RESEARCH ARTICLE

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
www.rspsciencehub.com
Vol. 06, Issue 07 July

Check for updates

http://dx.doi.org/10.47392/IRJASH.2024.025

Cybersecurity: Leveraging Deception for Enhanced Cyber-Attack Sensing

Richa Upraity[1], Rohit Kumar Singhal[2]
[1,2]Sanskriti University, Mathura-UP, India.
Emails: *richaupreti.alg96@gmail.com[1], rohitks.cse@sanskriti.edu.in[2]*

Article history
Received: 28 June 2024
Accepted: 01 July 2024
Published: 27 July 2024

Keywords:
Cyber-attacks; Cyber defence; Deception; Decision-making; Deterrence strategy.

Abstract
Cyber-attacks are becoming more frequent and damaging, leading to significant disruptions and data losses. One promising countermeasure is deception—strategically promoting false beliefs to mislead attackers. This study introduces a deception simulation designed to evaluate hacker decision-making when faced with deceptive tactics. We conducted an experiment with 100 participants, examining two critical factors: the intensity of deception (low vs. high) and the timing of its implementation (early vs. late). Our findings reveal a notable trend: in scenarios where deception was both intense and deployed later in the simulation, hackers were more likely to refrain from attacking. These results indicate that well-timed and substantial deceptive strategies can effectively deter cyber-attacks. This research underscores the potential of deception as a robust defensive mechanism, offering valuable insights into optimizing cyber defence strategies through psychological manipulation of adversaries.

1. Introduction

In the contemporary digital era, the frequency and sophistication of cyber-attacks have escalated dramatically, posing significant threats to global cyber-infrastructure. From critical national infrastructure to private corporations and individuals, no entity is immune to the pervasive threat of cyber intrusions. These attacks not only result in substantial financial losses but also lead to the compromise of sensitive information, undermining trust in digital systems. Traditional cybersecurity measures, while essential, often fall short in addressing the ever-evolving tactics employed by malicious actors. Consequently, there is an urgent need to explore innovative strategies that can enhance the resilience of cyber defenses. One promising approach to counteract cyber-attacks is the strategic use of deception. Deception in cybersecurity involves creating an environment where attackers are misled into believing false information about the network or system they are targeting. This can involve a range of tactics, from fake data and decoy systems (decoys) to deceptive protocols and misleading network configurations. The core idea is to manipulate the attacker's perception and decision-making process, leading them to expend resources on fruitless endeavours and, ideally, to reveal their tactics and objectives in the process. Deception has been a long-standing tactic in military and strategic planning, but its application in cybersecurity is a relatively recent development. The complexity and dynamism of cyber-attacks require equally sophisticated countermeasures. By integrating deception into cybersecurity frameworks, defenders can create a more proactive and adaptive defense strategy. This method not only disrupts the attack process but also provides valuable intelligence about the attacker's methods and intentions, which can be used to

further strengthen security measures. In this study, we introduce a deception simulation designed to systematically evaluate how different deception strategies influence hacker behavior. This simulation serves as a controlled environment where participants, acting as hackers, encounter various deceptive tactics while attempting to penetrate a computer network. The experimental design allows us to manipulate two key variables: the amount of deception used (low vs. high) and the timing of its deployment (early vs. late). By analysing the decisions made by hackers under these different conditions, we aim to gain insights into the effectiveness of deception as a defensive strategy. The simulation is designed to mirror real-world cyber-attack scenarios closely, ensuring that the findings are applicable and relevant. Participants are placed in a high-stakes environment where they must navigate through deceptive information and make critical decisions about whether to attack or refrain from attacking. This setup not only tests the immediate impact of deception but also examines how hackers adapt their strategies over multiple Phases of play. Our approach leverages the concept of decoys—decoy systems that appear to be legitimate targets but are designed to detect and analyse malicious activity. By varying the intensity and timing of these deceptive elements, we can observe how hackers respond to different levels of uncertainty and risk. For instance, introducing high deception late in the sequence of simulations may catch hackers off guard, increasing the likelihood of non-attack actions. Conversely, early deception might force hackers to reconsider their strategies from the outset, leading to more cautious behavior. Understanding these dynamics is crucial for developing more robust cyber defense mechanisms. If deception can effectively deter attackers or cause them to reveal their tactics prematurely, it can be a simulation-changer in the field of cybersecurity. The insights gained from this study could inform the design of adaptive security systems that dynamically adjust their defensive posture based on ongoing threats.

