Incorporating Cyber Denial and Deception Capabilities into the Nuclear and Radiological Domains

Chris Spirito[i], Christine Noonan[ii], Gina Lawson[ii], and Charlie Nickerson[i]

(i) Idaho National Laboratory, Idaho Falls, ID 83415
(ii) Pacific Northwest National Laboratory, Richland, WA 99354
{christopher.spirito, charles.nickerson}@inl.gov, {christine.noonan, gina.lawson}@pnnl.gov

Abstract

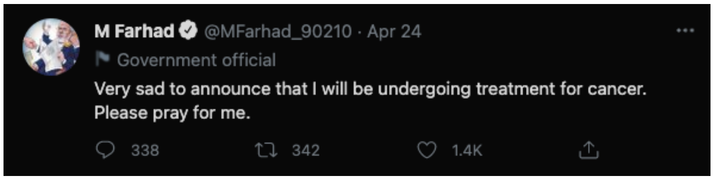
Ensuring the safe operation of elements within the Nuclear and Radiological Domains requires a proven approach to handling the cyber-security risk that is associated with the use of interconnected digital systems. The most common approach to this problem is to implement cyber-security best practices into the design of domain systems and field a cyber-defense capability centered on detection and response to anomalies that may indicate that a cyber-attack has taken place. One capability suite that is not often included within these best practices is *Cyber Denial and Deception (D&D)*, the ability to use the manipulation of facts and fictions to engage with an ever-clever set of cyber actors and prevent them from carrying out their mission objectives against your infrastructure. This paper provides an entry point for those not familiar with the practice of D&D and how these capabilities can be incorporated into the Nuclear and Radiological Domains.

Keywords

Nuclear Energy, Cyber-security, Cyber Denial and Deception

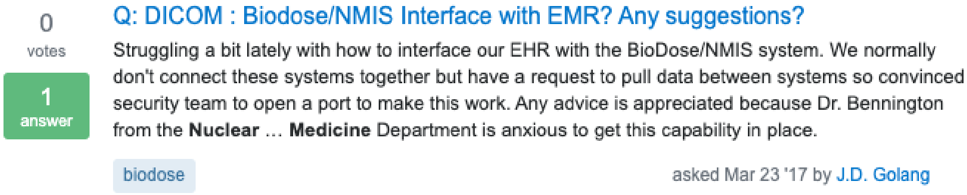
1. An Unusual Contract

You are a contract cyber-mercenary, not the best, but you make a good enough living gaining access to target environments and exfiltrating data under the terms of your shady contract. A new customer has asked you to penetrate and provide access to the computer systems within the Nuclear Medicine department at a Medical Center in Boston, Massachusetts. You recall a few weeks ago a dignitary from another country announcing on Twitter that they were going to undergo treatment for cancer. Not the usual type of account you follow, but he was assigned to you in a University Course to write a short biography on, and you remembered his fondness for Harvard Square while attending the Government Program at the JFK School so many years ago. Probably not related but good to keep in the back of your head.



M Farhad @MFarhad_90210 · Apr 24
Government official
Very sad to announce that I will be undergoing treatment for cancer. Please pray for me.

After agreeing to the contract, you devise your plan of attack and initiate an Open-Source Intelligence (OSINT) search for information about the Medical Center and the types of computer systems and networks usually found within Nuclear Medicine Departments. You find several forum posts on Stack Overflow when searching for ***Nuclear Medicine*** from a Bioengineering Software Developer (***J.D. Golang***) asking about how to interface their Electronic Medical Record system with BioDose/NMIS. The post was quite helpful, especially the information about the security bypass and systems connected, but also a reference to ***Dr. Bennington*** which brings the spear-phishing targets up to two (2).



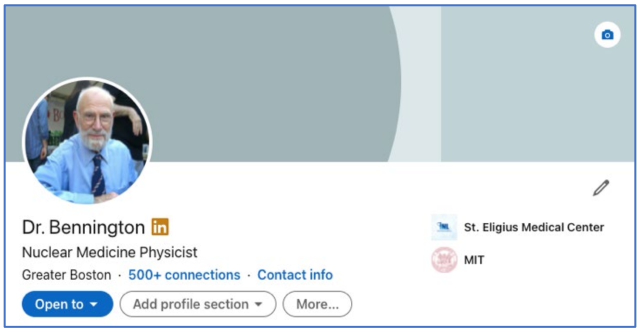
Q: DICOM : Biodose/NMIS Interface with EMR? Any suggestions?

