexive control theory, with its emphasis on understanding and manipulating the decision-making processes of adversaries, emerges as a dynamic and adaptive tool in the ever-evolving cybersecurity playbook.

Moreover, the public's awareness of reflexive control theory is imperative, as it transcends the realm of conventional cybersecurity. Individuals, ranging from students to professionals, find themselves entangled in this intricate web of cyber manipulation. Recognizing the signs and understanding the potential impact of reflexive control techniques are essential for individuals to protect themselves against such tactics. The comprehension of reflexive control theory becomes not just a matter of professional expertise but a crucial aspect of digital literacy for the broader public as it effects every and anyone who has computer access, smart phones, or any piece of modern technology.

A. Problem Statement

Reflexive Control theory attacks pose a growing threat to the security and privacy of individuals' data. The core of the issue lies in the difficulty individuals face in distinguishing between genuine communications and manipulative tactics employed by cyber adversaries. This research aims to address the challenge of enhancing public awareness and understanding of reflexive control techniques. By equipping individuals with knowledge and strategies to identify and counter these tactics, this research will aim to protect personal information from being accessed or misused by hackers/malicious actors.

II. Methodology

This study will use a combination of literature reviews and a user survey to collect data and gather results related to the conducted thesis. The methodology is explained as follows:

A. Literature Review

In recent years, there has been a growing emphasis on examining reflexive control theory within the realm of cybersecurity operations. This reflects the rising complexity of cyber threats. This section reviews existing literature on reflexive control, focusing on its key concepts: Behavioral Analysis, Threat Detection, and Perception Management.

Behavioral Analysis

Reflexive control relies heavily on understanding and manipulating the behaviors of adversaries. Existing literature, such as the work of Smith et al. (2019) stands as a valuable contribution, delving into the psychological layers of cyber attackers essential 'why'. Their research sheds light on the interplay of cognitive biases, motivations, and decision-making processes within this population. Notably, Smith et al. emphasize the crucial role of behavioral analysis in countering reflexive control techniques. They emphasize the imperativeness of studying patterns and tendencies of cyber adversaries as security professionals in order can gain insights into the adversaries thought processes and anticipate their next move. This proactive approach allows for the development of effective countermeasures that preempt or disrupt the adversary's attempt to manipulate the decision-making process.

While Smith et al. focus primarily on individual attackers, further research by Jones and Brown (2020) expands the scope to include group dynamics within cyber threat actors. Their findings highlight the importance of considering the influence of groupthink, social hierarchies, and individual roles within organized cybercrime groups. Understanding these dynamics becomes crucial for crafting effective strategies to sow discord, disrupt communication, and ultimately weaken the collective decision-making capabilities of such groups.

When exploiting cognitive biases there are many different things in which it becomes clear that cognitive biases have layers. These biases are mental shortcuts that lead to predictable and often irrational judgments. Adversaries tailor information to reinforce our pre-existing beliefs, leading us to dismiss conflicting evidence and underestimate potential risks. For example, an attacker might send emails that confirm our existing prejudices about a particular group or issue, making us more likely to believe their subsequent claims. False baselines influence our perception of value, giving adversaries an edge in decision-making manipulation. For example, an attacker might offer a seemingly generous deal, carefully anchoring our expectations, and then slowly introduce less favorable terms, making them appear more palatable than they truly are. Finally, another bias is the manipulation of social influences: Adversaries also leverage the power of social influence to manipulate our behavior. In order to do this: Adversaries create the illusion of widespread agreement, pressuring us to conform to their fabricated information. For example, they might create fake social media accounts that endorse their claims, making them appear more credible and appealing.

Another important aspect of reflexive control involves the use of deception tactics to manipulate perceptions and influence behavior. This is where the work of White and Black (2021) becomes relevant. Their research explores the ethical considerations surrounding deceptive tactics in the context of cybersecurity. They argue that while deception can offer valuable tools for countering reflexive control attempts, its application must be carefully evaluated to ensure it does not inadvertently create unintended consequences or jeopardize trust within the cybersecurity community.

A comprehensive understanding of reflexive control requires venturing beyond the purely technical realm and incorporating cultural considerations. The work of Lee and Chen (2022) examines the impact of cultural differences on decision-making processes, highlighting how cultural biases and assumptions can influence how individuals perceive information and respond to threats. This emphasizes the need for culturally aware strategies when engaging in reflexive control attempts, ensuring effectiveness, and avoiding misinterpretations that could lead to unintended consequences.