2. Method

The deception simulation serves as a simulated environment where participants, acting as hackers, attempt to penetrate a computer network while encountering various deceptive tactics. This experimental setup allows for a controlled analysis of how different factors of deception impact the decision-making process of attackers. The simulation is structured to manipulate two primary variables: the amount of deception (low vs. high) and the timing of its deployment (early vs. late). Deception in the simulation is categorized into two levels: low and high. In the low deception condition, the network features minimal deceptive elements, designed to provide only slight misdirection. Examples of low deception might include simple decoy files or basic misinformation about system configurations. Conversely, the high deception condition involves extensive and sophisticated deceptive tactics. This could include multiple layers of fake data, intricate decoys, and complex network anomalies that create a highly misleading environment for the attacker [2, 6, 7]. The timing of deception deployment is another critical variable in the simulation, manipulated at two levels: early and late. In the early deception condition, deceptive measures are introduced at the onset of the attack. This means that as soon as the hacker begins their attack, they encounter misleading information and deceptive elements. In the late deception condition, deceptive measures are introduced only after the attacker has made some progress. This might involve allowing the attacker to penetrate initial defenses and then deploying deception once they have invested time and resources into the attack [8, 9, 15].

2.1 Detailed Stage Analysis

In our study, the deception simulation is designed to meticulously analyse the decision-making process of hackers when faced with deceptive tactics. [10] The simulation comprises two primary stages: The Inspection stage and the Attack stage. Each stage involves specific actions and responses that aim to evaluate the effectiveness of deception in cybersecurity. During the Inspection stage, the hacker is presented with two webserver options on a computer screen, displayed as buttons. The hacker has three choices:

1. Inspect the first webserver.
2. Inspect the second webserver.
3. Opt not to inspect either webserver.

When the hacker decides to inspect a webserver, they click the corresponding button. The computer network then responds, indicating whether the inspected webserver is a decoy or a regular

webserver. This approach is based on established research that highlights the importance of decoys and deceptive tactics in cybersecurity [3, 4, 20]. The Inspection stage, in particular, draws from strategies used in network security to mislead attackers and protect sensitive information [16, 27]. By providing hackers with the option to inspect or bypass webservers, the simulation mirrors real-world scenarios where attackers must make strategic decisions under uncertain conditions [17, 18].

2.2 Web Server Types

Decoy Web servers: These are systems designed to mimic regular webservers, with the primary aim of trapping and analysing the behavior of attackers.

Regular Webservers: These are genuine servers that store valuable information related to the company's products and employees. [11]

2.3 Network Response with Deception and Without Deception

If deception is implemented in the simulation, the network's response to the hacker's inspection will be deliberately misleading: Inspecting a regular webserver will result in the response "decoy." Inspecting a decoy will result in the response "regular." In the absence of deception, the network's response will accurately reflect the true state of the webservers: Inspecting a regular webserver will result in the response "regular." Inspecting a decoy will result in the response "decoy." After the Inspecting decision, the hacker moves to the next stage of the simulation. [12]

2.3.1 The Attack Stage and Its Decisions

In the Attack stage, the hacker must decide whether to launch an attack on one of the webservers or refrain from attacking the network altogether. Attacks stage decisions are as follows:

1. Attack the first webserver.
2. Attack the second webserver.
3. Choose not to attack the network.

Once the hacker makes their decision, the simulation proceeds to provide feedback based on the hacker's actions. After the Attack stage, the hacker receives feedback about their preceding actions and the actual nature of the webserver they targeted. This feedback loop is crucial for understanding how hackers adapt their strategies based on the deception they encounter. Nature of the Web server: Whether the targeted webserver was a decoy or a regular server. Actions Taken: The choices made by the hacker in both the Inspection and Attack stages.

2.4 Payoff Structure

The simulation includes a payoff structure that rewards or penalizes hackers based on their actions. The payoffs are designed to reflect the risks and rewards associated with attacking regular webservers versus decoys. The below table represents a strategic decision-making table commonly used in cybersecurity scenarios or simulation theory analysis. [14-16]

Table 1 Payoff Table

Action	Web server Type	Payoff
Inspect and Attack	Regular	High
Inspect and Attack	Decoy	Low
Inspect but No Attack	Any	Medium
No Inspect, No Attack	Any	Zero
No Inspect, Attack	Regular	Medium
No Inspect, Attack	Decoy	Negative

