The Art of Deception
for Implementing Practical Cyber Resiliency

by **Roisin Dunn**

Abstract

In view of the sophistication, adaptiveness and persistence of cyber attacks, the current philosophy of trying to keep the adversaries out is no longer valid. Changing our current mindset to assume the adversary will breach defenses and preparing to "fight through" cyber attacks can ensure mission/business operation continuity. Cyber resiliency enables the "fight through" capability and provides transformational improvements by helping to reverse adversary advantage, minimize exploit impact to essential operations, increase adversary cost and uncertainty, and act as a deterrent. Cyber Deception, an emerging resiliency technique, provides an approach to defending systems against attacks without requiring detection of adversary activities. In addition, deception techniques provide valuable insight into current adversary targets and techniques, tactics, and procedures (TTPs). Although the instantiation of cyber deception capabilities within an organization can be challenging and controversial, there is little doubt regarding its benefits in an organization's security posture. This paper explores cyber deception as a practical cyber resiliency technique, overviews deception approaches, provides an implementation use case and presents current deception technologies.

Contents

1 Introduction

The Advanced Persistent Threat (APT) continues to wreak havoc on our systems and infrastructures. They are stealthy and persistent in their mission to infiltrate, steal information, and disrupt; creating chaos and ultimately halting operations within our cyber ecosystems. Preventing cyber adversaries from breaching defenses and gaining entrance to our ecosystem is a strategy prone to failure; we must make the job of the APT more difficult, costly or time consuming by enabling 'fight through' capabilities for continuing operation even if in a degraded state. Cyber Resiliency provides strategies and techniques for ensuring critical capabilities continue, despite successful attacks; it is an essential element of an overall defensive strategy for our cyber ecosystem.

Cyber deception, a key aspect of cyber resiliency, focuses on deliberately confusing the adversary so that their perceptions and decisions are influenced in favor of the defender. This confusion drives-up the cost to the APT by increasing their time and disrupting their assumptions. This paper explores the basics of cyber resiliency and dives into the controversial technique of cyber deception as a practical means of implementing resiliency. It addresses the controversy of deception, maps cyber deception to 800-53 controls and presents frameworks for cyber deception. In addition, it presents example technologies and techniques providing a short use case for demonstrating implementation within a particular domain (i.e., Healthcare, Critical Infrastructure). Finally, the paper provides some challenges, a way ahead for cyber deception in terms of resiliency and concludes by addressing the practicality of deception in terms of resiliency.

1.1 A Motivating Threat Landscape

Today's Advanced Persistent Threat (APT) continues to evolve at a rapid pace. The APT is defined as using a low and slow approach using stealthy, undetected methods. APTs require skill, motivation, and organization; they are well funded human teams focused on compromising defenses, exfiltrating data and maintaining undetected access. According to a 2019 IEEE Communications Surveys & Tutorials [1], the APT has moved from targeting nation states and *their associated entities to include private and corporate sectors. A 2022 threat report from the* European Union Agency for Cybersecurity, (ENISA) [2], states that the current prevalent threats include ransomware, malware, social engineering, threats against data, denial of service, internet availability, disinformation, and supply chain attacks. The Verizon 2022 DBIR Report [3] states System Intrusion (complex attacks that leverage malware and/or hacking to achieve their objectives including deploying Ransomware), continues to be a pattern demonstrated by the APT.

These threat reports indicate a motivating threat landscape; It is clear *existing security measures are inadequate; defenders can not keep pace with APT techniques, tactics, and procedures (TTPs).*

A general APT model suggested by M. Lehto [4] incorporates the tactics from MITRE ATT&CK; it can be used to provide steps and tactics associated with APT activities and deception capabilities. This general APT model is shown in Figure 1.

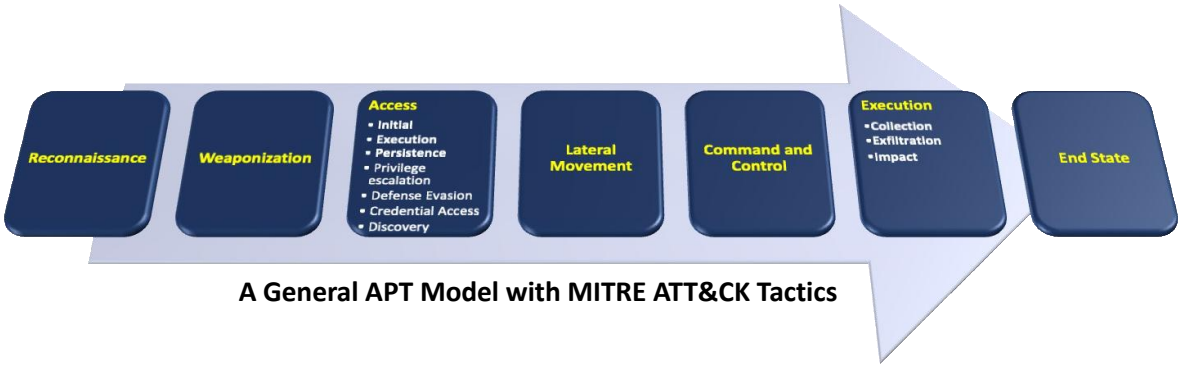

Figure 1. A General APT Model

1.2 Related Work

While significant work has been done separately on cyber resiliency and cyber deception [5-36], less effort has been devoted to bridging these two areas together and developing practical solutions to guide the implementation of cyber deception within the area of cyber resiliency.