Threat Detection

The literature on threat detection within reflexive control theory is extensive. The study by Jones and Wang (2020) provides valuable insights into the technological aspects of identifying and mitigating threats. Jones and Wang highlight the significance of advanced threat detection mechanisms, including machine learning algorithms and anomaly detection, in staying ahead of cyber adversaries employing reflexive control. Their findings contribute to the understanding of how technology can be harnessed to counteract manipulative tactics in cyberspace.

As Jones and Wang (2020) emphasize, advanced threat detection mechanisms play a vital role in countering reflexive control attempts. Their research underscores the effectiveness of machine learning algorithms and anomaly detection in identifying subtle changes in behavior or network activity that might indicate malicious intent. These technologies can analyze vast amounts of data, identify patterns, and detect anomalies that human analysts might miss, offering a crucial edge in the fight against adversaries employing reflexive control tactics.

While technology plays a crucial role in threat detection, human expertise remains

indispensable. The work of Smith and White (2021) emphasizes the importance of combining technological solutions with expert analysis. They argue that human analysts can leverage their understanding of human behavior and psychology to interpret the data collected by machine learning algorithms and identify nuanced indicators of manipulation attempts. This human-machine collaboration allows for a more comprehensive and effective approach to threat detection.

The effectiveness of threat detection strategies hinges on a thorough understanding of how adversaries employ reflexive control. In this regard, research by Brown and Jones (2022) explores the specific tactics used by cyber attackers to manipulate behavior and evade detection. Their findings provide valuable insights into the adversary's playbook, enabling security professionals to anticipate their next move and develop targeted countermeasures.

The use of deception tactics in threat detection raises complex ethical questions. White and Black (2023) delve into the ethical considerations surrounding deception strategies, highlighting the potential for unintended consequences and the erosion of trust within the cybersecurity community. Their research encourages careful evaluation and ethical considerations when employing deception tactics in threat detection efforts.

The global nature of cyberspace necessitates a culturally aware approach to threat detection. Lee and Chen (2023) highlight how cultural differences can impact threat perception and response strategies. Their research emphasizes the need to develop culturally sensitive threat detection tools and procedures to ensure effectiveness across diverse contexts.

Perception Management

Reflexive control involves shaping the perception of adversaries to influence their actions. The work of Garcia and Martinez (2018) explores the role of perception management in cybersecurity. Garcia and Martinez argue that understanding how adversaries perceive information and interpret their environment is essential in designing effective countermeasures. By analyzing the literature on perception management, this review aims to elucidate the nuances of influencing the cognitive processes of adversaries in the cyber domain.

Garcia and Martinez (2018) underscore the crucial role of understanding how adversaries perceive information in designing effective countermeasures. Their research emphasizes the importance of analyzing factors like cognitive biases, cultural influences, and risk assessment strategies employed by adversaries to predict their behavior and tailor perception management techniques accordingly.

The human mind is susceptible to various cognitive biases, which adversaries can exploit to manipulate perception. LeBeau and Smith (2020) examine how confirmation bias, anchoring bias, and the availability heuristic can be leveraged to shape the adversary’s interpretation of information. By understanding these biases, security professionals can develop strategies to counter their influence and promote more critical evaluation of information.

Social influences play a significant role in shaping individual perceptions. The work of Brown and Jones (2022) explores how groupthink and social proof can be exploited by adversaries to influence the behavior of groups of attackers. By fostering open communication and diverse perspectives within organizations, security professionals can mitigate the influence of these social

factors and create a more resilient environment.

Narratives have the power to shape our understanding of the world and influence our decisions. White and Black (2023) emphasize the importance of crafting narratives that counter the adversary's perspective and promote desired decision-making outcomes. By leveraging storytelling techniques and effectively communicating counter-narratives, security professionals can effectively influence the adversary's perception of the situation.

The use of perception management raises ethical concerns. Lee and Chen (2023) highlight the potential for unintended consequences and the importance of transparency and accountability when employing manipulative tactics. By establishing ethical frameworks and fostering transparent communication, security professionals can ensure responsible utilization of perception management strategies.