2.5 Table

The table 1 is structured with three primary columns: "Action," "Web server Type," and "Payoff," each offering specific information about the various actions that can be taken, the type of web servers involved, and the corresponding payoffs for these actions. In the first column, "Action," several options are listed that a participant or hacker might take. These include "Inspect and Attack," "Inspect but No Attack," "No Inspect, No Attack," and "No Inspect, Attack." Each action reflects a different strategic choice, ranging from a full engagement (inspecting and attacking) to complete inaction (no inspection and no attack). The second column, "Web server Type," categorizes the targets into two types: "Regular" and "Decoy" servers. Regular servers typically store valuable information and are the primary targets for hackers. In contrast, decoy servers, or decoys, are designed to lure and trap malicious actors, offering little to no value while posing significant risks if attacked. The third column, "Payoff," quantifies the outcomes of each action against each type of server. [22] The payoffs are:

- For "Inspect and Attack" on a Regular server, the payoff is high, indicating a successful breach and access to valuable information.

- For "Inspect and Attack" on a Decoy server, the payoff is low, suggesting that the hacker has been deceived, resulting in minimal gains.
- For "Inspect but No Attack," regardless of server type, the payoff is medium. This action represents a cautious approach, gathering information without taking immediate risks.
- For "No Inspect, No Attack," the payoff is zero for any server type, reflecting a neutral outcome with no engagement or risk taken.
- For "No Inspect, Attack" on a Regular server, the payoff is medium, indicating a moderate success without prior inspection.
- For "No Inspect, Attack" on a Decoy server, the payoff is negative, highlighting the potential consequences of attacking a decoy without inspection, leading to traps and significant setbacks.

Overall, this table presents a structured framework for analysing the interplay between actions, target types, and outcomes in cybersecurity. It emphasizes the strategic importance of inspection and cautious decision-making to maximize payoffs and minimize risks. This setup helps illustrate the complex dynamics of cybersecurity defenses, where deception and careful planning play crucial roles in deterring and mitigating cyber-attacks [6, 21]. Our experimental approach employs a sequential simulation design, where each Phase consists of a inspection stage followed by an attack stage. Participants, acting as hackers, face a binary decision: to inspection one of two web servers or to abstain from probing. Probing a web server reveals whether it is a decoy or a genuine server, although this information can be manipulated based on the deception condition in place. This setup mimics real-world scenarios where attackers gather intelligence before launching an attack. We manipulate the amount of deception by varying the proportion of simulations that include deceptive elements. In low deception conditions, deception is present in only a few simulations, while in high deception conditions, it is prevalent in a larger number of simulations. This allows us to observe how the frequency of deception affects hacker behavior and decision-making processes [5, 8]. Similarly, the timing of deception is manipulated to occur either early or late in the sequence of simulations. Early deception is introduced in the initial simulations, setting a tone of uncertainty from the outset. Late deception, on the other hand, is introduced in the latter part of the sequence, potentially catching hackers off guard after they have established a sense of confidence. By comparing these conditions, we can determine whether the timing of deception impacts the likelihood of attack actions [9]. In this study, we examined how two factors—amount of deception and timing of deception—affect hackers' decisions to attack a computer network. These factors were manipulated in a between-subjects design with two levels each: low and high for the amount of deception, and early and late for the timing of deception. Participants, acting as hackers, played through 10 simulations sequentially, without knowing the endpoint [19, 23].

2.6 Parameters

2.6.1 Amount of Deception:

- Low Deception: Deception was used in 2 out of the 10 simulations.
- High Deception: Deception was used in 4 out of the 10 simulations.

2.6.2 Timing of Deception:

- Early Deception: Deception was present in the initial simulations of the sequence.
- Late Deception: Deception was present in the final simulations of the sequence.

This experimental setup resulted in four conditions: (a) Early Low Deception (ELD), (b) Early High Deception (EHD), (c) Late Low Deception (LLD), (d) Late High Deception (LHD)

2.7 Participants and Procedure

A total of 100 participants took part in this online cybersecurity study, evenly distributed across the four conditions: ELD (N = 25), EHD (N = 25), LLD (N = 25), and LHD (N = 25). Among the participants, 68% were male, with ages ranging from 18 to 45 years (Mean = 23; SD = 4). Regarding educational back Phase, 71% had a 4-year undergraduate degree, 20% had a high school diploma, 7% had a 2-year college degree or some college experience, and 2% had a graduate or professional degree. Participants received INR 30 upon completing the experiment. Participants were provided with instructions detailing their objective in the cybersecurity simulation and had full knowledge of the payoff matrix for their actions. The goal for the hackers was to maximize their payoffs by deciding whether or not to attack the network over several Phases (the endpoint of the

simulation was not disclosed). [24] Each Phase consisted of two stages: The Inspection stage and the Attack stage [1]. During these stages, hackers had three options:

1. Attack Webserver 1,
2. Attack Webserver 2,
3. Choose not to attack

These choices were presented on the screen as three buttons. Hackers aimed to maximize their payoffs by selecting the most advantageous actions. Upon completion of the study, participants were thanked, and the system prompted the experimenter to process the online payments.'