2 Cyber Resiliency Overview: Enhancing Continuity in The Face of Attacks

Cyber resiliency provides strategies and techniques for ensuring critical capabilities continue, despite successful attacks; it is an essential element of an overall defensive strategy for our cyber ecosystem. Although different definitions exist for Cyber Resiliency, the definition used by many organizations is defined by the National Institute of Standards and Technology (NIST) as: *The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment*.[8] Whereas traditional strategies focus on keeping adversaries out, resiliency focuses on ensuring critical capabilities continue, despite successful attacks.

Consider the following analogy: a successful soccer team (Team A) has a collection of defensive actions and tactics. Defensive strategies and practice help the team anticipate offensive moves made by the other team (Team B). Defensively, Team A withstands attacks during a game using predetermined strategies but also by adapting to Team B's offensive formations- changing lineups between plays and even changing positions as a play unfolds. In addition, Team A recovers between plays—exchanging players to better defend against the offensive plays being made and replacing injured players. Using lessons learned, the defensive coordinator evolves Team A's defense's strategies and techniques to be better prepared for the next game. For cyber resilience, these defensive strategies are formed through cyber resiliency engineering processes.

These processes are detailed in NIST SP 800-160 V2 where a cyber resiliency engineering framework (CREF) presents a set of Goals, Objectives, Techniques, Implementation Approaches and Design Principles. These are constructed within a framework focused on guiding organizations through the process of implementing cyber resiliency within the context of their cyber ecosystem.

Within the framework, four high level goals; Anticipate, Withstand, Recover and Evolve, help organizations focus on their intended outcome in terms of resiliency. The objectives; Understand, Prepare, Prevent/Avoid, Continue, Constrain, Reconstitute, Transform, Re-architect; are more specific outcomes – focused on measures of effectiveness. Objectives are expressed to motivate assessment; making it easier to develop questions of how well or how quickly the objective can be achieved. The Techniques represent a set of technologies and processes implemented to instantiate or achieve the goals and the objectives. It is not necessary to implement all goals, objectives, techniques, and design principles; each organization uses the framework to determine those aspects of resiliency most important for their specific ecosystem.

The objectives support goals, the techniques support objectives, the approaches support techniques, and the design principles support the realization of the goals and objectives. The goals, objectives, and techniques definitions along with example relationships between the constructs is shown in Figure 2.

As shown, if an organization chooses *Withstand* as a goal, they would be focused on continuing essential functions despite successful execution of an attack by an adversary and their objective could be *Constrain*; limit damage from the adversity. Given this objective, effectiveness might be measured in terms of *How*

long one keeps an adversary in place, how much longer it takes for an adversary to reach its objectives, how much the effectiveness of the adversary attack is limited.. The techniques that could instantiate these goals and objective would be *Non-persistence, Segmentation and Substantiated Integrity*.

