NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE FIFTH MASQUERADE: AN INTEGRATION EXPERIMENT OF MILITARY DECEPTION THEORY AND THE EMERGENT CYBER DOMAIN

by

Justin J. Green

September 2020

Thesis Advisor:	Neil C. Rowe
Second Reader:	Kalev I. Sepp

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
THE FIFTH MASQUERADE: AN INTEGRATION EXPERIMENT OF MILITARY DECEPTION THEORY AND THE EMERGENT CYBER DOMAIN

5. FUNDING NUMBERS

6. AUTHOR(S) Justin J. Green

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Marine Forces Cyberspace Command, Fort Meade, Maryland 20755

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

For centuries, militaries throughout the world have used deception techniques to gain competitive advantage in warfare. This thesis evaluated the effect of deception with a particular commercial product within cyberspace. It measured the effect of its deception on the ability of attackers to achieve their objectives. The results of our experiments showed the deception could slow cyber-attacks. These results also suggested several future research opportunities and implementation strategies for deception in cyberspace operations.

14. SUBJECT TERMS
military deception, cyberspace operations, cyberspace deception

15. NUMBER OF PAGES
59

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

THE FIFTH MASQUERADE: AN INTEGRATION EXPERIMENT OF MILITARY DECEPTION THEORY AND THE EMERGENT CYBER DOMAIN

Justin J. Green
Gunnery Sergeant, United States Marine Corps
BS, University of Maryland University College, 2019

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN APPLIED CYBER OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
September 2020

Approved by: Neil C. Rowe
Advisor

Kalev I. Sepp
Second Reader

Thomas J. Housel
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

For centuries, militaries throughout the world have used deception techniques to gain competitive advantage in warfare. This thesis evaluated the effect of deception with a particular commercial product within cyberspace. It measured the effect of its deception on the ability of attackers to achieve their objectives. The results of our experiments showed the deception could slow cyber-attacks. These results also suggested several future research opportunities and implementation strategies for deception in cyberspace operations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

C2	Command and Control
CCAT	Cyber Course of Action Tool
CO	Cyberspace Operations
COA	Course of Action
DCO	Defensive Cyberspace Operations
DMZ	Demilitarized Zone
DODIN	Department of Defense Information Network
HIPS	Host Intrusion Prevention System
JCS	Joint Chiefs of Staff
LAT MOV	Lateral Move
MILDEC	Military Deception
NE	Nash Equilibrium
OCO	Offensive Cyberspace Operations
PII	Personally Identifiable Information
POR	Program of Record
VLAN	Virtual Local Area Network
WINRM	Windows Remote Management

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank the faculty and staff of Computer Science, Information Science and Defense Analysis departments for all the support with this project. A special thanks is appropriate for Dr. Kalev Sepp and Ryan Maness for their insight and advice on military deception and cyberspace strategy. I would also like to thank Dr. Neil Rowe, my primary advisor, for allowing me to have just the right amount of freedom and flexibility to shape this research but also keeping me on track to meet all necessary requirements. Additionally, I am truly grateful for the support from Soar Technology Inc., especially Robert Bixler and Mike Van Lent, for their tremendous support in time and resources to complete this work. Finally, and most importantly, I would like to thank my son, Tristan, who is my inspiration and who has had to sacrifice with me during this process. I love you, son, and everything I do is ultimately for you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

All warfare is based on deception.

—Sun Tzu, *The Art of War*

The initial ground offensive of Operation Desert Storm in February of 1991 is considered one of the most successful uses of military deception on record. It aimed at reinforcing the belief in a U.S. ground and amphibious assault from southern and eastern borders of Iraq. Deceptions included conducting training exercises close to the borders, amphibious landing drills by U.S. Marines in the Persian Gulf, and information operations targeting Iraqi intelligence and leadership suggesting where their assault would launch from. Meanwhile, two U.S. Airborne Corps units relocated to the western flank in preparation to conduct an envelopment maneuver, a military tactic used to seize objectives to an enemy's rear while denying their ability to withdraw (Wright, 2020). The more the Iraqi forces positioned their defenses to their southern and eastern borders, the more the U.S. used overt actions to reinforce the belief of an imminent attack at those locations. These actions included camouflaged decoy tanks, communication emulators, and various other psychological tactics to convince the Iraqis that the U.S. was staging a significantly large military presence at the southern border.

This strategy of deception was based primarily on Magruder's principle of the exploitation of preconception which states "it is generally easier to induce an opponent to maintain a preexisting belief than to present notional evidence to change that belief" (Joint Chiefs of Staff [JCS], 2017, A-1). On February 24, 1991, the assault began as planned with the "left flank" of the Iraqis exposed as the U.S. troops met minimal resistance. The overall plan was so effective that within 100 hours of its start, the entire ground force had achieved virtually all of its objectives (Wright, 2020). The deceptive nature of this operation was successful despite the complexity of interplay between multiple domains of warfare on the U.S. military side and a lack of control over the Iraqi military defenses. With that in mind,

this thesis explores how military deception theory and its associated techniques affect operations in the new and emerging domain of cyberspace.

This research evaluated the effect of deception within a simulated cyberspace domain. Background information on military deception theory, cyberspace operations, and the concept of deception in cyberspace will be discussed first to provide the appropriate context for the research. Following this, I examine the related research on cyberspace deception, particularly research involving game theory or that included real-world cyberspace operators. After this review, the methods for this experiment will be explained, including the criteria and metrics used in the analysis of the results. Next, a quantitative and qualitative analysis of the results will be presented. This research concludes with additional considerations and recommendations for future work in this subject area.

II. BACKGROUND

A. MILITARY DECEPTION

Fundamentally, deception is a method of convincing others to believe a false idea which can result in either a specific action or inaction. It influences the attitudes and behaviors of those being deceived to invoke a response that directly aids the deceiver. A well-known theory of deception identifies two categories: displaying that which is false and concealing that which is true (Bell and Whaley, 1991). Military deception (MILDEC) aims to alter how an adversary views, analyzes, decides, and acts (JCS, 2017). MILDEC is a type of military "information operation" which focuses on influencing the decision-making process of adversaries while protecting that of your own. MILDEC can be implemented at the strategic, operational, and tactical levels of warfare. It is planned and executed following the six primary principles shown in Figure 1.

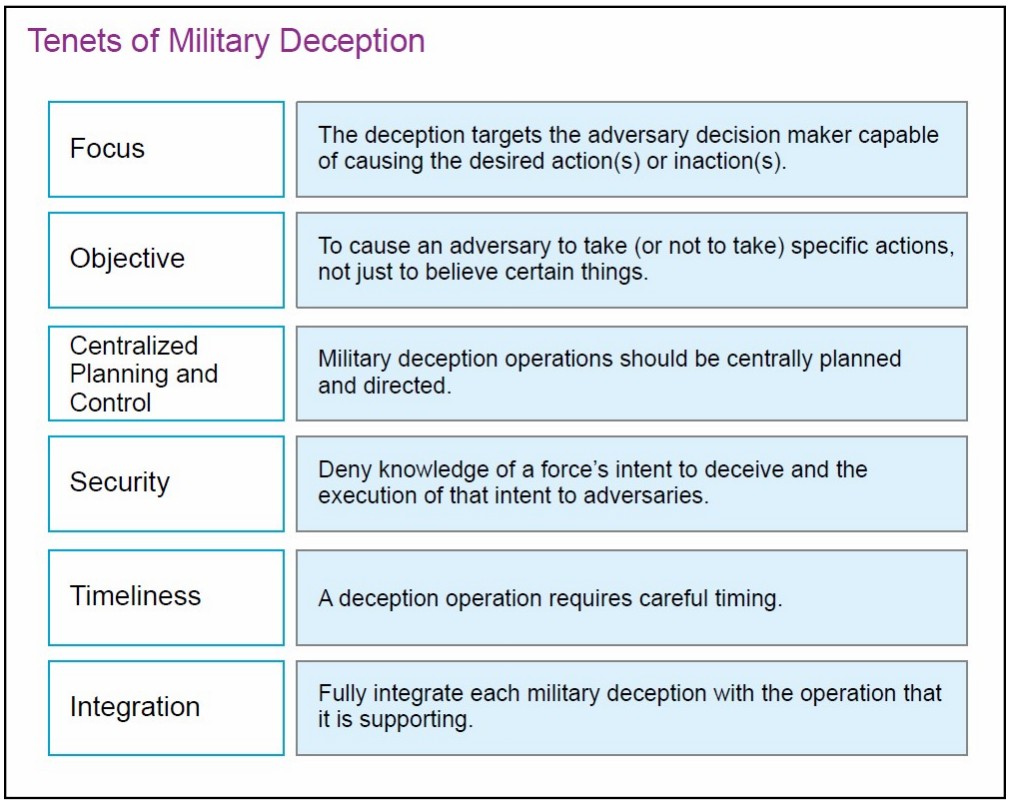

Figure 1. Six Tenets. Source: JCS (2017).