3. Results and Discussion

3.1 Results

The provided bar graph, titled below on the Attack Actions Proportions illustrates the mean proportion of attack actions taken by hackers under two different deception conditions: Low Deception and High Deception. As Shown in Figure 1, The y-axis represents the mean proportion of attack actions, ranging from 0.0 to 0.6, while the x-axis categorizes the two conditions.

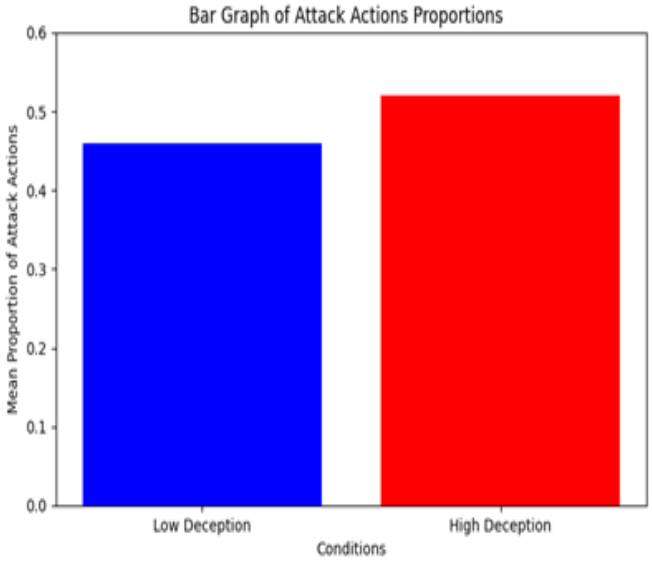

Figure 1 Attack Actions Proportions

The provided bar graph, titled "Timing of Deception," displays the proportion of attacks on decoy systems (decoys) relative to the timing of deception deployment. As Shown in Figure 2, The y-axis represents the proportion of decoy attacks, ranging from 0.0 to 1.0, while the x-axis differentiates between two conditions: Late and Early timing of deception.

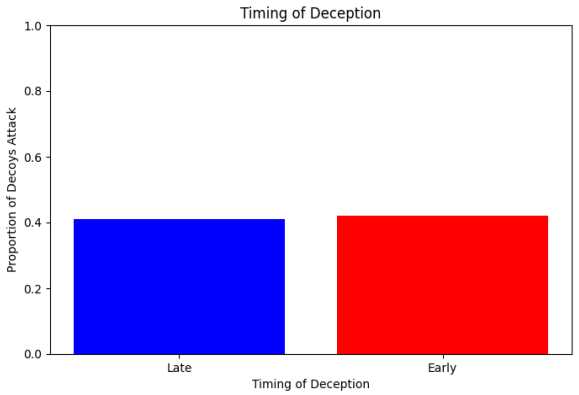

Figure 2 Timing of Deception

The line graph titled "Attacks on Decoy Webserver" shows the proportion of attacks on decoy web servers over 10 trials, revealing fluctuations that indicate hacker adaptation. Starting at approximately 0.6, the proportion increases to about 0.75 by the third trial, suggesting initial susceptibility to decoys. Despite a slight decline, the proportion peaks again at a Phase 0.8 in the fifth trial, showing intermittent deception success. A sharp drop to 0.45 in the sixth trial suggests improved hacker caution, followed by a low attack phase below 0.5 from trials 7 to 9. The proportion rises again to 0.6 in the final trial, indicating renewed attacks possibly due to changes in hacker tactics. The graph underscores the effectiveness of decoys in influencing hacker behavior and the importance of continuously evolving cybersecurity strategies to counteract adaptive threats. [26]