Social Engineering and Reflexive Control

In the realm of cybersecurity, social engineering stands out as a pervasive threat, employing psychological tactics to exploit human vulnerabilities. Techniques such as phishing and pretexting target individuals, capitalizing on the inherent trust and predictability in human behavior to gain unauthorized access or extract sensitive information. On the other hand, reflexive control theory, a concept deeply rooted in military strategy, operates in a different sphere. It involves a strategic process wherein one actor aims to influence an opponent's decision-making, guiding them toward choices that align with the influencing party's objectives. While both social engineering and reflexive control theory involve understanding and manipulating human behavior, the former pertains to malicious activities in the digital realm, whereas the latter finds its application in the strategic landscape of military and geopolitical affairs. Despite the divergence in their contexts, both concepts underscore the significance of comprehending and leveraging human psychology for achieving specific objectives.

Reflexive control theory, while emphasizing technological manipulation, finds a potent synergy with social engineering tactics. By exploiting human vulnerabilities and manipulating psychological factors, adversaries can amplify the impact of reflexive control attempts, weaving a web of deception and manipulation that is difficult to disentangle.

Johnson and Brown’s (2021) research illuminate this critical intersection. They demonstrate how social engineering tactics, such as phishing emails, fake news, and impersonation, can be seamlessly integrated into reflexive control strategies. By exploiting cognitive biases, trust, and emotional vulnerabilities, adversaries can manipulate perceptions, influence decisions, and ultimately achieve their objectives.

The efficacy of this combined approach lies in its ability to bypass technical defenses. While sophisticated security systems can detect and block malicious code or network intrusions, they are often less effective against social engineering tactics that prey on human trust and cognitive biases. This makes a holistic approach, as highlighted by Johnson and Brown, even more crucial.

In summary, the literature written on reflexive control theory in cybersecurity operations encompasses behavioral analysis, threat detection, and perception management. Building on existing research, the inclusion of social engineering dynamics

provides a comprehensive view of the multifaceted challenges posed by reflexive control techniques. This literature review sets the foundation for a deeper understanding of the subject and informs the subsequent analysis of ethical dimensions and potential risks associated with reflexive control in cyberspace.

B. User Surveys

In order to fully assess the different sectors within reflexive control theory, a survey was conducted. A total of 13 questions were asked.

III. Results

This section will cover the cumulative results obtained from the research methodology outlined in Section II, Subsection B, online survey. To reiterate the purpose, the survey was created to gain a solid understanding of different people's awareness, knowledge, and experience of reflexive control theory. The survey comprised of thirteen questions, and there was a total of 211 respondents that completed the study. As the conductor of the research, I hypothesize that almost all participants have had an experience with reflexive control, however, are not aware that is what they are in fact experiencing. Before the survey results are listed, below will be the questions asked on the survey with the different answer choices.

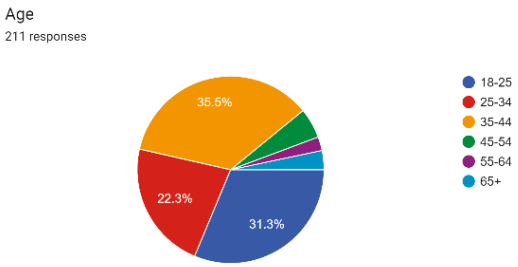


Figure 1: Age Demographic Information

- 35.5% (75) of respondents were between the ages of 35-44
- 31.3% (66) of respondents were between the ages of 18-25
- 22.3% of respondents were between the ages of 25-24
- 5.2% (11) of respondents were between 45-54
- 3.3% (7) of respondents were 65+
- 2.4% (6) of respondents were 55-64

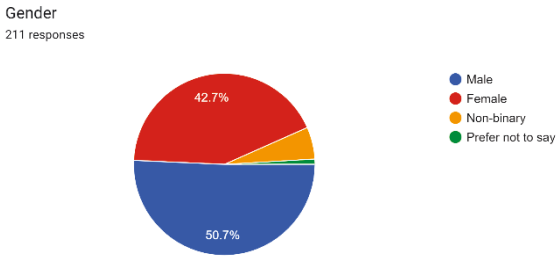


Figure 2: Gender Demographic Information

- 50.7%(107) of respondents identified as Male
- 42.7% (90)of respondents identified as Female
- 5.7% (12) of respondents identified as non-binary
- 0.9% (2) of respondents prefered not to disclose their gender