The planning of MILDEC occurs in five steps. First, mission analysis is conducted to determine if deception should be a part of the military operation or campaign. Next, a concept for the deception is developed to help achieve the commander's intent and mission objectives. Afterward, one course of action (COA) is selected and approved. Following the COA selection, a deception plan is developed that must be credible, flexible, and correctly timed to have a high probability of success (Latimer, 2003). Last, a review of the overall plan is conducted before its implementation.

Success for any deception operation depends heavily on a few key factors. Initially, a deceiver must thoroughly understand their adversary. Moreover, since MILDEC is typically focused on the leadership of an adversary, understanding of their mindset from intelligence information is key. Security of the deception is essential to ensuring success; both the operational plan which focuses on the deceiver's true intentions as well as the deception plan must be protected (Latimer, 2001). Also, the channels used to transmit the deception must be carefully chosen by the deceiver to have the best chance of reaching the target and being interpreted correctly. Lastly, the feedback from the target must be timely and systematically analyzed to allow for necessary adjustments to the deception plan.

B. CYBERSPACE OPERATIONS

Cyberspace, classified as the fifth domain of warfighting by the Department of Defense (DOD), is an increasingly interconnected, complex, and technology-driven environment that presents unique challenges for military operations. Conventional military capability (measured in numbers, weapons, and resources) is often of negligible importance in the cyberspace domain as strategy and tactics are more important and can give a competitive advantage to an otherwise weaker opponent. As in all domains of war, a well-thought-out and comprehensive strategy is essential to mission accomplishment. Within the traditional domains (air, land, maritime, and space), deception tactics and techniques are critical elements in the planning and execution of operations.

Cyberspace operations (CO) are defined by Joint Publication 3-12 as the "employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." The three types of cyberspace operations within the DOD are

offensive, defensive and Department of Defense Information Network (DODIN) operations. This thesis focuses on the interaction between offensive and defensive operations. Offensive operations project power in and through adversary cyberspace terrain while defensive operations protect one's own cyber resources against adversarial threats. DODIN operations include actions required to build, maintain, and securely operate networks to ensure confidentiality, integrity, and availability (JCS, 2018).

The cyberspace domain depends on the information environment to support operations being conducted in the other warfighting domains. Also, cyberspace operations can affect the dynamic other domains in the same way that traditional military operations can affect cyber domain. Cyberspace has complexity across the three interrelated layers of physical, logical, and cyber-persona (JCS, 2018). This complexity allows for a wide range of targeting options for cyber-attacks, but also increases the surface area for attacks we must defend. The reliance on information and feedback in the cyberspace domain make it highly susceptible to deception.

C. CYBERSPACE DECEPTION

Cyberspace deception has gained attention over the past decade. The consensus is that cyberspace is an offense-dominated environment in which defense is at a disadvantage (Lindsay and Gartzke, 2016). Nonetheless, deceptive strategies can bring a balance to cyberspace. Traditionally, computer systems and other devices within cyberspace (e.g., network and mobile devices) provide accurate information about themselves for operation and administration. Moreover, most computer systems are, by design, deterministic in nature. Therefore, the cyberspace domain, containing systems and networks that rely on the sharing of information to make decisions, is prime for deception. Cyberspace deception can be used in each type of cyber operations to enhance their effectiveness and decrease the adversary's ability to achieve their objectives.

Deception in cyberspace is conducted like traditional MILDEC operations. The key factors required for a successful deception operation mentioned earlier still hold true. Similarly, the benefits of MILDEC being a force multiplier, mission enhancer, and strategic enabler apply within the cyberspace domain as well. The traditional military taxonomies

of deception can also be applied to its use in cyberspace. Lies, camouflage, displays or decoys, and disinformation are useful types of deception that can be executed within cyberspace. As mentioned above, computer systems are typically designed to provide accurate information to users or administrators. Therefore, lies can deceive by intentionally providing false information. Lies are distinguished from disinformation as they are answers to queries or request for information, whereas disinformation is provided without the requirement for being requested (Rowe, 2016). Camouflage and decoys, the two types of deception in this research, can cause expenditure of resources from an adversary. For example, changing a name of an important file or system, to cause the adversary to spend more time and resources to verify its true identity, is a camouflage deception in cyberspace. Similarly, creating replica systems on a network that serve no purpose other than adding complexity to confuse adversaries, is an example of how decoys can be implemented.

Those examples were primarily for use in defensive cyber operations. They help the defender achieve a key objective, ensuring that detection plus response times of the defender remains less than the overall attack time. With deception, defenders have a higher probability of successfully defending and responding to an attack as it can increase the amount of time it takes an adversary to complete their objectives. Furthermore, the deception techniques of decoys, honeypots, and honeynets decrease false positives as any interaction with them not by the defender should not occur. The next section will explore the most relevant research on the use and evaluation of cyberspace deception.

III. LITERATURE REVIEW

A. CASE FOR CYBERSPACE DECEPTION

The case for deception in cyberspace operations begins with the historical success of military deception in the history of warfare. From the Battle of Cannae during the Second Punic War, to Operation Barbarossa during World War II, and, more recently, Operation Left Hook in Operation Desert Storm, deception has been a key strategy to gain the competitive advantage in military operations. Throughout history, many lessons have been learned and guidelines developed for deception in warfare (Monroe, 2012). As the Information Revolution continues, the reliance on information systems by nations and their militaries also increases, creating a capability and vulnerability paradox (Schneider, 2019). All actions within cyberspace depend on the storing, processing, or transmitting of information from these systems, which introduce opportunities for deception.

Another benefit of using deception in cyberspace is that it can bring stability to the domain (Gartzke and Lindsey, 2016). From an offensive perspective, intrusions and other cyber-attacks rely heavily on deception. Defensively, deception can cause uncertainty for attackers who may not be able to tell whether or not they are receiving accurate information. This uncertainty can create stability within the domain, as attackers will be less likely expend resources in environments where deception may be presence. This perspective challenges the notion of cyberspace as an offense-dominant domain by using deception to confuse and trap attackers (Gartzke and Lindsey, 2015). Furthermore, the prevalence of cyber espionage activities increases opportunities for deception in cyberspace (Valeriano et al., 2018).

Taxonomies for traditional deception practices apply to cyberspace (Rowe and Rothstein, 2004). A variety of deception techniques can achieve more effective detection and defense for cyber-attacks (Han, Kheir, and Balzarotti, 2018). A more thorough explanation of these concepts with considerations for the laws and ethics of cyberspace deception are discussed in (Rowe and Rrushi, 2016). Active cyber defense and modeling strategies for the planning and execution of cyberspace deception are discussed in (Jajodia

et al., 2016). Furthermore, specific circumstances for the use of cyberspace deception are explored with use cases and models for implementation in (Heckman et al., 2015).

B. RELATED WORK

Integrating deception into the cyberspace domain is not new, but most research focuses on a single perspective. For example, using real and fake results in network scans can confuse an attacker conducting reconnaissance of a network (Jajodia et. al., 2016). One type of research uses a game-theoretic analysis with complex algorithms to determine the effective techniques of deception in a simulated environment (Wang and Lu, 2018). Another variant using game theory evaluates an optimal defender strategy against powerful adversaries in a cyber deception game (Fang et. al. 2018). Lastly, game theory can evaluate the technique of concealing decoys and can enhance the effectiveness of cyberspace deception (Miah et al., 2020).

An important design element of cyberspace conflict scenarios is attack modeling. Most approaches model the interplay between cyber-attacks and the opposing defense measures. One method of attack modeling focuses on a set of conditions, primarily trust and availability, used in defining effects on human behavior of cyber-attacks (Cayirci and Ghergherehchi, 2011). Another approach uses attack graphs for visual representation of cyber-attacks that exploit vulnerabilities within networks. The complexity of these graphs, due to the size and scale of networks today, requires significant efforts in their generation (Liu et al., 2012). A goal of attack modeling is to determine an attacker's intent and objectives and determine the best defensive strategies to use against them. Research and experiments conducted using costs and incentive-based methodologies show promise to deduce this type of information (Liu, Zang, and Yu, 2005)

Another way to evaluate deception in cyberspace involves real networks and human operators instead of simulated agents. A large study, Tularosa, included over 130 red teams to help assess how defensive deception affects cyber attackers (Ferguson-Walter et al., 2018). This study consisted of questionnaires, cognitive tasks, and measurements of physiological effects to determine the extent deception affected participants. The first part of the study detailed the experimental design, implementation, and limitations while the

second portion (currently still being analyzed) will explain the findings (Ferguson-Walter et. al., 2018). Another study explored how deception affected humans in an experiment with four variants (Ferguson-Walter et al., 2017). The first variant investigated whether decoys alone were enough to deceive the red team, while the second told the red team members that deception could be present in the environment. The third variant told red team members that deception was present in the environment however, no deception techniques were activated. Lastly, for the fourth variant, the red team members were given complete knowledge of the environment including how the deceptive techniques worked. The intent was to determine how the actual presence of deception compared to the knowledge of deception.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. METHODOLOGY

A. OVERVIEW

The Cyberspace Course of Action Tool (CCAT) was developed by Soar Technology Inc. (located in Ann Arbor, MI), and funded by the Defense Advanced Research Projects Agency, to support research for military decision-making in the cyberspace domain (SoarTech). CCAT was used in this research to evaluate the effect of deception in cyberspace by developing and executing a cyber wargame scenario in a simulated environment. In collaboration with SoarTech, I created the scenario design and components, agent actions, deceptions, and evaluation metrics specifically for this research. The specifics of each are

B. SCENARIO DESIGN

The scenario was designed to emulate a cyber wargame using simulated attacker and defender agents. The two objectives for each model were for the attacker agent to exfiltrate the personally identifiable information (PII) file "PII.txt," and to corrupt or destroy the "sysconfig.conf" file on the Program of Record (POR) server. The POR server simulated a mission-critical server commonly found in operational military networks. The PII.txt file simulated a military roster with PII data (e.g., social security numbers, addresses, phone numbers, and blood type). The "sysconfig.conf" file simulated a system file used for running a critical service on the POR server.