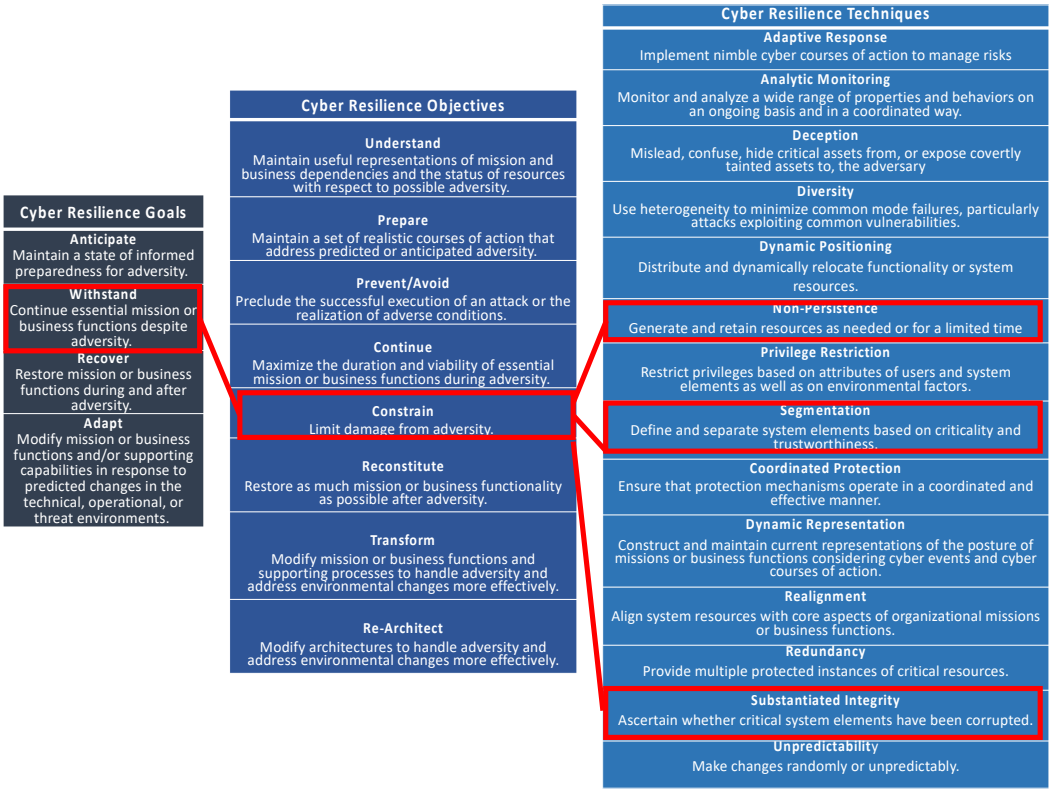

Figure 2. Cyber Resiliency Engineering Framework Goals, Objectives, and Techniques

Effective use of the CREF depends on organizations understanding the concept of resiliency within the context of their specific organization; a Crown Jewels Analysis (CJA) is means of determining this context. Simplified processes for determining appropriate resiliency measures are drawn from NIST SP 800-160 V2 and shown in Table 1 below.

Table 1. Processes For Assessing Cyber Resiliency Measures

STEP	QUESTIONS	POTENTIAL ACTIVITIES
Understand the current context and ecosystem	⇒ What are the concerns and priorities in terms of cyber resiliency capabilities? ⇒ How does the current ecosystem support critical operational capabilities?	⇒ Identify current programmatic, architectural, and operational, and threat context. ⇒ Perform CJA to determine critical services, assets, and operations. ⇒ Prioritize cyber resiliency capabilities given current context.
Establish a baseline	⇒ Does the ecosystem meet needs in terms of cyber resilience?	⇒ Identify existing CR capabilities, determine gaps/issues. ⇒ Define measurement criteria and make initial assessment.
Analyze the system	⇒ How do cyber threats, vulnerabilities and risks affect operations?	⇒ Determine high value assets and services ⇒ Identify attack points within the ecosystem ⇒ Understand and represent the adversary perspective. ⇒ Identify and prioritize enhancements
Define and analyze specific solutions	⇒ How can overall resilience be improved by improving cyber resiliency?	⇒ Define potential technical and procedural solutions. ⇒ Define potential solutions for supporting systems and processes. ⇒ Analyze potential solutions with respect to criteria.
Develop recommendations	⇒ What is the recommended plan of action?	Identify and analyze alternatives. Assess alternatives and recommend an action plan

Changing our current 'build higher, thicker walls' strategy to keep the adversary out is prone to failure. The adversary will be in our systems; their aim is to collect information or disrupt operations; cyber resiliency capabilities focus on keeping operations going despite successful attacks by the adversary. Using the strategies and approaches presented, organizations can implement cyber resiliency approaches to enable continuity of operations. One particularly powerful approach is the implementation of cyber deception.

3 The Art and Science of Cyber Deception

Deception, the art misleading or confusing adversaries, is a strategy used throughout the ages of human history. As noted in Sun Tzu's Art of War he wrote "*All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive.*" [12]. Throughout military history various tactics such as decoys, disinformation, concealment, and camouflage have been employed to provide an advantage to defenders by confusing adversaries and increasing their reaction times. Although deception tactics are centuries old, according to a Cyber Expert Feedback Report [27], the concept of deception for cybersecurity is only decades old; beginning with the idea of implementing basic honeypots to trace intruders by Clifford Stoll (*The Cuckoo's Egg: Tracking a Spy through a Maze of Computer Espionage, 1989).*

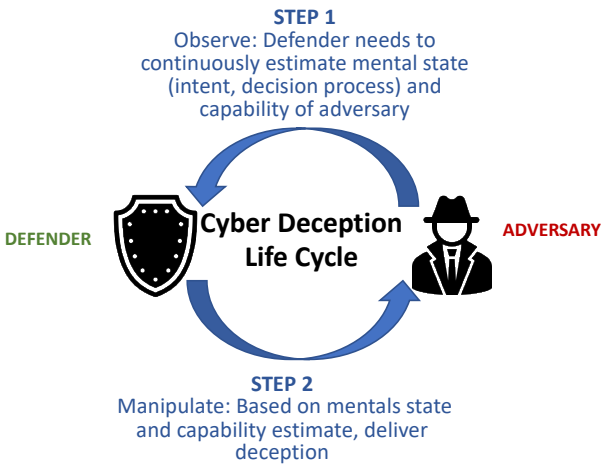

Figure 3. Cyber Deception Lifecycle Concept

Cyber deception, a resiliency technique and proactive defense capability, focuses on reversing the defenders' disadvantages and disrupting the adversaries in in the early stages of their kill chain/APT model. The cyber deception life cycle shown in Figure 3 is a concept presented by Cliff and Lu [13]. Multiple rounds of these life cycle engagements will not only improve the defender's knowledge of the adversary but will allow the defender to adjust deception capabilities. Since the Cliff, Lu study in 2018, the field of cyber deception has evolved; research continues and commercial industry markets, sells and deploys various instantiations of deception technology. Complex TTPs and innovations are widely explored by the research community, and, in time successful research will be productized and move into commercial industry, but, much of this research does not include practical implementation methods.