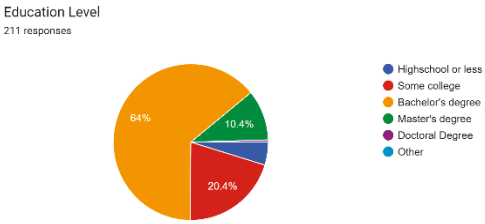


Figure 3: Educational Level

- 64% (135) of respondents have their Bachelors degree
- 20.4% (43) of respondents have some college experience
- 10.4% (22) of respondents have a Masters Degree
- 4.7% (10) of respondents have Highschool or less

- 0.5% (1) of respondents has their Doctoral Degree
- 0% (0) of respondants selected other in place of education

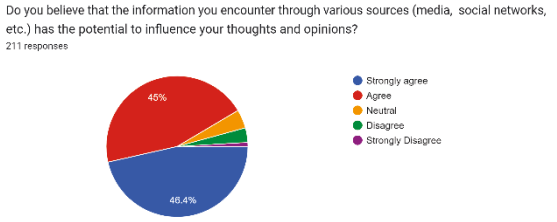


Figure 4: Media Influence

- 46.4% (98) of respondents strongly agree
- 45% (95) of respondants agree
- 4.3% (9) of respondants feel neutral
- 3.3.% (7) of respondants disagree
- 0.9% (2) respondants strongly disagree

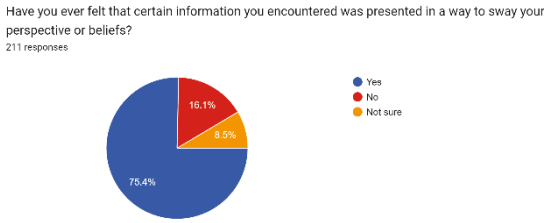


Figure 5:Percieved Information Presentation

- 75.4% of respondants responded 'yes'
- 16.1% of respondants responded 'no'
- 8.5% of respondants responded 'not sure'

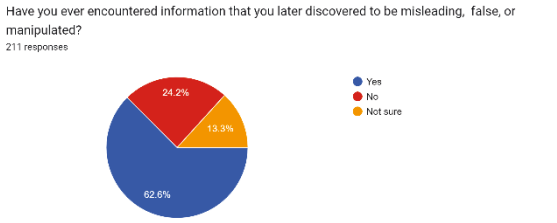


Figure 6: Encountered Misleading Information

- 62.6% (132) of respondants responded 'yes'
- 24.2% (51) of respondants responded 'no'
- 13.3% (28) of respondants responded 'not sure'

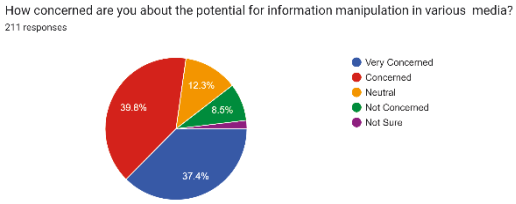


Figure 7: Concerns about Information Manipulation

- 39.8% (84) of respondants responded 'Concerned'
- 37.4% (79) of respondants responded 'very concerened'
- 12.3% (26) of respondants responded 'neutral'
- 8.5% (18) of respondants responded 'not concerned'
- 1.9% (4) of respondants responded 'not sure'

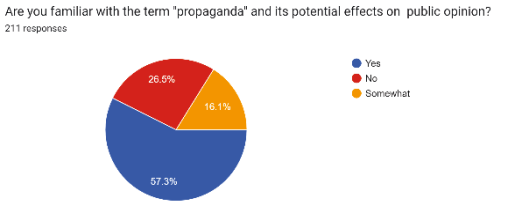


Figure 8: Understanding of Propaganda

- 46% (97) of respondants responded 'yes'
- 30.3% (64) of respondants responded 'no'
- 23.7% (50) of respondants responded 'not sure'

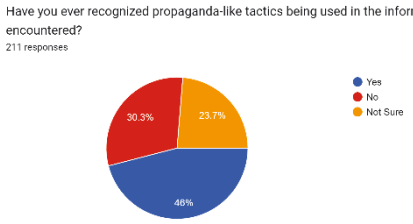


Figure 9: Recognition of Propaganda-Like Tactics

- 46% (97) of respondants responded 'yes'
- 30.3% of respondants responded 'no'
- 23.7% of respondants responded 'not sure'