The experiment consisted of four variant models in which the attacker and defender agents competed against each other. Variant One was the control experiment and provided baseline metrics of how each agent performed in a direct engagement. Variant Two contained two decoy servers and two decoy files. Variant Three included two instances of camouflage: the PII.txt and the sysconfig.conf files were both renamed. Finally, the previous two variants were combined to create the fourth variant. Variant Four also allowed the defender agent to deploy additional decoy or camouflage tactics, if desired. The variants and their associated techniques are:

- Variant One: No deception

- Variant Two: Decoys
- Variant Three: Camouflage
- Variant Four: Decoys and camouflage

The decision process for the agents was based on Empirical Game-Theoretic Analysis, specifically a version called "double oracle" that also included deep reinforcement learning (DO-EGTA with RL) (Wright et al., 2019). This method iterates over a series of two-player games learning the best strategies for each side. Before the evaluation games, both attacker and defender agents underwent training which consisted of them attempting various actions in different sequences to determine a strategy. The optimal strategy for an agent, despite any strategy used by their opponent, is called the Nash equilibrium (NE). To determine what agent strategies would be used for the evaluation period, a sample of strategies derived from the training period were compared to the computed Nash equilibrium; the strategies, for both attacker and defender agents, closest to the equilibrium were selected for the evaluation. The time limitations for experimentation did not permit evaluation of all strategies. Instead, this experiment sampled strategies that resulted from the training period. The time required to train an agent depends on the hardware and resources available, including system processing power and storage capacity (see Chapter VI).

C. SCENARIO COMPONENTS

1. Network Map

The network used for this scenario, seen in Figure 2, simulated a scaled-down version of a standard military network with traditional security components, segmentation, devices, and services. It consisted of three virtual local area networks (VLANs) containing servers, workstations, a firewall, and networking devices commonly found on a small military network. The demilitarized zone (DMZ) VLAN contained a network boundary firewall and router. The DMZ VLAN also included three front-end servers supporting email, web services, and applications which acted as proxies to their back-end server counterparts in the server VLAN. This configuration required the attacker to exploit the

front-end servers to access the back-end servers where the objective files were located. The user VLAN contained one router, two standard Windows client (WinCli) machines and one WinCli administrator machine. Two POR client (PORCli) machines in this VLAN had direct access to the POR servers in the server network. Lastly, the server VLAN contained one router, two domain controllers, two web database servers (webserver back-ends), two file servers, two POR servers, one mail (back-end), and one application server (back-end). The goal nodes on the map (the servers that contain the objective files) are indicated in gold, and the decoy servers are indicated in blue.

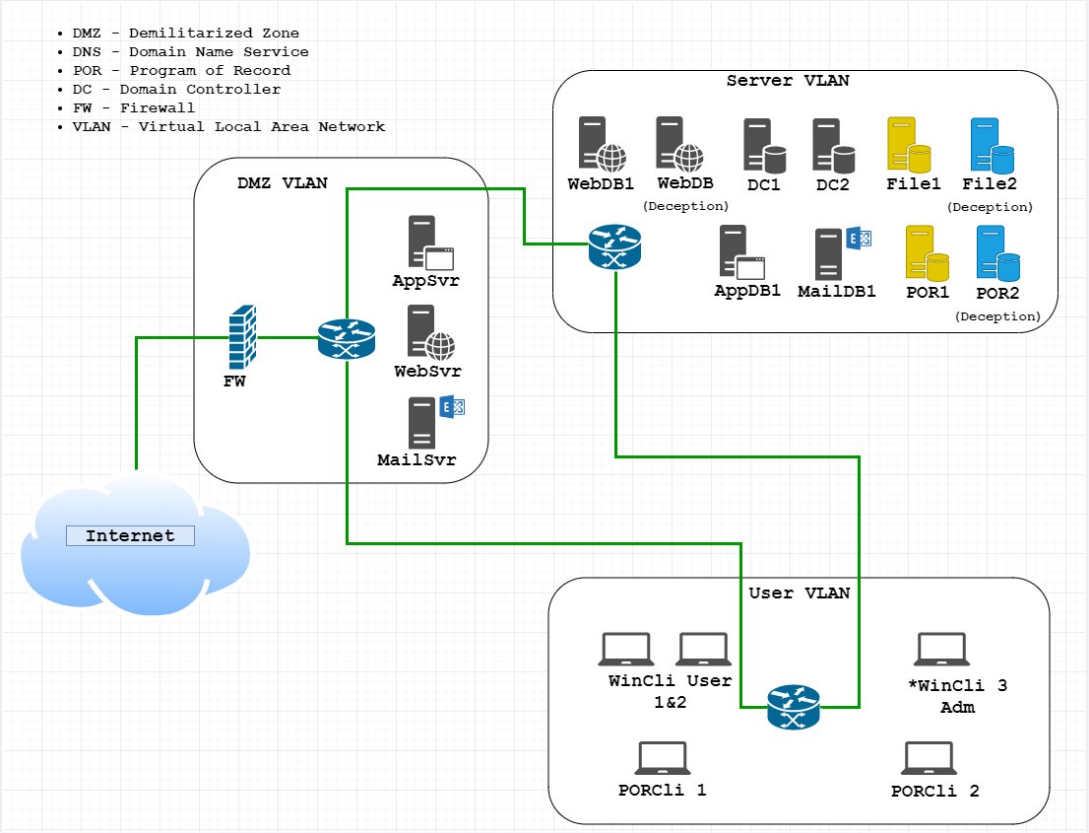

Figure 2. Scenario Network Map

2. Flowcharts

The attack flowchart in Figure 3 and defender flowchart in Figure 4 were created in collaboration with SoarTech to show the cyber scenario from the attacker's and the

defender's perspectives, respectively. Actions available to the agents are indicated by squares. After an action is selected, a security condition indicated by a circle will become available if that action was executed successful. Security conditions represent information about the network or an asset on the network (i.e., a web server or the application port of a web server). The probability of an action being executed successfully depends on the complexity of the action; thus, more complex actions have a slightly lower probability of success. Also, an element of randomness is factored into the environment which simulates the uncertain nature of cyberspace attacks and defenses operating as intended. All security conditions resulting from the attacker's actions can be seen by both the attacker and defender agents; however, the defender security conditions are hidden from the attacker. The attacker flowchart (Figure 3) was created to represent a streamlined version of the standard cyber kill chain combined with several tactics and techniques from the MITRE ATT&CK framework (MITRE, 2020). The box in Figure 3 delineates actions conducted on the defender network (inside the box) and actions the attacker would conduct outside on its own network. The MITRE ATT&CK framework was also used to develop the actions in defender flowchart (Figure 4) to best defend against the attacker actions. All defender actions in Figure 4 are conducted within the network.