An examination of cyber deception research shows ongoing studies such as:

⇒ Ghost Patches: Fake Patches for Fake Vulnerabilities - *This approach models the software security patching lifecycle. Patches fix security flaws, but when deployed, can be used to develop malicious exploits. To make exploit generation using patches more resource intensive, they propose inserting deception into software security patches. These ghost patches mislead attackers with deception and fix legitimate flaws in code.* [7]

⇒ Deception-Enhanced Threat Sensing for Resilient Intrusion Detection - *Enhancing standard web services with deceptive responses to cyberattacks can be a powerful and practical strategy for improved intrusion detection. Such deceptions are particularly helpful for addressing and overcoming barriers to effective machine learning-based intrusion detection encountered in many practical deployments*. [14]

⇒ From Patches to Honey-Patches: Lightweight Attacker Misdirection, Deception and Disinformation - *A methodology is proposed for reformulating a broad class of security patches into honey-patches - patches that offer equivalent security but that frustrate attackers' ability to determine whether their attacks have succeeded or failed*. [15]

⇒ Leveraging Computational Intelligence Techniques for Defensive Deception: A Review, Recent Advances, Open Problems and Future Directions - *Computational intelligence provides an appropriate set of tools for creating advanced deception frameworks. Computational intelligence comprises two significant families of artificial intelligence technologies: deep learning and machine learning. These strategies can be used in various situations in Defensive Deception technologies.* [11]

⇒ Artificial Intelligence and Game Theory Models for Defending Critical Networks with Cyber Deception - *Introducing game theory concepts and models to represent and reason over the use of cyber deception by the defender and the effect it has on attacker perception.* [16]

⇒ Resisting Multiple Advanced Persistent Threats via Hypergame-Theoretic Defensive Deception - *In this work, they formulate an attack defense hypergame where multiple APTs attackers and a single defender play a repeated game with different perceptions. The hypergame model systematically evaluates how various DD strategies can defend proactively against APT attacks. They present an adaptive method to select an optimal defense strategy using hypergame theory for strategic defense as well as machine learning for adaptive defense.* [17]

⇒ Cyber Deception Against Zero-Day Attacks: A Game Theoretic Approach – *This study addresses the question of "How to allocate honeypots over the network?" to protect its most valuable assets. To this end, they develop a two-player zero-sum game theoretic approach to study the potential reconnaissance tracks and attack paths that attackers may use*. [18]

Cyber deception pilot studies presented in 'Friend or Faux: Deception for Cyber Defense' by NSA [24], validated cyber deception capabilities. These 2017 studies showed that using decoy systems increase attacker uncertainty regarding what is real and what is slows the attacker and disrupts activities. The study also observed that when a deception environment is employed, adversary TTPs can be observed and valuable intelligence is gleaned; this intelligence is used to adjust and hone defender TTPs.

Since 2017, cyber deception has evolved with companies producing commercial products with impactful deception capabilities such as honeypots, honeynets, masking, mimicking, inventing, repacking, and dazzling. These commercial capabilities, as documented at Lupovis [28] and shown in Table 2 can be implemented in technology and processes.

Table 2. Example Cyber Deception Capabilities

DECEPTION TECHNIQUE	DESCRIPTION
Honeypots	A trap set to detect, deflect, or counteract attempts at your data or unauthorized use of information systems.
Honeynets	A collection of honeypots used to lure attackers away from critica data and systems
Masking	A method to hide legitimate assets or data by making the real data undetectable
Mimicking	Replacing hidden assets with decoys that look real
Inventing	Creating new assets that don't exist but look like they do.
Repacking	Making real assets look as irrelevant as possible
Dazzling	Flooding attackers with so much information they cannot distinguish real from fake.

3.1 Deception, Cyber Resiliency and NIST 800-53 Relationships

When using the CREF detailed in NIST SP 800-160 V2, Deception is defined as the capability to "*mislead, confuse, hide critical assets from, or expose covertly tainted assets to the adversary*." It supports the Objectives of *Prepare/Avoid* and *Understand* and all four Goals within the CREF; with a defined purpose from 800-160 V2 as "*Mislead, confuse, or hide critical assets from the adversary, thereby making the adversary uncertain of how to proceed, delaying the effect of the attack, increasing the risk of being discovered, causing the adversary to misdirect or waste its resources, and exposing the adversary tradecraft prematurely* ". In addition to the current capabilities shown in Table 2, 800-160 V2 details potential implementation approaches and examples for deception; a simplification of this information is shown in Table 3.