Struggling a bit lately with how to interface our EHR with the BioDose/NMIS system. We normally don't connect these systems together but have a request to pull data between systems so convinced security team to open a port to make this work. Any advice is appreciated because Dr. Bennington from the **Nuclear** ... **Medicine** Department is anxious to get this capability in place.

biodose

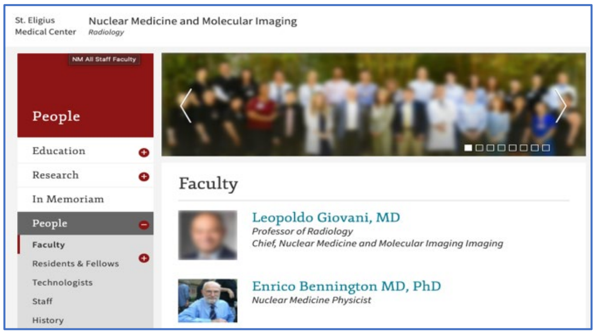
asked Mar 23 '17 by J.D. Golang

Next stop on the reconnaissance tour is LinkedIn to learn more about ***Dr. Bennington***, a Medical Physicist at St. Eligius Medical Center. With a few more searches you find the web page of the Medical Center along with his Email Address.



Dr. Bennington
Nuclear Medicine Physicist
Greater Boston · 500+ connections · Contact info

St. Eligius Medical Center
MIT



St. Eligius
Medical Center

Nuclear Medicine and Molecular Imaging
Radiology

Faculty

Leopoldo Giovani, MD
Professor of Radiology
Chief, Nuclear Medicine and Molecular Imaging Imaging

Enrico Bennington MD, PhD
Nuclear Medicine Physicist

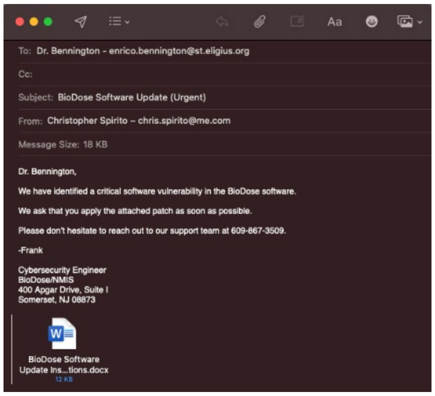
You review the System Requirements for BioDose/NMIS that list *Windows Server 2012, 2016 SP2, 2019 or Windows 10 64 bit* as target Server Operating System options and *Windows 10 64* bit as the target Workstation Operating System. Thankfully you purchased an exploit for Windows 2016 SP2 and looking at the Stack Overflow post you found from 2017 it is possible that their Server Operating System is old and unpatched. You package up your exploit within a Microsoft Word document using a Microsoft Word Remote Code Execution Vulnerability[1] and compose an Email to Dr. Bennington:

Dr. Bennington,

We have identified a critical software vulnerability in the BioDose software.
We ask that you apply the attached patch as soon as possible.

Please don't hesitate to reach out to our support team at 609-867-3509.
-Frank

Cybersecurity Engineer
BioDose/NMIS
400 Apgar Drive, Suite I
Somerset, NJ 08873



To: Dr. Bennington - enrico.bennington@st.eligius.org
Cc:
Subject: BioDose Software Update (Urgent)
From: Christopher Spirito – chris.spirito@me.com
Message Size: 18 KB

Dr. Bennington,

We have identified a critical software vulnerability in the BioDose software.

We ask that you apply the attached patch as soon as possible.

Please don't hesitate to reach out to our support team at 609-867-3509.