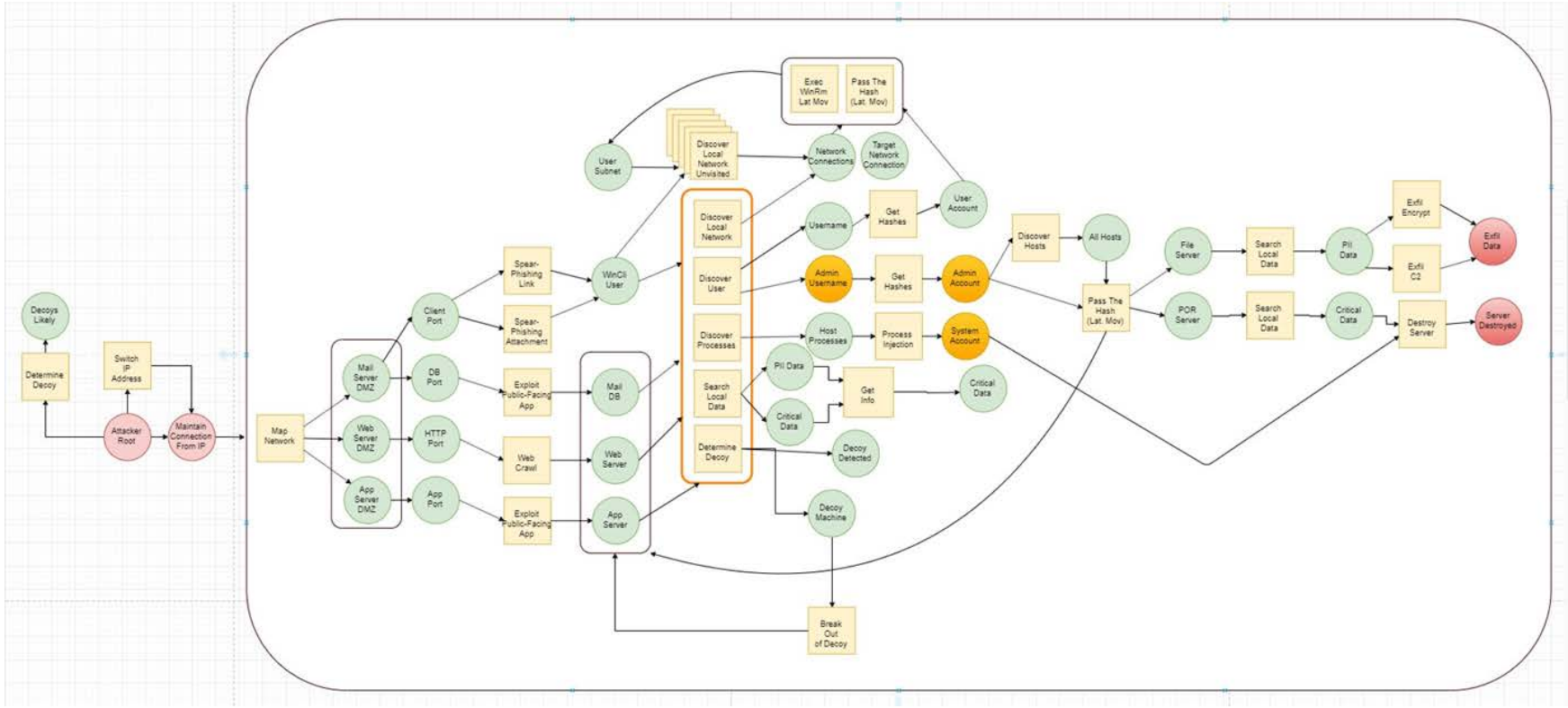

Figure 3. Attacker Flowchart

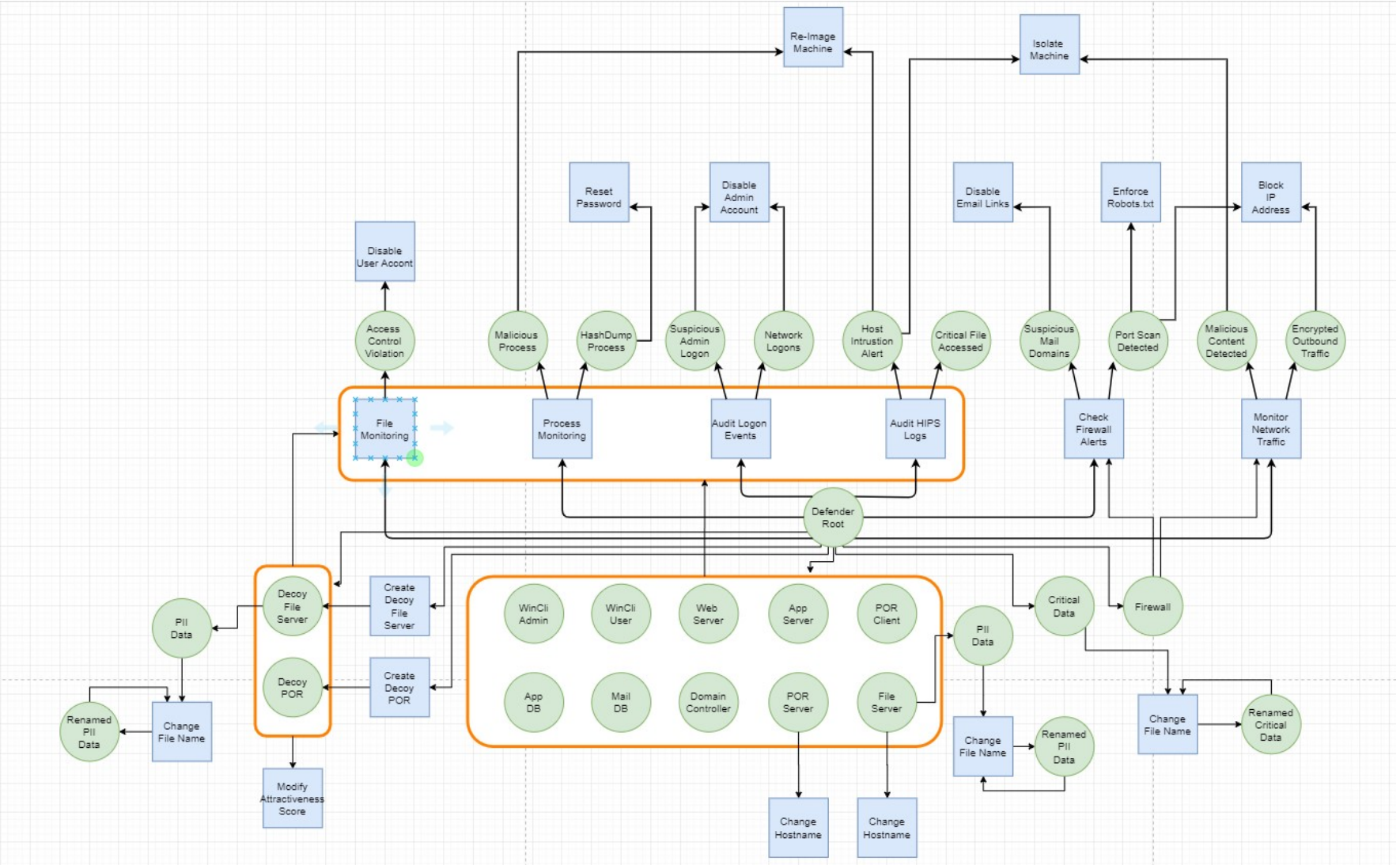

Figure 4. Defender Flowchart

D. AGENT ACTIONS

This section describes the actions that were available to the attacker and the defender agents during the experiment. Each action selected by the attacker has an associated cost that is subtracted from the overall score at the end of the game (see Table 1). Each objective for the attacker has a reward value which is added to the attacker's overall score. Similarly, the defender has costs associated with their actions that are also detailed in Table 1. Each agent can attempt as many actions as they want during a turn as long as that action is available (i.e., the action becomes available based upon successful completion of prerequisite actions).

Table 1. Costs and Rewards

Attacker Action	Cost	Reward	Defender Action	Cost	Linked Action
Connect to Network	5	-	Audit Logon Events	15	Exec WinRm Lateral Move, Pass the Hash
Map Network	5	-			
Spear-phish Link	10	-	Monitor Network Traffic	25	Map Network, Exfiltrate Data, Spear-phishing
Spear-phish Attachment	20	-			
Exploit Public-Facing Mail	15	-	Check Firewall Alerts	15	Map Network, Exfiltrate Data, Spear-phishing, Web Crawl
Web Crawl	10	-			
Exploit Public-Facing App	15	-			
Discover Local Network	10	-	Audit HIPS Logs	25	Critical Service Destruction/Corruption
Discover User	10	-			
Discover Processes	20	-	File Monitoring	20	Search Local Data
Search Local Data Host	10	-	Process Monitoring	30	Process Injection, Get Hashes
Get User Hash	25	-			
Get Admin Hash	35	-	Isolate Machine	60	Exfiltrate Data
Process Injection	35	-	Block IP Address	20	Map Network, Exfiltrate Data, Spear-phishing
Get Info	20	-			
Pass the Hash	30	-	Enforce Robots.txt	20	Web Crawl
Exec WinRm Lateral Movement	20	-	Disable Email Links	25	Spear-phishing Link
Discover Hosts	15	-	Disable Admin Account	50	Pass the Hash
Search Local Data File Server	10	-	Disable User Account	50	Exec WinRm Lateral Move, Pass the Hash, Search Local Data, Get Hashes
Search Local Data Critical Server	20	-			
Exfiltrate Data Encrypted	35	100-300			
Exfiltrate C2	25	100-300	Reset Password	20	Get Hashes
Critical Service Destruction	25	900	Re-Image Machine	90	Process Injection
Critical Service Corruption	75	1200			
Decoy Scenario Actions	**Cost**	**Reward**	**Decoy Scenario Actions**	**Cost**	**Linked Action**
Determine Decoy	10	-	Create Decoy File Server	150	-
Break Out of Decoy	10	-	Create Decoy POR	150	-
Check File	10	-	Change File Name	35	-

1. Attacker Actions

The first actions the attacker agent can select are preparatory in nature. The "Determine Decoy" action assesses the probability of decoys within the environment, and the "Switch IP Address" action will temporarily prevent the defender agent from blocking the attack. Following this, the attacker can only choose the "Map Network" action, which is a type of network reconnaissance. This action simulates a probing scan on a target network. If successful, the security conditions for the servers in the DMZ subnet and their open ports are displayed.