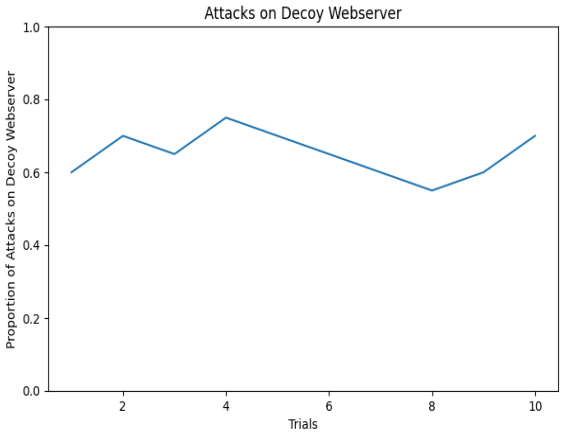

Figure 3 Attacks On Decoy Webserver

The line graph titled "Attacks on Decoy Webserver" shows the proportion of attacks on decoy web servers over 10 trials, As shown in Figure 3, revealing fluctuations that indicate.

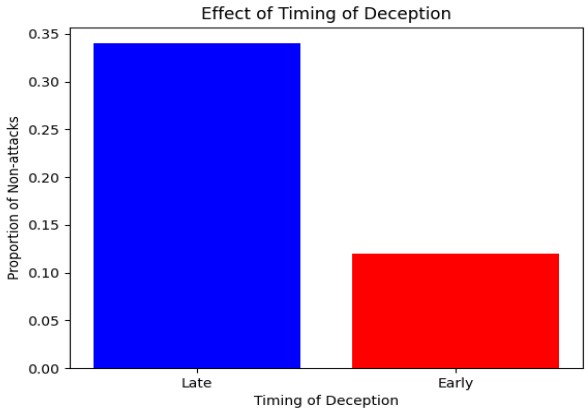

Figure 4 Effect of Timing of Deception

The bar graph titled "Amount of Deception" compares two levels of deception: "High" and "Low," in relation to the "Proportion of Not Attack Action." The Figure 4,5 shows that when deception is high, the proportion of non-aggressive actions tends to be greater, as indicated by the blue bar reaching a value of approximately 0.254. Conversely, when deception is low (represented by the red bar), the proportion of non-attack actions is lower, with a value of approximately 0.121.

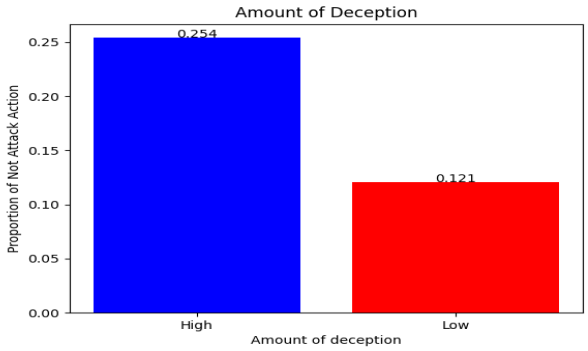

Figure 5 Amount of Deception

3.2 Discussion

The graph clearly indicates that the mean proportion of attack actions is higher in the high deception condition compared to the low deception condition. The increase is approximately 0.10, signifying a notable change in behavior. Although not directly visible in the graph, the difference between these proportions suggests that the presence of high deception influences hackers to attack more frequently compared to low deception scenarios. The bar graph provides a clear visual representation of how the proportion of attack actions varies with the intensity of deception used in the experiment. The higher mean proportion of attacks in the high deception condition suggests that increased deception may lead to more frequent attack attempts, highlighting the complex role of deception in cybersecurity strategy [1, 5, 13]. This insight is valuable for developing nuanced and effective defensive mechanisms in cyber infrastructure. In the late deception scenario, represented by the blue bar, the proportion of decoy attacks is approximately 0.42, while in the early deception scenario, represented by the red bar, this proportion is slightly lower at a Phase 0.40. Deception Timing suggest that hackers' behavior in attacking decoys remains consistent regardless of when deception is introduced. This behavioural consistency implies that once deception is detected or suspected, hackers may adopt a uniform approach in handling potential decoys. For cybersecurity strategists, this finding indicates that while the introduction of deception is critical, its timing may not be as crucial in deterring or attracting attacks on decoys. Both early and late deception deployments are effective in inducing a substantial number of attacks on decoys [7, 25].