-Frank

Cybersecurity Engineer
BioDose/NMIS
400 Apgar Drive, Suite I
Somerset, NJ 08873

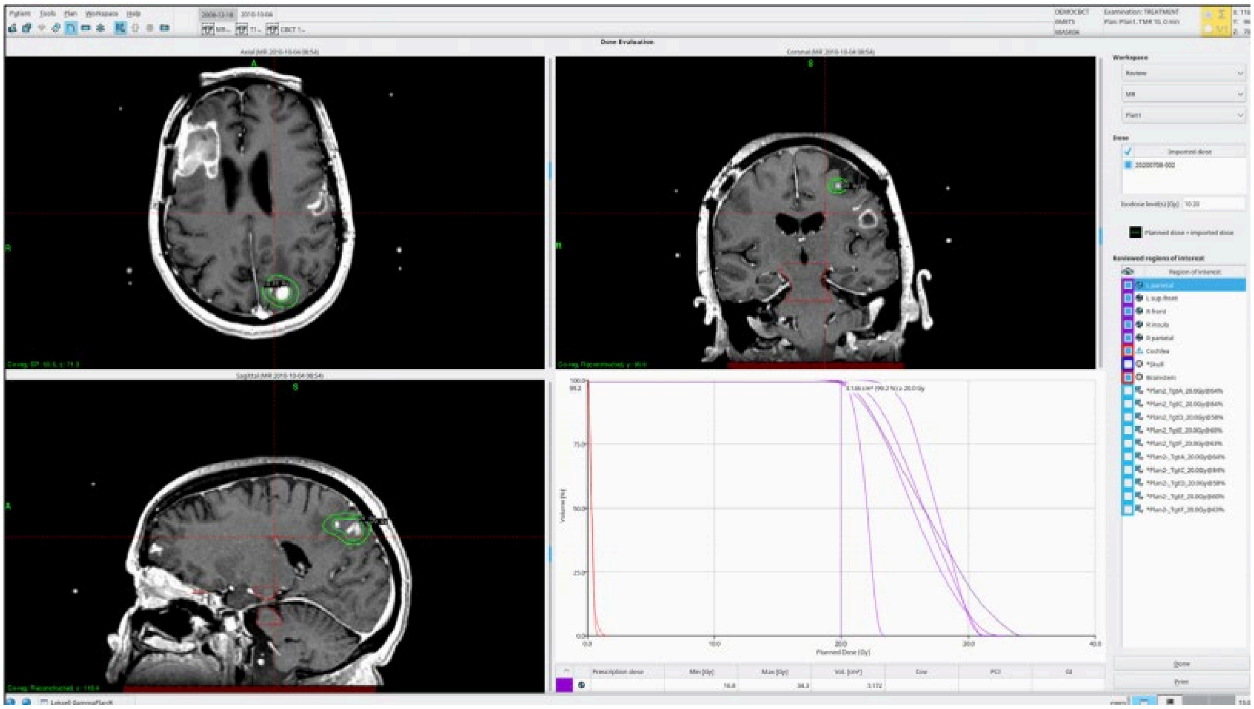
BioDose Software Update Ins...tions.docx
12 KB

You send the Email and the following day one of your Command and Control (C2) servers alerts you that your malware installed the remote access tool and was able to establish a persistent C2 channel for access.

[1] Microsoft Word Vulnerabilities. https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-529/Microsoft-Word.html

Using your remote access tool command menu, you launch a Powershell session on the target system and restart the internal reconnaissance process. Inside the Documents folder you find PDFs related to Nuclear Medicine, some MS Word Documents (including the one you sent) describing Hospital Policies, and an Excel Spreadsheet named *Passwords.xls*. Inside the Excel file is a list of Hostnames, IP addresses, Usernames, and Passwords. The file last modified time is 3 hours ago.

One of the Hostnames is *Leksell GK* and when performing a quick scan of the system you see that the Remote Desktop Port (3389) is open and listening. You create a tunnel to that system and port through the remote access tool over the C2 channel so you can connect to the RDP from your home hacker network. The connection opens, prompting you for the Username and Password. You copy and paste the credentials from the Excel Sheet, logging you into the system and producing a User Interface that reveals itself as the Elekta Leksell Gamma Knife.[2]



At this point you are excited as you can now complete your assignment and provide access to this target environment to your customer and collect your paycheck for a mission accomplished. Except, a few moments later the door of your home is kicked in and you are placed under arrest. As you sit and wait to be interviewed by the arresting agents you start thinking about what could have gone wrong. What happened? Did St. Eligius have a Cyber Denial and Deception Capability?