The next possible actions represent the initial access stage where an attacker chooses a specific attack action, based on its availability, to gain entry into the network. The five actions available include two spear-phishing email actions (link and attachment), two exploits of public-facing applications (one by the database port of the mail server and one by the application port on the application server), and an inventory (web crawl) on the web server by use of its Hypertext Transport Protocol (HTTP) port. If any of these actions are successful, a security condition will appear for an asset in either the server VLAN or the user VLAN, depending on which action was chosen. For example, if either spear-phishing action is selected and executed successfully, a security condition for a WinCli user becomes available. Similarly, if the web crawl action is selected, the security condition for the web server (back-end) in the server VLAN becomes available.

The next stage includes a set of discovery actions used by the attacker to identify more information about the network and assets. These actions will be performed only on the assets identified by the preceding security conditions available. The first action is "Discover Local Network" which will show other assets on the same VLAN. A special variant of this action is "Discover Local Network (Unvisited)" which will only show only assets not previously selected. The security information obtained as a result of these two actions are the network addresses of the assets within the VLAN. The next action available is "Discover User," which queries an asset to determine what user accounts reside on it and returns with a security condition for each account successfully identified. Also, this action may result in the identification of an administrative user who can access more information. The "Discover Processes" action queries the local asset to find running processes and

returns a list of those processes if successful. The last two actions in this stage are “Search Local Data,” which identifies files in the asset, and “Determine Decoy,,” which tests whether an asset is a decoy. The first can result in two security conditions, PII data and critical data, while the latter returns a security condition indicating if the asset is a decoy device or not.

The subsequent stage contains privilege-escalation and lateral-movement actions for the attacker. The “Get Hashes” attempts to dump the password hashes from a selected user account or administrative account. If the “Get Hashes” action executes successfully, it provides the attacker a user account or administrative account to use in follow-on actions. Next, the “Exec WinRm Lat Mov” and “Pass the Hash (Lat Mov)” actions represent two ways to move laterally to a different asset within the VLAN. The “Process Injection” action simulates the attacker migrating from a process with user level privileges to one with administrator privileges. Lastly, the “Get Info” action determines whether the file being queried is the correct one needed for the objective.

The last set of attacker actions comprise the “impact” stage. The first of these actions includes “Search Local Data,” which tells the agent if the PII file is on the current asset and “Destroy Server” which disables the POR server. The last two actions in this stage are “Exfil Encrypt” and “Exfil C2” which simulate the exfiltration of the PII.txt file by an encrypted channel or command and control channel, respectively.

2. Defender Actions

Figure 4 depicts the types of defender actions available: traditional defensive measures and deception techniques. The overall goals for the defender are to identify the actions the attacker has completed, try to restrict future actions, and ultimately prevent the attacker from achieving its objectives. At the start of each game, the defender can select from six defensive actions which begins at the defender’s root (located in the center of Figure 4). The file monitoring action checks whether a specific file has been accessed by the attacker. Process monitoring looks for malicious processes or specific processes that indicate the attacker has performed a “Get Hashes” action. The “Audit Logon Events” action shows if a suspicious administrator login or a lateral move has been conducted by

the attacker agent. This is followed by the “Audit HIPS Logs” action, which checks the host’s intrusion-prevention-system logs for indicators of malicious activity or critical files being accessed. The “Check Firewall Alerts” action indicates that the attacker has successfully executed either a spear-phishing attack action or the “Map Network” activity. The final action initially available to the defender is “Monitor Network Traffic” which identifies exfiltration of information by encrypted traffic and other malicious indicators throughout the network.

Subsequent defender actions use more active measures to protect the network and prevent attacker from achieving their objectives. These actions include disabling a user or administrator account, resetting a password, or disabling email links (which blocks the attacker’s ability to choose that spear-phishing action). Also, the “Enforce Robots.txt” action impedes the attacker’s use of web crawling, while the “Block IP Addresses” action prevents all internal and external traffic from the attacker. If successful, the “Block IP Addresses” action will require the attacker to execute the “Change IP Address” action to resume its attack. The last level for defender actions contain two actions to be used as a last resort. The first is re-imaging of the asset which resets the asset to its initial state and removes all attacker progress. The final action isolates the asset, which prevents any network connections, making the asset unreachable.

All defender actions listed above are traditional defense measures. The actions located below the “Defender Root” security condition in Figure 4 show the deceptions and their associated security conditions. Each action relates to either the decoy or camouflage technique. Some actions can be used more than once; for instance, the “Change File Name” can be selected under multiple security conditions to apply to different files. Another example of an action that can be used more than once is “Modify Attractiveness Score” which allows a defender to change how the attacker agent views a decoy. A higher score will increase the probability of the attacker choosing that action.

Decoy deceptions mimic or copy legitimate resources. They add complexity and confusion, causing uncertainty and requiring more time for an adversary to verify information. This experiment used decoy servers and decoy files. The decoy servers mimicked File Server 1 (FS1) and the Program of Record (POR) Server 1. The decoy files

mirrored the files directly attached to the attacker's objectives, PII.txt and sysconfig.conf. Camouflage renamed them as Camo_PII.txt and Camo_Sysconfig.conf. The purpose of this deception was to make the attacker spend more resources (such as time) in identifying the true nature of the file, thereby increasing the defender's chance to detect the attacker and respond with preventive actions.

E. EVALUATION CRITERIA AND METRICS

Several factors were considered to evaluate the success of the deception during the experiment. These factors are:

- What type of cyberspace operation could the deception support: offensive, defensive, or traditional military operations?
- What background experience and knowledge did each agent have; for instance, were the agents previously trained in the environment or did they know of the other agents' capabilities?
- How much of the agent strategy related to deception, and what was its goal?
- How many additional resources or costs were used during the wargame on both sides? For instance, how much time was spent by the attacker to determine if deception was being used?
- How much did each deceptive technique affect the ability of the opponent to achieve their objectives?
- How much did each deceptive technique affect the agent's choice of actions and its overall strategy?
- Which actions were chosen most frequently by the agents?

The metrics described next were chosen to quantify the above criteria.

- Overall score: Total points (positive or negative) received by an agent for successful and unsuccessful actions.
- Action frequency: The number of times an action was taken in the game.
- Timesteps: The number of turns taken in a game by an agent.
- Objective accomplishment: Whether an agent successfully achieved an objective. By default, a defender agent does not accomplish its objective if the attacker agent achieves either of its objectives.

V. EXPERIMENTS, RESULTS, AND DISCUSSION

Before the evaluation portion of the experiment, each agent was trained to be more intelligent, efficient, and effective. The training for each scenario was done in parallel on a cloud-computing platform and lasted approximately 3 weeks. The resources to train the agents and evaluate them were one CentOS 7 core server with an i7-7820X processor at 3.60GHz, 8 cores, 128 gigabyte random access memory, and two Nvidia Tesla V100 32 gigabyte graphical processing units. The evaluation period consisted of 100 games, per variant, between the fully trained attacker and defender agents whose strategies were closest to the Nash Equilibrium. The results of the evaluation indicated the effect of deception in the variants using the metrics described previously.

The overall score metric determines the total cost (i.e., resources) spent and the rewards received (i.e., goals) for each agent during the game. Rewards are only granted to the attacker if it achieves an objective; therefore, the defender's overall score will always be a negative value. Also, any reward value the attacker receives will be considered a cost to the defender and deducted from its overall score. Therefore, the effectiveness and efficiency of both the attacker and defender agents can be evaluated based on how low their overall score value is at the end of each game.

The number of times an action is taken by both agents was recorded and then averaged to determine each action's frequency. This metric indicates which actions each agent used most and how deception affected their choice of actions. The timestep metric was calculated based on the number of turns each agent played during a game until an objective was achieved. The maximum number of timesteps allowed in a game was set at 40. The average number of timesteps per variant was then calculated to determine how each implementation of deception affected the attacker's time. The final metric, mission accomplishment, tracked whether the attacker agent achieved any objective during the game. This metric was separated into two categories as there were two objectives: (1) exfiltration of data and (2) corruption or destruction of the POR server. The raw results for action frequency, overall score, objective accomplishment, and timestep counts are provided in the experiment results section of the appendix. Increases from the baseline

variant are highlighted in green, decreases are highlighted in red, blue indicates there was no change from the baseline, and black indicates the timestep limit of 40 was reached without the attacker achieving an objective.