Table 3. CREF Related Deception Approaches and Examples

DECEPTION APPROACH	EXAMPLES
Obfuscation: Make information difficult for the adversary to find and understand.	⇒ Encrypt data at rest ⇒ Use steganographic encoding ⇒ Encrypt transmitted data ⇒ Encrypt authenticators ⇒ Randomize communications patterns ⇒ Conceal the presence of system components on an internal network. ⇒ Mask, encrypt, hash, or replace identifiers ⇒ Obfuscate traffic via onion routing ⇒ Apply chaffing to communications traffic ⇒ Add a large amount of valid but useless information to a data store ⇒ Perform encrypted processing.
Disinformation: Deceive adversaries	⇒ Post questions and false information to a public forum about the system ⇒ Create false credentials and honey tokens
Misdirection: Direct adversary activities to deception environments or resources	⇒ Establish and maintain honeypots, honeynets, or decoy files ⇒ Maintain a full-scale, deception environment
Tainting: Make whatever adversaries steal identify those adversaries or harm them	⇒ Use beacon traps ⇒ Employ internal network table cache poisoning ⇒ Include false entries or steganographic data in files to enable them to be found via open-source

NIST SP 800-53 Rev 5, Security and Privacy Controls for Information Systems and Organizations, is a security and compliance framework containing recommended security and privacy controls for federal information systems and other organizations. Although 800-53 was designed for federal agencies it is adopted by many other organizations looking for best practice security and privacy controls. Derived from 800-160, Table 4 provides an example list of the controls covered by approaches.

Table 4. Deception-related Controls of 800-53

Control No. and Name	Deception Technique/Approach
CP-9(8) System Backup - Cryptographic Protection	Deception/ Obfuscation
AI-3(1) Device Identification And Authentication |Cryptographic Bidirectional Authentication	Deception/ Obfuscation
SC-7(16) Boundary Protection | Prevent Discovery Of System Components	Deception/ Obfuscation
SC-8(1) Transmission Confidentiality and Integrity | Cryptographic Protection	Deception/ Obfuscation
SC-8(4) Transmission Confidentiality And Integrity | Conceal Or Randomize Communications	Deception/ Obfuscation
SC-26 Decoys	Deception/Misdirection
SC-28(1) Protection of Information At Rest | Cryptographic Protection	Deception/ Obfuscation
SC-30 Concealment and Misdirection	Deception/Obfuscation/Misdirection
SC-30(4) Concealment and Misdirection| Misleading Information	Deception/Disinformation
SC-30(5) Concealment and Misdirection | Concealment of System Components	Deception/ Obfuscation
SC-35 External Malicious Code Identification	Deception/Misdirection
SC-44 Detonation Chambers	Deception/Misdirection
SI-19 De-Identification | Differential Privacy	Deception/Obfuscation
SI-20 Tainting	Deception/Tainting
SR-5 Acquisition Strategies, Tools, and Methods	Deception/Obfuscation

3.2 Deception-Related Frameworks

Currently, various Deception-related frameworks are evolving within research projects and initiatives; examples of this work are demonstrated by Jafarian, H. and Niakanlahiji, A. [29] and Li, H. and Guo, Y [30]. Since these proposed frameworks exist within a body of research, it is assumed that it will quite some time before these could become practice. Additionally, Kristen Heckman addresses the idea of an abstract framework within her book "Cyber Denial, Deception and Counter Deception" [19] but, to-date, this has not been substantively implemented in practice.

Several frameworks already mentioned such as NIST SP 800-160 and NIST SP 800-53 address some high-level aspects of cyber deception. Although these frameworks are quite practical and used extensively in the community, the guidance is not geared specifically towards cyber deception. In addition, although MITRE ATT&CK does not specifically address deception, aspects of deception are mitigation suggestions for some ATT&CK TTPs.

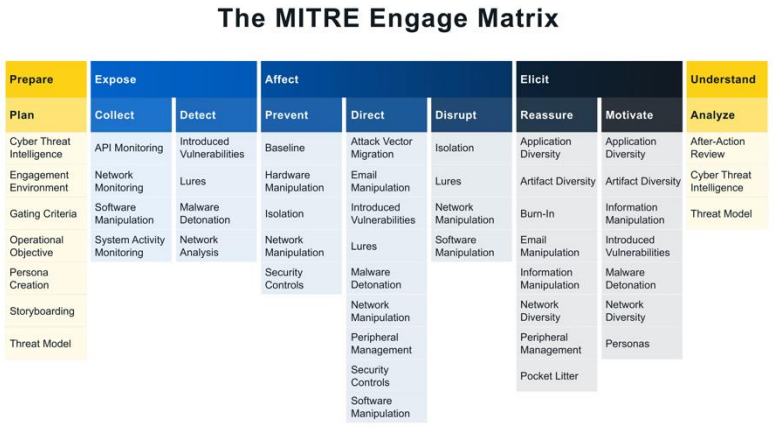

Figure 4. MITRE Engage Matrix from engage.mitre.org

Over the past several years, MITRE developed and launched the MITRE Engage Framework (https://engage.mitre.org) for planning and discussing adversary engagement activities (i.e., deception activities). The framework consists of a matrix, a series of tools (e.g., guides, mission essential task list template, etc.) geared to educate and arm defenders for implementing cyber deception into their cyber defense arsenal. The matrix, shown in **Error! Reference source not found.**, consists of high-level goals, approaches, and activities. [31] In addition, although MITRE D3FEND (https://d3fend.mitre.org) is not formally a framework, it is a knowledgebase of cybersecurity countermeasures with one countermeasure area focused on Deceive with specifics on decoy environments and decoy objects.