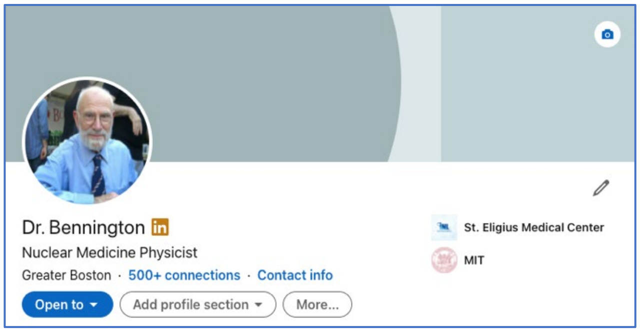
[2] Elekta Leksell GammaPlan. https://www.elekta.com/radiosurgery/leksell-gammaplan/

2. The St. Eligius Cyber Denial and Deception Capabilities

Last year the Chief Information Security Officer at St. Eligius decided that in addition to her traditional cyber-security best practices and incident response capabilities she wanted to develop and implement an Active Defense[3] capability that included Cyber Denial and Deception. During the planning process her team created scenarios that utilized the cyber-attack lifecycle and were reasonable approximations for the types of attacks they believed were plausible against their infrastructure systems and services. One driving principle for establishing these capabilities was to push detection far enough left of hack so that sandbox environments could be leveraged to lure the attacker and observe and engage them long enough for attribution to be possible, working in conjunction with law enforcement partners.

The 67th Attorney General of the United States John Mitchell once remarked, *Watch what we do, instead of what we say*. This became known as the "John Mitchell's Principle" and is associated with the creation of Deceptive Virtual Personas. When we create a virtual persona, we must develop the legend, crafting a history and life story in a process known as *Screenwriting the Legend. Screenwrite the behavior in the legend, then itemize the details needed for the online persona. Instantiate the personal across multiple online domains… and then confirm the fine print on the resume.*[4]

Dr. Bennington is a deceptive virtual persona, created to act as a lure for attackers who may be interested in the Nuclear Medicine department at St. Eligius. The Email address is linked to an alert that is sent to the cyber-security incident response team, triggering a response process that includes deploying additional Cyber D&D capabilities. In this case when the attacker sent the malware, it was subsequently extracted and analyzed in a sandbox, and then executed in a virtual environment that is a realistic representation of the Nuclear Medicine Department, such that a less savvy attacker will be convinced they have arrived at or near their final target.



Dr. Bennington
Nuclear Medicine Physicist
Greater Boston · 500+ connections · Contact info
St. Eligius Medical Center
MIT

When building out the virtual environment the CISO and her team utilized many of the techniques described in the paper *Active Cyber Defense with denial and deception: A cyber-wargame experiment*.[5] One technique they learned about was from the *Blackjack Computer Network Defense (CND) Tool* that was developed and tested as part of a MITRE Cyber D&D experiment. In this experiment attackers are redirected to different versions of a website, crafted to create alternate versions of reality, feeding the attacker information that will mislead them and reinforcing information they have ingested from other sources to provide a sense of confidence over their target environment.

[3] Lachow, Irv. Active Cyber Defense. A Framework for Policymakers. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS_ActiveCyberDefense_Lachow_0.pdf

[4] Cyber Denial, Deception and Counter Deception - A Framework for Supporting Active Cyber Defense. Advances in Information Security 64, Springer 2015, ISBN 978-3-319-25131-8, pp. 1-174

[5] Heckman, Kristin & Walsh, Michael & Stech, Frank & O'Boyle, Todd & DiCato, Stephen. (2013). Active cyber defense with denial and deception: A cyber-wargame experiment. Computers & Security. 37. 72-77. 10.1016/j.cose.2013.03.015.

As the attacker conducted their internal reconnaissance, they found documents that would seem very much at home, medical journal articles about Nuclear Medicine and information about Hospital policies. If he had looked a little harder, he might also have found some network diagrams but how could he not take advantage of the Excel spreadsheet that contained the Hostnames and Passwords. This is what is called in the Cyber D&D domain *pocket litter: blue team documents and artifacts* that should have associated triggers for identifying when they are used. Like the trigger on Dr. Bennington's Email account, for each of the Hostnames, Usernames, and Passwords, if they are used on the designated system or any of the systems in the virtual environment an alert is sent to the cyber defense team that an intruder (attacker) is within the system and can be observed and interacted with.