A. VARIANT ONE—NO DECEPTION

This initial variant was used as a baseline for comparison with the three other variants in which deception techniques were implemented. The average defender score for this baseline variant was -3849.75. This was the defenders lowest average score across the four variants, indicating that the defender's costs increased when deception was introduced. The average attacker score was -1534.15 for the baseline variant. As with the defender, this score was the lowest for the attacker across all variants, which indicates the attacker incurred (as expected) more costs during variants containing a type of deception.

An average of 174 actions were taken by the attacker during this variant. The most frequent action by the attacker was the "Discover Local Network" which was selected an average of 20 times per game. The action chosen the fewest amount of times by the attacker was the "Spear-phishing Link" with an average of four times a game. The defender selected the "Process Monitoring" action most often with an average of 13 times per game, while the "Isolate Machine" was the least selected, averaging only one selection per game. The defender agent executed an average of 93 actions per game during this variant. Lastly, the average number of timesteps to complete each objective were 25 and 32 for the exfiltration and corruption/destruction objectives, respectfully.

B. DECEPTION VARIANTS

The overall scores for both attacker and defender agents in the deception variants decreased as compared to each of their baselines. The decoy variant decreased the average score of the defender by over 300 points, which was the largest change recorded across all deception variants. Most of the overall scores for the variants containing deception resulted in decreases for both the attacker and defender. The number of games, out of the 100 used for the evaluation period, that resulted in a decreased overall score are displayed in Table 2 (i.e., the percentage of time a game resulted in a lower score compared to the baseline).

Table 2. Percentage of Time Score Decreased (100 Games)

	Camouflage	Decoy	Hybrid
Attacker	66%	53%	61%
Defender	57%	64%	57%

The average number of actions taken for the attacker and defender increased from the baseline in each deception variant. For the attacker agent, there was an average increase of approximately 20 actions per game whereas the defender's average increase was only 10. The "Exploit Public-Facing Mail" action was chosen the least with an average of one selection per game. There was no deviation from the baseline in the most frequent action selected (Discover Local Network). "Audit Logon Events" was the highest selected action by the defender with an average of 11 per game. In contrast, the "Isolate Machine" action was never selected by the defender agent during these variants.

The number of timesteps in the decoy variant for the exfiltration objective was the only category to experience a decrease. In all other cases, the average number of timesteps increased slightly across all deception variants. The minimal change was less than one timestep on average. Despite the small change in timesteps, the percentage of time that the attacker successfully achieved their objectives displayed a more significant decrease. For the exfiltration objective, success decreased 14% for the attacker, while the corruption and destruction objective resulted in a 12% decrease.

C. DISCUSSION

Without deception, there was a higher success rate for the attacker agent achieving their objectives as compared to the variants with deception techniques present. Moreover, the number of average timesteps correlated with the percentage of successful objectives achieved. A higher success rate correlates to a lower average in timesteps. Conversely, a higher average number of timesteps indicates a lower success rate.

The overall scores indicate that the presence of deception caused both the attacker and defender agents to incur more costs to achieve their objectives. This result was expected as deploying any additional defensive techniques will require more costs for defenders. Similarly, the attacker will experience increased costs for the additional techniques used to mitigate the presence of the decoy. The defender had a smaller deviation than the attacker between the scores in the deception variants as compared to their baselines. On average, the defender's score with deception was 236.93 points higher than the baseline, whereas the attackers score with deception was 239.81 points higher. This comparison, although minimal, demonstrates that deception affects the overall score of the attacker more than the defender.

The number of average actions taken by the attacker were noticeably higher in the variants with deception (approximately 20 more actions per game). These increases are evidence that deception techniques can impose additional costs on an attacker, which give the defender more opportunities for detection. In total, there were 8 actions the attacker increased selection frequency for (i.e., attacker found them to be more successful). The attacker decreased frequency in 10 actions. Finally, there were 7 actions where the frequency remained equal to its baseline averages. These results indicate the attacker considered a higher number of actions to be less effective when operating in a deception environment.

The results from the analysis of the timestamps indicate two things. First, the deception techniques increased the average amount of time it took the attacker to achieve its objectives. If defenders can use deception to increase the overall attack time, they increase the amount of time they have to detect and respond to the attack. Thus, the goal of defenders should be to ensure detection and response time remain less than the total amount of time for an attacker to reach their objective. Second, deception decreases the success rate of attackers achieving their objectives. During the baseline variant, the attacker agent achieved its objective 95% of the time for exfiltrating documents and 78% of the time for corrupting or destroying the critical server. Deception decreased the attacker's ability to achieve each objective by an average of over 12%.

VI. CONCLUSION AND FUTURE WORK

The success of deception in supporting military operations has been well documented throughout history. Although the domain of cyberspace brings challenges to the traditional approach to warfare, it also presents ample opportunities to use deception. The cyberspace domain is built on the need to transmit, process and store information, which intrinsically makes it vulnerable to deception. “The internet’s capacity for deception is what facilitates its use” (Gartzke and Lindsey, 2015, p. 327). The research in this thesis suggested that using deceptive tactics in the cyberspace domain is an effective defensive strategy. Furthermore, these techniques can affect real-world attackers significantly, particularly in increasing the amount of time required to complete an objective and by imposing additional costs.

Further research should compare game-theoretic results with the experience of cyber operators to identify areas in which each approach can be improved. Second, a more detailed scenario design and its accompanying components is needed to validate the effects of deception with other constraints within a network (e.g., network protocols, inherent security measures, and user or administrator interaction). Also, the attacker and defender capabilities need to expand to more advanced techniques to determine how these deceptive techniques would perform in real-world scenarios. Third, the effect of deception from an offensive perspective is necessary to provide a comprehensive evaluation of its effectiveness.

This research provided a framework which can be expanded to identify how well deception can be used in other types of cyber operations. Ironically, cyberspace is the most modern and complex warfare domain, yet it may benefit the most from one of the oldest and simplest tactics in warfare.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. EXPERIMENT RESULTS

The figures in the Appendix show the quantitative results of the 100-game evaluation period for each variant:

A. OVERALL SCORES

The overall scores, shown in Figures 5–7, display the sum of all costs expended and rewards achieved for both the attacker and defender agents.

	Baseline	Decrease	Increase	Neutral				
Game	Defender Score				Attacker Score			
Number	Baseline	Camoflague	Decoy	Hybrid	Baseline	Camoflague	Decoy	Hybrid
1	-3295	-5420	-2865	-4100	-2260	-690	-2870	-1685
2	-5175	-4855	-3800	-4215	-130	-1350	-1930	-1660
3	-4755	-4565	-4900	-4855	-775	-1380	-785	-1040
4	-4985	-4435	-4910	-4600	-215	-1640	-770	-1340
5	-4275	-3925	-5205	-4560	-1090	-1890	-475	-1365
6	-4425	-4430	-3860	-3965	-675	-1620	-1950	-1980
7	-2510	-4995	-4925	-3310	-2865	-765	-745	-2260
8	-3280	-3425	-4095	-3060	-2000	-2490	-1915	-2890
9	-3905	-3670	-4180	-3670	-1390	-1945	-1685	-1995
10	-3555	-3130	-3500	-5450	-1945	-2790	-2280	-180
11	-2895	-4520	-3725	-3295	-2600	-1605	-1985	-2320
12	-3775	-4145	-4285	-4490	-1675	-1665	-1695	-1325
13	-2710	-2970	-4755	-3930	-2590	-2830	-1325	-1950
14	-4870	-3830	-4715	-3255	-460	-2215	-1325	-2820
15	-2955	-3795	-3875	-3785	-2545	-1975	-1925	-2195
16	-3570	-4325	-4455	-3200	-1925	-1375	-1320	-2865
17	-3600	-3140	-3755	-4385	-1700	-2580	-1990	-1395
18	-4180	-4060	-5195	-3995	-1335	-1925	-455	-1945
19	-3985	-4505	-4955	-4145	-1330	-1385	-750	-1900
20	-2500	-4125	-3315	-4405	-2840	-1615	-2495	-1340
21	-4605	-3805	-3365	-5890	-710	-2190	-2290	-135
22	-3570	-3560	-4160	-5710	-1725	-2280	-1415	-145
23	-3780	-3805	-4345	-4000	-1635	-2185	-1360	-1960
24	-4215	-2925	-3755	-5200	-1300	-2890	-2260	-770
25	-5245	-3580	-3905	-4905	-175	-1980	-1950	-740
26	-2940	-4790	-4475	-2950	-2580	-1275	-1385	-2600
27	-3745	-4750	-4475	-4245	-1665	-1000	-1625	-1390
28	-4855	-3025	-4255	-4355	-415	-2815	-1665	-1395
29	-3540	-2975	-4240	-4945	-1685	-2870	-1380	-790
30	-4735	-3155	-2810	-4420	-770	-2815	-2875	-1610
31	-3100	-3380	-5285	-3955	-2270	-2535	-450	-1965
32	-3415	-3660	-4455	-3170	-1965	-2235	-1355	-2530
33	-3965	-2875	-3070	-3105	-1380	-2855	-2840	-2835
34	-3205	-3545	-2825	-3250	-2300	-2245	-2860	-2825
35	-3090	-5460	-4425	-4165	-1960	-425	-1615	-1685
36	-4570	-3060	-2820	-5430	-720	-2805	-2890	-160
37	-5085	-4655	-4010	-3880	-135	-1285	-1640	-1940
38	-5130	-4975	-3935	-4315	-220	-795	-1965	-1695
39	-3570	-3030	-4870	-4420	-1645	-2885	-1085	-1640
40	-3590	-5540	-4090	-2945	-1645	-460	-1930	-2855
41	-3440	-3035	-3875	-4175	-1920	-2815	-1695	-1675
42	-3240	-3050	-5705	-3165	-1900	-2815	-180	-2615