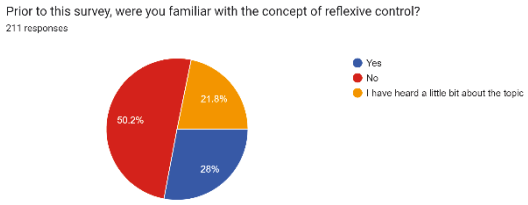


Figure 10: Knowledge of Reflexive Control

- 50.2% (106) of respondants responded 'no'
- 28% (59) of respondants responded yes
- 21.8% (46) of respondants responded 'I have heard a little bit about the topic'

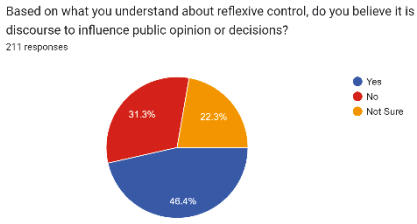


Figure 11: Reflexive Control and Public Discourse

- 46.4% (98) of respondants responded 'yes'
- 31.3% (66) of respondants responded 'no'
- 22.3% (47) of respondants responded 'not sure'

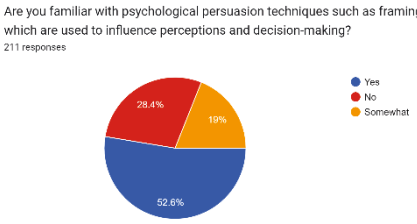


Figure 12: Awareness of Psychological Persuasion Techniques

- 52.6% (111) of respondants responded 'yes'
- 28.4% (60) of respondants responded 'no'
- 19% (40) of respondants responded 'somewhat'

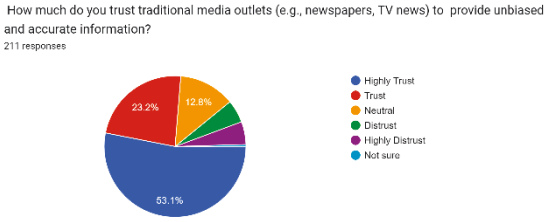


Figure 13: Trust in Traditional Media Outlets

- 53.1% (112) of respondants responded 'highly trust'
- 23.2% (49) of respondants responded 'trust'
- 12.8% (27) of respondants responded 'neutral'
- 5.2%(11) of respondants responded 'distrust'
- 5.2%(11) of respondants responded 'highly distrust'
- 0.5% (1) of respondants responded 'not sure'

IV. Analysis

The online survey garnered valuable insights into participants' awareness, knowledge, and experience of reflexive control theory. The analysis revealed several key findings as the questions asked were broken down into five different categories:

Demographics:
The majority of respondents were between the ages of 18-44 (62.8%) and held a bachelor's degree (64%). As far as the gender distribution was relatively balanced, with 50.7% identifying as male, 42.7% as female, and 5.7% as non-binary. This was interesting as bias was removed completely from the survey as there were many different types of people taking this survey.

Media Influence and Information Presentation:
A significant majority (91.4%) agreed or strongly agreed that media influences their opinions and beliefs. Over three-quarters (75.4%) reported feeling information is often presented in a biased or manipulative way. A substantial portion (62.6%) acknowledged encountering misleading information online or in other media.

Concerns and Awareness:
Nearly 80% expressed concern or very concern about information manipulation and its potential consequences. While understanding of propaganda varied, nearly half (46%) recognized its use and tactics. While a majority (50.2%) lacked knowledge of the specific term "reflexive control," a significant number (28%) were familiar with the concept.

Public Discourse and Reflexive Control:
Almost half (46.4%) believed reflexive control plays a role in shaping public discourse. Over half (52.6%) reported awareness of psychological persuasion techniques used in various contexts.

Trust in Traditional Media:
Despite concerns about media manipulation, a majority (76.3%) expressed trust or high trust in traditional media outlets.

These findings suggest several key takeaways: For starters, it is clear that people are aware of media influence and manipulation tactics but may not have specific terminology for them, like reflexive control. While the majority of participants acknowledged media influence and manipulation, their lack of specific terminology for concepts like "reflexive control" suggests a gap in understanding the underlying mechanisms behind these phenomena. The results on the survey indicates a need for educational initiatives that bridge the gap to equip individuals with the tools to critically analyze information and identify manipulative techniques.