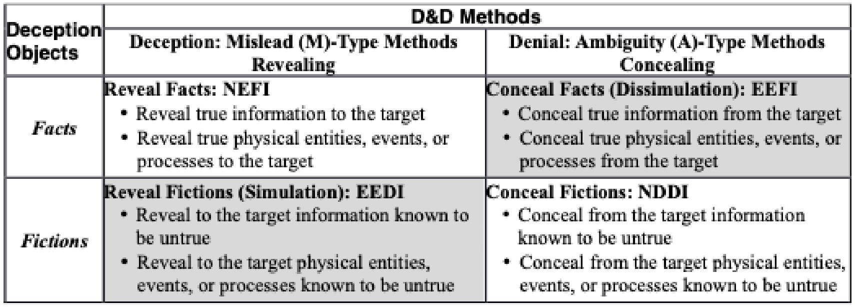
3. Designing and Implementing Cyber Denial and Deception Capabilities

The St. Eligius Cyber D&D capability suite is a good example of how stand-alone or loosely connected capabilities can be implemented in a straight-forward way to improve the probability of earlier detection of adversary behavior against or within your networks and computer systems. As organizations work through their Cyber D&D and Counterdeception development cycles, they will do so utilizing two co-dependent methodologies. The first is a Methods Matrix that classifies the types of artifacts that will be used and the second is a Deception Chain that will implement the artifacts within fielded capabilities.

Denial and Deception Methods Matrix

The Denial and Deception Methods Matrix is divided into four quadrants that map *Deception Objects (Facts and Fiction)* to *D&D Methods (Deception/Misleading and Denial/Concealing).* This matrix was developed by a Team at MITRE and adapted from Edward Waltz and Michael Bennett's book *Counterdeception Principles and Applications for National Security.*

Table 1: D&D Methods Matrix



Deception Objects	D&D Methods	
	Deception: Mislead (M)-Type Methods Revealing	**Denial: Ambiguity (A)-Type Methods Concealing**
Facts	**Reveal Facts: NEFI** • Reveal true information to the target • Reveal true physical entities, events, or processes to the target	**Conceal Facts (Dissimulation): EEFI** • Conceal true information from the target • Conceal true physical entities, events, or processes from the target
Fictions	**Reveal Fictions (Simulation): EEDI** • Reveal to the target information known to be untrue • Reveal to the target physical entities, events, or processes known to be untrue	**Conceal Fictions: NDDI** • Conceal from the target information known to be untrue • Conceal from the target physical entities, events, or processes known to be untrue

Source: Adapted from Bennett & Waltz (2007)

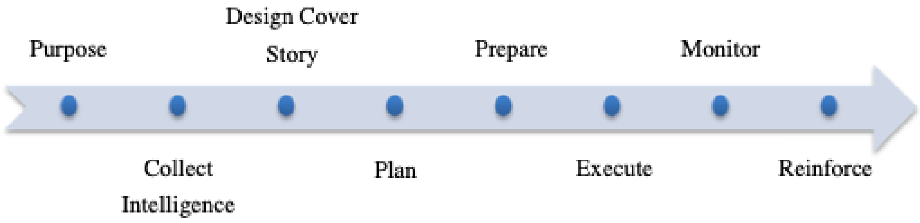
The four types of information are:

- **Non-essential friendly information (NEFI)** are facts that the deceiver reveals to the target.
- **Essential elements of friendly information (EEFI)** are pieces of factual information that the defender Cyber D&D team must protect.
- **Essential elements of deception information (EEDI)** are key fictions that the defender cyber-D&D team must reveal to the target of the deception.
- **Non-disclosable deception information (NDDI)** are fictions that the deceiver must conceal from the target.

We will create these artifacts for use within our deception or counter-deception operation.

Deception Chain

The Deception Chain is a series of steps, similar to the Cyber Kill Chain, that illustrates the phases that a cyber threat actor or defender will work through as they design D&D or Counter D&D capabilities.