Figure 5. Overall Scores Part 1

43	-3370	-4475	-4755	-4875	-1940	-1320	-1020	-1050
44	-3420	-4420	-3850	-3105	-2240	-1660	-1680	-2805
45	-5105	-4510	-4400	-4785	-465	-1335	-1390	-1080
46	-3975	-2900	-4895	-5285	-1375	-2890	-780	-430
47	-3700	-4175	-4450	-3105	-1680	-1655	-1320	-2585
48	-3895	-3360	-4395	-3890	-1345	-2805	-1405	-1955
49	-4035	-4110	-3785	-3405	-1330	-1685	-2185	-2555
50	-4630	-4070	-3080	-4415	-720	-1940	-2855	-1665
51	-4130	-4095	-5450	-3990	-1360	-1910	-465	-1910
52	-3985	-4100	-3595	-4495	-1400	-1665	-2215	-1340
53	-4305	-4735	-4760	-3295	-1035	-1315	-1055	-2780
54	-3170	-5265	-3205	-2935	-2305	-710	-2535	-2870
55	-3270	-4905	-5700	-3760	-2295	-1010	-150	-2005
56	-2695	-4700	-4290	-5060	-2595	-1070	-1680	-750
57	-2670	-3100	-5220	-4330	-2890	-2795	-710	-1675
58	-3780	-3515	-3015	-2790	-1710	-2525	-2890	-2900
59	-5095	-5685	-4035	-4950	-175	-415	-1960	-1060
60	-4760	-5755	-5555	-3105	-515	-130	-175	-2835
61	-3770	-4385	-3945	-5315	-1685	-1380	-1930	-700
62	-3925	-3005	-3230	-3045	-1600	-2880	-2525	-2870
63	-3970	-5115	-2770	-3385	-1395	-740	-2845	-2275
64	-4555	-4185	-4940	-5275	-1030	-1910	-770	-780
65	-5330	-3440	-3960	-5225	-125	-2280	-1710	-475
66	-4845	-4015	-3815	-4115	-510	-1660	-1930	-1960
67	-3565	-3580	-3770	-5185	-1965	-2230	-1970	-720
68	-4175	-3140	-4245	-4935	-1385	-2860	-1690	-1045
69	-3935	-4235	-4955	-4430	-1305	-1935	-1030	-1675
70	-3545	-4080	-4195	-3145	-1725	-1905	-1645	-2870
71	-3780	-4190	-4260	-5275	-1635	-1890	-1420	-455
72	-3480	-2805	-5005	-3105	-2000	-2865	-720	-2875
73	-3995	-4210	-3585	-3920	-1370	-1350	-1970	-2235
74	-3920	-4535	-4200	-5145	-1365	-1295	-1630	-715
75	-3630	-3885	-4040	-3705	-1715	-1985	-1950	-2245
76	-5210	-3130	-3335	-2695	-180	-2775	-2530	-2910
77	-5140	-4270	-2925	-4480	-90	-1625	-2880	-1580
78	-3470	-2725	-3670	-2980	-1970	-2825	-1940	-2900
79	-2845	-2900	-4035	-3965	-2840	-2875	-1635	-1905
80	-3910	-5980	-3845	-2935	-1650	-70	-1990	-2890
81	-4525	-5240	-4280	-3215	-755	-750	-1625	-2585
82	-4455	-3970	-3640	-2930	-1060	-1690	-2280	-2895
83	-2530	-5130	-3440	-3075	-2845	-760	-2295	-2870
84	-3035	-4395	-5695	-3825	-2305	-1650	-155	-2215
85	-3280	-4010	-3700	-5355	-1950	-1655	-1990	-690
86	-3655	-5805	-5400	-4985	-1950	-135	-430	-760
87	-2620	-3060	-2910	-3780	-2615	-2775	-2875	-1935

Figure 6. Overall Scores Part 2

88	-4750	-3075	-3415	-4645	-740	-2870	-2490	-1365
89	-3670	-3930	-4420	-4165	-1725	-1920	-1630	-1615
90	-4000	-4265	-3740	-4475	-1415	-1660	-2230	-1665
91	-4095	-3730	-2825	-4535	-1330	-2260	-2865	-1390
92	-3235	-3050	-4280	-2825	-2255	-2810	-1640	-2855
93	-4495	-3715	-5230	-3125	-680	-2185	-760	-2620
94	-2855	-3750	-3730	-4110	-2545	-2260	-2220	-1665
95	-3040	-4360	-6000	-3140	-2255	-1605	-100	-2825
96	-3575	-4995	-4555	-4425	-1720	-1050	-1320	-1585
97	-3485	-3040	-5280	-3590	-2005	-2870	-735	-2265
98	-3075	-3720	-3350	-4830	-2260	-1910	-2570	-1065
99	-3735	-4465	-2990	-4065	-1695	-1300	-2625	-1945
100	-4050	-4400	-5365	-5295	-1330	-1635	-435	-710
Avg	-3849.75	-4026.90	-4158.25	-4074.90	-1534.15	-1861.05	-1658.30	-1802.55

Figure 7. Overall Scores Part 3

B. ACTION FREQUENCY

The action frequency, shown in Figures 8 and 9, displays the all available actions and amount of times they were attempted for each agent.

			Baseline	Neutral	Increase	Decrease	
Attacker Action	Cost	Reward	Baseline Scenario	Camoflague Scenario	Decoy Scenario	Combined Scenario	Average Deception
Connect to Network	5	-	1	1	1	1	1.00
Map Network	5	-	7	9	7	5	7.00
Spear-phish Link	10	-	4	6	7	10	7.67
Spear-phish Attachment	20	-	5	5	5	4	4.67
Exploit Public-Facing Mail	15	-	5	1	1	1	1.00
Web Crawl	10	-	5	6	2	2	3.33
Exploit Public-Facing App	15	-	7	3	5	3	3.67
Discover Local Network	10	-	20	21	20	20	20.33
Discover User	10	-	14	14	19	16	16.33
Discover Processes	20	-	12	12	15	16	14.33
Search Local Data Host	10	-	17	18	14	14	15.33
Exfiltrate Local Data	20	-	9	9	7	7	7.67
Get User Hash	25	-	6	7	8	6	7.00
Get Admin Hash	35	-	5	4	3	3	3.33
Process Injection	35	-	5	5	6	6	5.67
Get Info	20	-	10	10	12	12	11.33
Pass the Hash	30	-	7	7	4	2	4.33
Exec WinRm Lateral Movement	20	-	6	6	5	7	6.00
Discover Hosts	15	-	6	8	5	4	5.67
Search Local Data File Server	10	-	10	9	10	8	9.00
Search Local Data Critical Server	20	-	10	11	12	11	11.33
Exfiltrate Data Encrypted	35	100-300	1	1	1	1	1.00
Exfiltrate C2	25	100-300	1	1	1	1	1.00
Critical Service Destruction	25	900	1	1	1	1	1.00
Critical Service Corruption	75	1200	0	0	0	0	0.00
Determine Decoy	10	-	0	0	13	11	8.00
Break Out of Decoy	10	-	0	0	3	3	2.00
Check File	10	-	0	22	0	22	14.67
Average Action Count			174.00	197.00	187.00	197.00	193.67

Figure 8. Attacker Action Frequency

Defender Action	Cost	Linked Action	Baseline Scenario	Camoflague Scenario	Decoy Scenario	Combined Scenario	Average Deception
Audit Logon Events	15	Exec WinRm Lateral Move, Pass the Hash	9	13	11	16	13.33
Monitor Network Traffic	25	Map Network, Exfiltrate Data, Spearphishing	9	11	12	13	12.00
Check Firewall Alerts	15	Map Network, Exfiltrate Data, Spearphishing, Web Crawl	12	12	14	13	13.00
Audit HIPS Logs	25	Critical Service Destruction, Critical Service Corruption	10	12	12	10	11.33
File Monitoring	20	Search Local Data	10	9	9	9	9.00
Process Monitoring	30	Process Injection, Get Hashes	13	9	13	8	10.00
Isolate Machine	60	Exfiltrate Data	1	0	0	0	0.00
Block IP Address	20	Map Network, Exfiltrate Data, Spearphishing	4	5	6	5	5.33
Enforce Robots.txt	20	Web Crawl	6	6	4	4	4.67
Disable Email Links	25	Spearphishing Link	5	6	6	2	4.67
Disable Admin Account	50	Pass the Hash	3	4	3	4	3.67
Disable User Account	50	Exec WinRm Lateral Move, Pass the Hash, Search Local Data, Get Hashes	5	3	3	2	2.67
Reset Password	20	Get Hashes	6	9	8	6	7.67
Re-Image Machine	90	Process Injection	0	0	0	0	0.00
Create Decoy File Server	150	-	0	0	1	1	0.67
Create Decoy POR	150	-	0	0	1	1	0.67
Change File Name	35	-	0	8	0	9	5.67
Average Action Count			**93.00**	**107.00**	**103.00**	**103.00**	**104.33**

Figure 9. Defender Action Frequency

C. TIMESTEPS AND OBJECTIVE ACCOMPLISHMENT

The results for the amount of timesteps required for the attacker to achieve its objectives are shown in Figures 10–12.