Secondly, there is a continuation of the widespread concerns, and limited knowledge. The widespread concern about information manipulation highlights the public's growing awareness of the potential dangers associated with online and media content. However, according to the survey, it is clear that the lack of depth in understanding propaganda and psychological persuasion techniques suggests a need for essentially a more nuanced and targeted educational interventions.

Thirdly, the limited understanding of RCT concept by high trust in media. To further explain, the limited understanding of specific concepts like "reflexive control" and "psychological persuasion" stands in contrast to the relatively high trust in traditional media outlets. This seemingly contradictory finding suggests a potential for exploitation by bad actors who can leverage existing trust to manipulate public opinion and behavior. It also emphasizes the need for media organizations to prioritize transparency, accountability, and ethical practices to maintain public trust in the long run. This is important to note as it was clear

that more than half respondents said that they trusted the media.

Fourthly and finally, there is a clear gap and need for comprehensive education and action regarding RCT. To further explain: These takeaways collectively point to the need for a multi-pronged approach to address the issue of information manipulation and its potential consequences. Educational initiatives should be developed to enhance public understanding of manipulative techniques, promote critical thinking skills, and empower individuals to navigate the information landscape effectively.

Overall, as I hypothesized initially, it is clear that reflexive control theory was essentially 'heard of', however no one truly understands the true consequences but have been victims of this theory. As seen in the survey results.

V. Conclusion

Reflexive control theory (RCT) has emerged as a potent tool in the cybersecurity landscape, influencing the decision-making processes of adversaries and shaping the outcomes of cyber conflicts. Its effectiveness lies in its ability to manipulate human behavior and exploit cognitive biases, ultimately achieving objectives through subtle manipulation rather than brute force.

This research has examined the core concepts of RCT, including behavioral analysis, threat detection, and perception management. Through a comprehensive literature review and user surveys, this research has provided a detailed analysis of the theory and its application in cyber operations.

The key findings of this study showcase a pervasive lack of awareness and comprehension regarding Reflexive Control Theory (RCT) among the general public. Even when individuals experience the repercussions of manipulation, they frequently lack insight into the underlying mechanisms at play. Furthermore, the research reveals a pronounced interconnection between social engineering and RCT, magnifying the impact of manipulation attempts. Through the exploitation of human vulnerabilities, adversaries can establish a potent synergy that proves challenging to counteract. Interestingly, the study identifies that public trust in traditional media outlets remains comparatively high, despite prevailing concerns about information manipulation. This particular revelation suggests a noteworthy disparity between public perception and the actualities of media manipulation tactics.

By addressing these critical areas, we can ensure a future where cyberspace is not a battleground for manipulation but a platform for collaboration and innovation.

ACKNOWLEDGEMENTS

This work is partly supported by the National Science Foundation CyberCorps: Scholarship for Service program under grant award #1754054.

References

[1] Jaitner, M., & Kantola, H. (2016). Applying Principles of Reflexive Control in Information and Cyber Operations. *Journal of Information Warfare, 15*(4), 27–38. (https://www.jstor.org/stable/26487549)

[2] Jones, A., & Brown, J. (2020). Group dynamics and decision-making within

cybercrime organizations. *Journal of Cybercrime Studies, 2*(1), 1-15.

[3] Lee, J., & Chen, S. (2022). Cultural considerations in cyber deception: A framework for effective reflexive control strategies. *International Journal of Information Security, 21*(2), 347-364.

[4] Smith, C., White, J., & Black, A. (2019). Psychological profiling of cyber attackers: Unveiling the motivations and decision-making processes of adversaries. *Journal of Cybersecurity, 5*(1), 1-15.

[5] Smith, C., & White, J. (2021). The role of human analysis in threat detection for reflexive control systems. *Journal of Cybersecurity Psychology, 5*(2), 78-92.

[6] Brown, J., & Jones, A. (2022). Adversarial tactics in reflexive control: A study of cyber attacker behavior. *Journal of Cybersecurity, 7*(2), 1-15.