To understand the Deception Chain, we can apply it to the capabilities deployed at St. Eligius Medical Center. The CISO defined the **Purpose** for implementing the Cyber D&D program as fielding a capability that pushes detection of cyber adversaries as far left of hack as possible, offering additional time and space for the cyber defenders to position themselves to repel the attacker. The Cyber D&D Team at St. Eligius **Collected Intelligence** and created scenarios that mapped to their organizational concerns, thinking through what their adversary (the cyber attacker) would experience and what their reaction (action) trees would look like. The team then **Designed the Cover Story** for Dr. Bennington and started the **Planning** process to analyze the environmental characteristics to decide what needs to be visible and what needs to be hidden and when those properties change based upon the storyline. The Cyber D&D Team then entered the **Preparation** phase where the information artifacts are created based upon the *Denial and Deception Methods Matrix*. The last three phases of the Deception Chain are implemented in a small cycle with an option to return to previous phases as necessary. The Cyber D&D team will **Execute** the storylines, implement **Monitoring**, and then **Reinforce** any of the storylines as needed. At St. Eligius, the Execute-Monitor-Reinforce actions could have included creating additional deception objects for the attacker to observe on social media that reinforced data that was placed within the virtual environment. Two challenges for Cyber D&D teams are determining how long to allow storylines to play out and ensuring control of their operational environment.

Denial and Deception Tactics and Tools

In the next section we will create Cyber D&D Method Matrixes for a sample set of Nuclear domains to illustrate some of the possibilities, but first let's enumerate some of the D&D Tactics and Tools that we will use when crafting our *Deception Chains*.

Select Tactics[6]
Masking (concealing characteristics)
Repackaging (add/change labels/characteristics)
Dazzling (obscure characteristics)
Red Flagging (obvious display of characteristics)
OPSEC (ensuring discretion in operations)

Select Tools[7]
Anonymizing Proxy
Backdoor Trojan
Clickjacking
Honeypot, Honeynet, Honeytoken
Jamming

[6] For a complete list of Concepts and Tools, please refer to Cyber Denial, Deception and Counter Deception - A Framework for Supporting Active Cyber Defense. Advances in Information Security 64, Springer 2015, ISBN 978-3-319-25131-8, pp. 23-24

[7] Ibid.

4. Cyber D&D Method Matrixes for the Nuclear and Radiological Domains

To better understand how Cyber D&D Methods can be applied within the Nuclear and Radiological Domains to support defensive cyber capabilities, let's create four Cyber D&D Method Matrixes for the following sub domains: Physical Protection, Response, Nuclear Material and Accounting (NMAC), and Transportation Security.

Physical Protection

Deception Objects	D&D Methods	
	Deception: Mislead (M)-Type Methods Revealing	Denial: Ambiguity (A)-Type Methods Concealing
Facts	**Reveal Facts: NEFI** • ***Paltering***: *Publish Wi-Fi camera vulnerability* • ***Feints:*** *Reveal cyber detection capability*	**Conceal Facts (Dissimulation): EEFI** • ***Repackaging***: *GeoIP altered OSINT data* • ***Dazzling***: *Altering environ (pivot-prevention)*
Fictions	**Reveal Fictions (Simulation): EEDI** • ***Decoying:*** *Create Fictional PPS Manager* • ***Mimicking:*** *Fictional PPS Vendor Social Media*	**Conceal Fictions: NDDI** • ***OPSEC:*** *Cyber D&D OPSEC* • ***Delaying:*** *Tarpit deployment on ingress net*

When analyzing Cyber D&D implementations, remember that D&D is centered on interacting with the threat actor. Using traditional cyber defense techniques an organization may observe a threat actor performing actions on their infrastructure using sensors and analytical techniques, but in D&D there is a deliberate attempt to engage the cyber actor to draw them out and place them in controlled environments to observe, engage, and keep them away from operational systems and critical functions.

Implementing Cyber D&D in support of Physical Protection could include publishing Wi-Fi camera vulnerabilities and revealing cyber detection capabilities having already implemented sensors to trigger off actions against these misleading facts that have been revealed (NEFI). Assuming that there will be foreign actors interested in the physical security systems, GeoIP altered OSINT data is fed to visitors to shape their perceptions and lead them to an altered environment, dazzled up to limit and prevent pivoting. Fictional PPS Managers and PPS Vendor Social Media accounts are created as part of the Simulation strategy, all while exercising impeccable OPSEC to ensure that only a small circle within the facility are knowledgeable of these actions since secrecy is paramount to successful Cyber D&D Ops.