3.3 Metrics for Cyber Deception

Successful implementation and use of technology, process or tactics is dependent upon the measurement of effectiveness or performance of that capability. Metrics are measures that are quantifiable and can be challenging in cybersecurity and cyber deception. Ongoing research studies such as those presented by Al amin, Shetty and Kamhoua [32], focus on providing mathematical formulas to calculate defender and attacker metrics. Others, such as those developed by Bodeau, Graubart [33] can be a combination of qualitative and quantitative such a) *The Number of external venues in which misleading or false information is presented* or b) *Percentage of external communications which are encrypted*. Other forms of measurement such as a) *Time between the receipt of threat intelligence and the determination of its relevance,* or b) *Adversary dwell time in deception environment,* are also measured. While metrics for deception can be difficult, they could be measured simply by simply answering a few questions such as:

- ⇒ Is the cyber deception capability providing useful threat intelligence? Are defenders able to observe attackers and better understand their behaviors?
- ⇒ Did attacker dwell time decrease or were we able to detect the attacker earlier in their lifecycle?
- ⇒ How long was the adversary engaged in the deceptive environment?

These are examples of the types of metrics or measures used by commercial vendors producing cyber deception technologies. To answer these questions, commercial products are tested in cyber range and war gaming environments with red (adversary) and blue (defender) teams performing logged activities. Questions regarding defender performance, adversary engagement, etc. are answered by analyzing after action activity logs for both teams.

3.4 Current Cyber Deception Technologies

Growth of both commercial and open-source cyber deception technologies is increasing rapidly. Robust research over the several decades produced a healthy selection of technologies, platforms, and processes across the market. Deception technologies can be appliance based, token based, and enterprise level based. The commercial tools are comprehensive and have a developed customer service, ease of deployment and other advantages; disadvantages include high startup costs and some lack of flexibility. Open-source tools are available and while they are less costly, they require expert customization which leads to hidden operations costs and the potential for open-source projects to be canceled. A sampling of open source tools includes: DejaVu, canarytokens, Thug, DCEPT, and Dionaea. As noted in the previous section, multiple resources are available for no cost at engage.mitre.org

Currently, per CSOonline, some of the top deception technologies available commercially are **Acalvio ShadowPlex, Attivo ThreatDefend Deception and Response Platform, Illusive Shadow, CounterCraft Cyber Deception Platform, Fidelis Deception platform, and** TrapX DeceptionGrid (CommVault). [34]

Cyber Deception technologies and capabilities are now available and can be implemented when organizations have the time, skill, and financial resources. They are a powerful tool in the cyber resiliency toolbox.

3.5 Cyber Deception Use Case

The Healthcare sector faces multiple cybersecurity concerns; from ransomware to medical device monitoring. Enabling the security of medical devices such as drug infusion pumps, patient monitors, x-ray scanners is of the utmost importance to patients, the medical staff, and the healthcare business itself.

To demonstrate the utility of deploying a cyber deception capability within a healthcare facility such as a hospital, consider the organization is focusing on patient safety and providing error-free monitoring of patient care devices. To implement resiliency, we consider that the attacker has already breached perimeter defenses (cyber resiliency defined as the attacker is already inside). Medical devices present difficulties for maintaining a regular patching routine; this makes them vulnerable and a high value target for the adversary.

Consider the following cyber resiliency implementation of deception. If for example, decoy medical devices were installed on the same network as the real medical devices; an adversary would have a difficult time distinguishing the real devices from the decoy devices. If the decoys were configured in such a way as to alert the defenders when they are 'touched' then the defender could recognize adversary activity during the reconnaissance phase and entice them into engagement; this capability would provide quick detection and identification. In addition, if fake credentials to lead to the decoys were created; it would allow defenders to have better visibility into adversaries accessing critical capabilities and data. [35]

This use case demonstrates the powerful impact of implementing cyber deception capabilities to enhance patient safety and protect sensitive data.

4 Conclusion

Although cyber deception capability deployment shows clear defense benefits, due its complexity, many organizations hesitate to implement this powerful cyber resiliency capability. Implementing deception capabilities requires an organization with deep technical skills and an understanding of the organization's operations, the associated services and assets and an understanding of the adversary attack vectors. It is resource intensive to purchase, deploy, manage, and understand the cyber deception capabilities. For organizations with limited resources, it may not be a practical resiliency solution; but, with planning, and strategic actions, the benefits would out-weigh the costs.