	Baseline	Did Not Finish	Neutral	Increase	Decrease			
Game Number	Attacker Timesteps (Exfiltration)				Attacker Timesteps (Corruption/Destruction)			
	Baseline	Camoflague	Decoy	Hybrid	Baseline	Camoflague	Decoy	Hybrid
1	14	31		31		31		31
2	19	25	25	31	34	32	25	31
3	32	20	25	18	32	37	25	39
4	22	38	32	20	25	38	32	39
5	24	40	23	21	37	40	30	32
6	31	36	27	29	31	36	27	29
7		33	30	22		33	30	
8	32	27	34		32		34	
9	20	28	22	27	36	28	25	27
10	39		22	24	39			30
11	17	34	27	17		34	27	
12	37	36	24	20	37	36	40	40
13	20		19	31			33	31
14	15	26	20		31		40	
15	24	40	27	19		40	27	
16	29	21	25		29	38	38	
17	26	28	33	18	36		33	36
18	21	39	18	33	31	39	25	33
19	21	24	34	33	35	35	34	33
20		40	17	21		40		36
21	34	23	15	16	34			31
22	18	14	16	23	27		40	36
23	17	25	23	29	25		33	29
24	28		25	39	30			39
25	21	36	32	31	33	36	32	31
26	19	17	19	27		37	30	
27	25	17	38	18	28	39	38	35
28	17		35	23	32		35	32
29	33		15	31	33		36	31
30	39			31	39			31
31	24	16	15	33			30	33
32	29	13	21	19	29		32	
33	23				39			
34	26	22						
35	39	20	38	35	39	32	38	35
36	27			15	27			28
37	20	16	22	36	26	28	38	36
38	26	27	26	37	29	27	26	37
39	30		21	30	30		40	30
40	32	14	35		32	30	35	
41	33		38	19	33		38	37
42	29		17	19	29		32	

Figure 10. Timesteps Part 1

43	25	15	15	22	25	25	34	30
44	15	23	31			26	31	
45	20	18	16	15	34	31	36	37
46	24		29	21	25		29	27
47	33	17	17	15	33	37	25	
48	24		21	40	38		27	40
49	23	35	16	20	33	35		
50	32	26		34	32	26		34
51	15	36	16	31	28	36	25	31
52	22	26	22	25	29	32		32
53	20	18	18		34	30	31	
54	22	34	21			34		
55	15	21	13	30		37	31	30
56	24	25	25	33		37	25	33
57			35	24			35	36
58	30	17			30			
59	15	26	38	15	34	33	38	40
60	24	22	16		29	34	39	
61	40	16	25	29	40	27	25	29
62	34		26		34			
63	22	35		26	30	35		
64	21	40	34	29	37	40	34	29
65	22	24	14	14	35		33	32
66	16	30	27	30	33	30	27	30
67	38	27	32	30	38		32	30
68	16		40	22	25		40	32
69	20	30	24	20	33	30	33	37
70	16	39	20		32	39	35	
71	37	36	22	26	37	36	32	30
72	38		30		38		30	
73	15	16	37	16	38	32	37	
74	26	16	34	30	37	30	34	30
75	20	29	32	16	36	29	32	
76	23		15		30			
77	27	37		33	31	37		33
78	28		39		28		39	
79			38	27			38	27
80	35	15	34		35	25	34	
81	39	38	38	15	39	38	38	
82	26	18	22		35	37		
83		29	20			29		
84	20	15	17	27		38	27	
85	29	18	40	34	29	25	40	34
86	30	27	21	31	30	31	31	31
87	23			36				36

Figure 11. Timesteps Part 2

88	36		16	22	36			39
89	33	30	26	32	33	30	34	32
90	15	40	18	13	39	40		25
91	24	22		20	34			34
92	24		37				37	
93	36	22	29	21	36		29	
94	26	24	17	37				37
95	23	38	14			38	33	
96	16	26	15	15	37	33	35	38
97	26		32	26	26		32	
98	20	28	14	20		28		34
99	31	19	25	25	31	33		25
100	16	33	23	33	29	33	39	33
Avg	25.28	26.34	25.07	25.39	32.62	33.48	32.79	32.89
Success Percent	95	76	89	79	78	61	73	64

Figure 12. Timesteps Part 3

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Bell, J. B., & Whaley, B. (1991). *Cheating and deception*. Transaction Publishers.

Cayirci, E., & Ghergherehchi, R. (2011, December). *Modeling cyber attacks and their effects on decision process*. *In Proceedings of the 2011 Winter Simulation Conference* (WSC) (pp. 2627–2636). IEEE.

Ferguson-Walter, K. J., LaFon, D. S., & Shade, T. B. (2017). *Friend or faux: deception for cyber defense*. Journal of Information Warfare, 16(2), 28–42.

Ferguson-Walter, K., Shade, T., Rogers, A., Trumbo, M. C. S., Nauer, K. S., Divis, K. M., ... & 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).

Gartzke, E., & Lindsay, J. R. (2015). *Weaving tangled webs: Offense, defense, and deception in cyberspace*. Security Studies, 24(2), 316–348.

Han, X., Kheir, N., & Balzarotti, D. (2018). *Deception techniques in computer security: A research perspective*. ACM Computing Surveys (CSUR), 51(4), 1–36.

Heckman, K. E., Stech, F. J., Thomas, R. K., Schmoker, B., & Tsow, A. W. (2015). *Cyber denial, deception and counter deception*. Springer.

Jajodia, S., Subrahmanian, V., Swarup, V., & Wang, C. (2016). *Cyber deception* (Vol. 6). Springer.

Joint Chiefs of Staff. (2018). *Cyberspace Operations (JP 3-12).* https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Joint Chiefs of Staff. (2017). *Military Deception (JP 3-13.4).* https://jdeis.js.mil/jdeis/new_pubs/jp3_13_4.pdf

Latimer, J. (2003*). Deception in War: Art bluff value deceit most thrilling episodes cunning mil hist from the trojan*. Abrams.

Lindsay, J. R., & Gartzke, E. (2016). *Coercion through cyberspace: the stability-instability paradox revisited*. The Power to Hurt: Coercion in Theory and in Practice, 176–204.

Liu, Z., Li, S., He, J., Xie, D., & Deng, Z. (2012, December*). Complex network security analysis based on attack graph model*. In 2012 Second International Conference on Instrumentation, Measurement, Computer, Communication and Control (pp. 183–186). IEEE.

Liu, P., Zang, W., & Yu, M. (2005). *Incentive-based modeling and inference of attacker intent, objectives, and strategies*. ACM Transactions on Information and System Security (TISSEC), 8(1), 78–118.

Miah, M. S., Gutierrez, M., Veliz, O., Thakoor, O., & Kiekintveld, C. (2020, January). *Concealing cyber-decoys using two-sided feature deception games*. In HICSS (pp. 1–10).

The MITRE Corporation. (2020) MITRE ATT&CK. https://attack.mitre.org/

Monroe J. D. (2012). *Deception: Theory and practice*. Calhoun: The NPS Institutional Archive. http://hdl.handle.net/10945/7388

Rowe, N. C., & Rothstein, H. S. (2004). *Two taxonomies of deception for attacks on information systems*. Journal of Information Warfare, 3(2), 27–39.

Rowe, N. C., & Rrushi, J. (2016). *Introduction to cyberdeception*. Berlin: Springer International Publishing.

Schneider, J. (2019). *The capability/vulnerability paradox and military revolutions: implications for computing, cyber, and the onset of war*. Journal of Strategic Studies, 42(6), 841–863.

SoarTech Inc. (2017). https://soartech.com/cyberspace/

Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press.

Wang, C., & Lu, Z. (2018). *Cyber deception: Overview and the road ahead*. IEEE Security & Privacy, 16(2), 80–85.

Wright, D. *"Deception in the desert,"* accessed (July 11, 2020), https://www.armyupress.army.mil/Books/Browse-Books/iBooks-and-EPUBs/Deception-in-the-Desert/.

Wright, M., Wang, Y., & Wellman, M. P. (2019, June). *Iterated deep reinforcement learning in games: History-aware training for improved stability*. In EC (pp. 617–636).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California