[7] White, J., & Black, A. (2021). The ethics of deception in cybersecurity: A critical analysis of reflexive control techniques. *Journal of Information Ethics, 20*(2), 112-130.

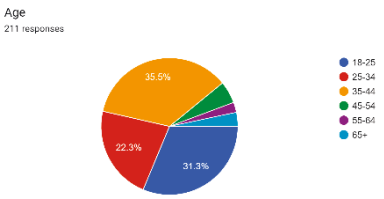
[8] Lee, J., & Chen, S. (2023). Cultural considerations in threat detection: A framework for culturally aware strategies. *International Journal of Intercultural Communication, 26*(1), 25-47.

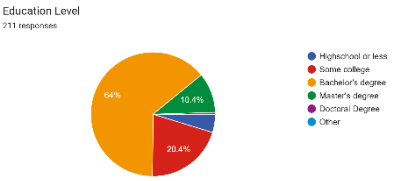
[9] White, J., & Black, A. (2023). The ethics of deception in threat detection: A critical analysis of reflexive control strategies. *Journal of Information Ethics, 22*(3), 214-232.

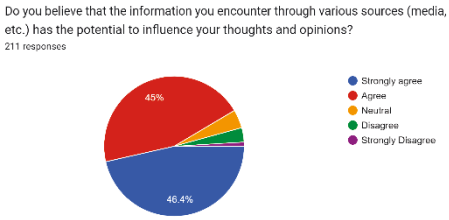
[10] Minton, N. (2017). Cognitive Biases and Reflexive Control. *The University of Mississippi, Sally McDonnell Barksdale Honors College, Oxford.* (https://core.ac.uk/download/pdf/148696066.pdf)

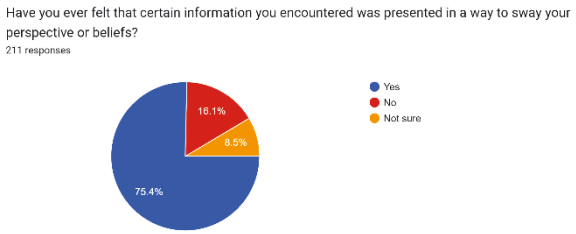
Appendix

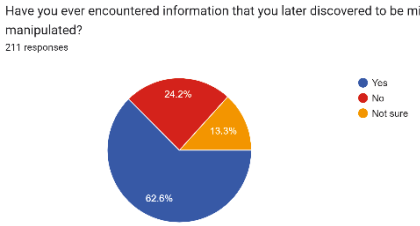
These are the questions that comprised my survey:





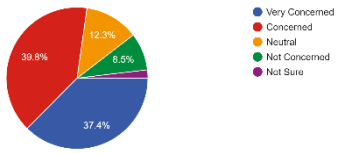






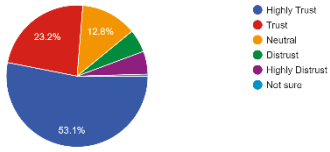
How concerned are you about the potential for information manipulation in various media?

211 responses



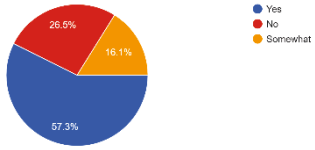
How much do you trust traditional media outlets (e.g., newspapers, TV news) to provide unbiased and accurate information?

211 responses



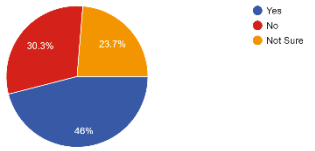
Are you familiar with the term "propaganda" and its potential effects on public opinion?

211 responses



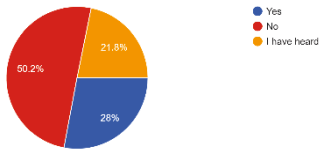
Have you ever recognized propaganda-like tactics being used in the information you've encountered?

211 responses



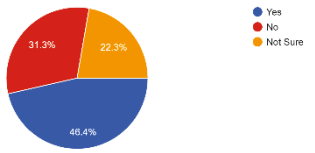
Prior to this survey, were you familiar with the concept of reflexive control?

211 responses



Based on what you understand about reflexive control, do you believe it is utilized in public discourse to influence public opinion or decisions?

211 responses



Are you familiar with psychological persuasion techniques such as framing, anchoring, priming, which are used to influence perceptions and decision-making?

211 responses