The future of cyber deception is bright as the abundance of research moves into practical solutions. One area that should be explored is the effect on adversary behavior when deception is a known factor. Will the adversary give up and go away or will they continue in an attempt to determine fake from real? Other areas to explore are the usability of the existing frameworks, the use of artificial intelligence and machine learning in this domain and measurement of effectiveness in automated environments.

This paper explored the basics of cyber resiliency and detailed aspects of cyber deception as a practical resiliency implementation. By understanding cyber deception 800-53 controls, current frameworks for cyber deception and example technologies we can understand the practicality of implementing this resiliency capability. The simple use case provided within the healthcare sector shows how deception can provide a safer environment for patient medical devices.

In conclusion, organizations should consider cyber deception as a powerful resiliency capability that can augment traditional security defenses.

5 Bibliography and Works Cited

1. Pandey, A.B., Tripathi, A., Vashist, P.C. (2022). "*A Survey of Cyber Security Trends, Emerging Technologies, and Threats*". In: Agrawal, R., He, J., Shubhakar Pilli, E., Kumar, S. (eds) Cyber Security in Intelligent Computing and Communications. Studies in Computational Intelligence, vol 1007. Springer, Singapore. https://doi.org/10.1007/978-981-16-8012-0_2
2. ENISA, "*ENSI Threat Landscape 2022*", November 2022: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
3. Verizon, "*Verizon 2022 Data Breach Investigations Report*", 2022
4. M Lehto, "*APT cyber-attack modelling - building a general model*", Proceedings of the 17th International Conference on Information Warfare and Security, 2022
5. Mohan PV, Dixit S, Gyaneshwar A, Chadha U, Srinivasan K, Seo JT. "*Leveraging Computational Intelligence Techniques for Defensive Deception: A Review, Recent Advances, Open Problems and Future Directions*". *Sensors*. 2022; 22(6):2194. https://doi.org/10.3390/s22062194
6. Alshamrani, Adel, et al. "*A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities*." IEEE Communications Surveys & Tutorials 21.2 (2019): 1851-1877. ." n.d.
7. Avery, j., Spafford, E.J. "*Ghost Patches: Fake Patches for Fake Vulnerabilities*." n.d.
8. National Institute of Standards. "*NIST Special Publication 800-160 Volume 2, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*." Publication. 2021.
9. Neil C. Rowe, Juliann Rrushi. "*Planning Cyberspace Deception*." Springer, Cham, 2016.
10. Pandey, A.B., Tripathi, A., Vashist, P.C. (2022). "*A Survey of Cyber Security Trends, Emerging Technologies, and Threats.*" In: Agrawal, R., He, J., Shubhakar Pilli, E., Kumar, S. (eds) Cyber Security in Intelligent Computing and Communications. Studies in Computational Intelligence, vol 1007. Springer, Singapore. https://doi.org/10.1007/978-981-16-8012-0_2
11. Mohan, Pilla Vaishno et al. "*Leveraging Computational Intelligence Techniques for Defensive Deception: A Review, Recent Advances, Open Problems and Future Directions*." *Sensors (Basel, Switzerland)* vol. 22,6 2194. 11 Mar. 2022, doi:10.3390/s22062194
12. Sun Tzu, "The Art of War"
13. C. Wang and Z. Lu, "*Cyber Deception: Overview and the Road Ahead*," in *IEEE Security & Privacy*, vol. 16, no. 2, pp. 80-85, March/April 2018, doi: 10.1109/MSP.2018.1870866.
14. Araujo, F., Ayoade, G., Hamlen, K.W., Khan, L. (2019). "*Deception-Enhanced Threat Sensing for Resilient Intrusion Detection.*" In: Al-Shaer, E., Wei, J., Hamlen, K., Wang, C. (eds) Autonomous Cyber Deception. Springer, Cham. "https://doi.org/10.1007/978-3-030-02110-8_8" https://doi.org/10.1007/978-3-030-02110-8_8
15. Frederico Araujo, Kevin W. Hamlen, Sebastian Biedermann, and Stefan Katzenbeisser. 2014. "*From Patches to Honey-Patches: Lightweight Attacker Misdirection, Deception, and Disinformation.*" In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14). Association for Computing Machinery, New York, NY, USA, 942–953., https://doi.org/10.1145/2660267.2660329
16. Fugate, S., & Ferguson-Walter, K. (2019). "*Artificial Intelligence and Game Theory Models for Defending Critical Networks with Cyber Deception*". *AI Magazine*, *40*(1), 49-62. https://doi.org/10.1609/aimag.v40i1.2849