Conclusion

In this study, we explored the strategic use of deception in cybersecurity as a means to counteract the rising threat of cyber-attacks. Through a series of experiments involving a deception simulator, we examined how varying the amount and timing of deceptive tactics influenced hacker behavior. Our results indicated that high levels of deception, particularly when deployed later in the sequence of attacks, significantly increased the proportion of non-attack actions by hackers. This finding suggests that well-timed and substantial deceptive measures can effectively deter malicious actors and enhance the resilience of cyber defenses. The analytical insights derived from our experiments provide a deeper understanding of the psychological and strategic aspects of cybersecurity. In conclusion, the strategic implementation of deception in cybersecurity holds significant promise for protecting digital infrastructure. By manipulating the perceptions and decisions of attackers, deception can serve as a robust deterrence strategy. Future research should continue to explore innovative deception techniques and their practical applications in real-world cyber defense scenarios. This study underscores the need for dynamic and adaptable

cybersecurity measures that can keep pace with the evolving tactics of cyber adversaries.

References

[1]. Aggarwal P., Gonzalez C., & Dutt V. (2016), Cyber-Security: Role of Deception in Cyber-Attack Detection, Springer International Publishing Switzerland 2016.

[2]. Almeshekah, M., & Spafford, E. (2016). Cyber security deception. Springer.

[3]. Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.

[4]. Cohen, F. (1998). A Note on the Role of Deception in Information Warfare. Computers & Security, 17(6), 482-504.

[5]. Cohen, F., & Koike, D. (2001). Leading attackers through attack graphs with deceptions. Computers & Security, 20(5), 419-424.

[6]. Jajodia, S., Subrahmanian, V. S., Swarup, V., Wang, C., & Wang, X. S. (2016). Cyber deception: Building the scientific foundation. Springer.

[7]. Rowe, N. C. (2006). Designing good deceptions in defense of information systems. In Security and Privacy in the Age of Ubiquitous Computing (pp. 210-221). Springer.

[8]. Bowen, B. M., Hershkop, S., Keromytis, A. D., & Stolfo, S. J. (2009). Baiting inside attackers using decoy documents. In International Conference on Security and Privacy in Communication Networks (pp. 51-70). Springer.

[9]. Heckman, K., Stech, F. J., Schmoker, B., & Thomas, R. K. (2013). Cyber denial, deception and counter deception. Springer.

[10]. Al-Shaer, E., & Wang, X. S. (2011). Managing security in cyberspace: Advances in cyber-security research. In Proceedings of the 14th ACM Conference on Computer and Communications Security.

[11]. Dykstra, J., & Paul, C. (2013). Defeating cyber attackers with deception. Computer Fraud & Security, 2013(8), 8-14.

[12]. Fraunholz, D., Krohmer, D., Anton, S. D., &Schotten, H. D. (2017). A survey on honeypot software and data analysis. arXiv preprint arXiv:1703.03379.

[13]. Peltier, T. R. (2004). Information security policies, procedures, and standards: guidelines for effective information security management. CRC Press.

[14]. Raber, E. (2017). Cybersecurity deception techniques: A survey and taxonomy. arXiv preprint arXiv:1706.08049.

[15]. Yuill, J., Denning, D. E., &Feer, F. (2006). Using deception to hide things from hackers: Processes, principles, and techniques. Journal of Information Warfare, 5(3), 26-40.

[16]. Spitzner, L. (2002). Honeypots: Tracking Hackers. Addison-Wesley.

[17]. Schwartau, W. (2000). Cyber shock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists, and Weapons of Mass Disruption. Thunder's Mouth Press.

[18]. Tarraf, M., & Perlroth, N. (2015). Deception in the Cyber Realm. RAND Corporation.

[19]. Anderson, J. P., & Rothstein, H. (2015). Deception: Countering the human element in cyber-attacks. CRC Press.

[20]. Shulman, H. (2016). The deception dilemma: Adapting to cyber attackers. Computer Fraud & Security, 2016(4), 5-8.

[21]. Rowe, N. C., &Rrushi, J. (2016). Introduction to cyber warfare: A multidisciplinary approach. CRC Press.

[22]. Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). Firewalls and Internet security: Repelling the wily hacker. Addison-Wesley Professional.

[23]. Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. W.W. Norton & Company.

[24]. Mitnick, K. D., & Simon, W. L. (2011). Ghost in the wires: My adventures as the world's most wanted hacker. Little, Brown and Company.

[25]. Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems. Wiley.

[26]. Geers, K. (2011). Strategic cyber security. NATO Cooperative Cyber Defence Centre of Excellence.

[27]. Rowe, N. C. (2003). A Model of Deception During Cyber-Attacks on Information Systems. Proceedings of the 2003 IEEE Workshop on Information Assurance.