17. Z. Wan, J. -H. Cho, M. Zhu, A. H. Anwar, C. Kamhoua and M. P. Singh, "*Resisting Multiple Advanced Persistent Threats via Hypergame-Theoretic Defensive Deception*," in *IEEE Transactions on Network and Service Management*, doi: 10.1109/TNSM.2023.3240366.
18. Sayed, M.A., Anwar, A.H., Kiekintveld, C., Bosansky, B., Kamhoua, C. (2023). "*Cyber Deception Against Zero-Day Attacks: A Game Theoretic Approach*". In: Fang, F., Xu, H., Hayel, Y. (eds) Decision and Game Theory for Security. GameSec 2022. Lecture Notes in Computer Science, vol 13727. Springer, Cham. https://doi.org/10.1007/978-3-031-26369-9_3
19. Heckman, K., Stech F, Thomas, R., Schmoker, B., Tsow, A. 2015. "*Cyber Denial, Deception and Counter Deception*"
20. "*A Framework for Supporting Active Cyber Defense*". Springer Cham. "https://link.springer.com/book/10.1007/978-3-319-25133-2" https://link.springer.com/book/10.1007/978-3-319-25133-2
21. Cifranic, N., Hallman, R., Romero-Mariona, J., Souza, B., Calton, T., Coca, G., "*Decepti-SCADA: A cyber deception framework for active defense of networked critical infrastructures, Internet of Things*", Volume 12, 2020,100320, ISSN 2542-6605, "https://doi.org/10.1016/j.iot.2020.100320" https://doi.org/10.1016/j.iot.2020.100320 .
22. Amit Kleinmann[1]Ori Amichay[1] Avishai Wool David Tenenbaum Ofer Bar Leonid Lev, "*Stealthy Deception Attacks Against SCADA Systems*", "https://arxiv.org/pdf/1706.09303.pdf" https://arxiv.org/pdf/1706.09303.pdf
23. Romero-Mariona, J.; Hallman, R.; Kline, M.; San Miguel, J.; Major, M. and Kerr, L. (2016). "*Security in the Industrial Internet of Things - The C-SEC Approach*". In *Proceedings of the International Conference on Internet of Things and Big Data - IoTBD,* ISBN 978-989-758-183-0, SciTePress, pages 421-428. DOI: 10.5220/0005877904210428
24. Ferguson-Walter, K., LaFon, D., & Shade, T. (2017). "*Friend or Faux: Deception for Cyber Defense.*" *Journal of Information Warfare*, *16*(2), 28–42. HYPERLINK "https://www.jstor.org/stable/26502755" https://www.jstor.org/stable/26502755
25. Q. Duan, E. Al-Shaer, M. Islam and H. Jafarian, "*CONCEAL: A Strategy Composition for Resilient Cyber Deception-Framework, Metrics and Deployment*," *2018 IEEE Conference on Communications and Network Security (CNS)*, Beijing, China, 2018, pp. 1-9, doi: 10.1109/CNS.2018.843319
26. C. Wang and Z. Lu, "*Cyber Deception: Overview and the Road Ahead*" in IEEE Security & Privacy, vol. 16, no. 02, pp. 80-85, 2018.
27. Kimberly J. Ferguson-Walter, Maxine M. Major, Chelsea K. Johnson, Craig J. Johnson, Dakota D. Scott, Robert S. Gutzwiller, Temmie Shade, "*Cyber Expert Feedback*: Experiences, Expectations, and Opinions About Cyber Deception, Computers & Security", 2023
28. H. Brice, "*The ultimate guide to cyber deception technology*", "https://www.lupovis.io/the-ultimate-guide-to-cyber-deception-technology/" https://www.lupovis.io/the-ultimate-guide-to-cyber-deception-technology/
29. Jafarian, H., Niakanlahiji, A., "*A Deception Planning Framework for Cyber Defense*", Proceeds of the Hawaii International Conference on System Sciences, 2020, https://core.ac.uk/reader/286030293

30. Li, H., Guo, Y., Huo, S. *et al.* "*Defensive deception framework against reconnaissance attacks in the cloud with deep reinforcement learning*". *Sci. China Inf. Sci.* **65**, 170305 (2022). https://doi.org/10.1007/s11432-021-3462-4

31. The MITRE Corporation, "MITRE Engage", https://engage.mitre.org/ , 2023.

32. M. A. R. Al Amin, S. Shetty, and C. Kamhoua, "*Cyber Deception Metrics for Interconnected Complex Systems,*" *2022 Winter Simulation Conference (WSC)*, Singapore, 2022, pp. 473-483, doi: 10.1109/WSC57314.2022.10015347.

33. Bodeau, D., Graubart, R., Woodill, J. "*Cyber Resiliency Metrics, Measures of Effectiveness and Scoring*", 2018, https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

34. Breeden, J., "*5 Top Deception Tools*", 2022, https://www.csoonline.com/article/3596076/5-top-deception-tools-and-how-they-ensnare-attackers.html

35. Attivo Networks, "*Deception Based Threat Detection For Healthcare*", whitepaper, n.d, https://www.attivonetworks.com/wp-content/uploads/sites/13/documentation/Attivo_Networks-Threat_Detection_Healthcare.pdf

36. Liebowitz, David, et al. "Deception for cyber defence: challenges and opportunities." *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE, 2021