Response

Deception Objects	D&D Methods	
	Deception: Mislead (M)-Type Methods Revealing	Denial: Ambiguity (A)-Type Methods Concealing
Facts	**Reveal Facts: NEFI** • ***Paltering:*** *Reveal Guard States (resources)* • ***Negative Spin:*** *Guard Training & Readiness*	**Conceal Facts (Dissimulation): EEFI** • ***Repackaging:*** *Publish Cyber Response Plan* • ***Red Flagging:*** *Publish Honeynet IP Addresses*
Fictions	**Reveal Fictions (Simulation): EEDI** • ***Mimicking:*** *Fictional (expected) response* • ***Decoying:*** *Guard Force Comms Honeypot(net)*	**Conceal Fictions: NDDI** • ***OPSEC:*** *Cyber D&D OPSEC* • ***Positive Spin:*** *Validate Fictional Response Plan*

The Response Cyber D&D plan includes revealing guard states and resources and using negative spin to downplay guard training and readiness. This will be complemented by establishing a Guard Force Communications Honeypot and publishing a fictional cyber response plan and Honeynet addresses. As the threat actor engages, a positive spin action will be undertaken to validate the fictional response plan.

Nuclear Material and Accounting (NMAC)

Deception Objects	D&D Methods	
	Deception: Mislead (M)-Type Methods Revealing	**Denial: Ambiguity (A)-Type Methods Concealing**
Facts	**Reveal Facts: NEFI** • ***Paltering***: *Publish NMAC Team Details* • ***Feint****: Fake Material Information (fictious lab)*	**Conceal Facts (Dissimulation): EEFI** • ***Dazzling****: NMAC binary obfuscation* • ***Masking:*** *Criteria-altered material values*
Fictions	**Reveal Fictions (Simulation): EEDI** • ***Mimicking:*** *Trojan Horse binary infect actor* • ***Inventing:*** *Credential File (dazzle)*	**Conceal Fictions: NDDI** • ***OPSEC:*** *Cyber D&D OPSEC* • ***Delaying****: Encrypting Fictional Password File*

Cyber D&D for NMAC provides a good example of how to implement these methods against a well bounded system and network, especially one in which there is a concern about insider threats. For this scenario we publish details on the NMAC Team and include in a publication details on fake materials from a fictitious lab. Assuming the cyber actor has penetrated the NMAC system or network, a credential file (dazzle) is left out to be discovered along with an infected binary that if installed beacons to a capture service to trigger a response from the incident response team. So as not to make the attack too easy (and less believable), the NMAC software binary is obfuscated, and material values are altered before display based upon pre-set criteria. In this case the dazzle file is encrypted (lightly if you will) to conceal the fiction (NDDI) and implement a delay providing the incident response team additional time to respond.

Transportation Security

Deception Objects	D&D Methods	
	Deception: Mislead (M)-Type Methods Revealing	**Denial: Ambiguity (A)-Type Methods Concealing**
Facts	**Reveal Facts: NEFI** • ***Negative Spin:*** *Publish (Patched) Vulnerability* • ***Feint:*** *Fake RF Signals for Convoy Comms*	**Conceal Facts (Dissimulation): EEFI** • ***Red Flagging:*** *LEA (obf. Transport Details)* • ***Dazzling:*** *Security Container Cyber Details*
Fictions	**Reveal Fictions (Simulation): EEDI** • ***Decoying:*** *Deploy Tracking System Honeynet* • **Double Play:** *Emergency Comms & Dispatch*	**Conceal Fictions: NDDI** • ***OPSEC:*** *Cyber D&D OPSEC* • ***Delaying****: Deploying Beatable Fictional Auth*

The last example we provide is for Cyber D&D and Transportation Security. The methods used for this scenario include publishing details on a patched vulnerability and implement manufactured RF signals for convoy communications. A tracking system honeynet is established with the knowledge that it will likely be one of the high value targets of this subdomain. Law Enforcement is engaged to publish obfuscated transportation details and the physical security container will be dazzled to project an advanced cyber protection capability. In order to conceal the fictional environments created in the EEDI stage, a beatable fictional authentication system will be used to delay the attacker and provide the defender additional time to respond.

5. Conclusion

In this paper we have introduced the concepts of Cyber Denial and Deception within the Nuclear and Radiological Domains. While the complexity of this topic should not be overlooked, and the resource commitment recognized as significant, the overall benefit from even a constrained implementation should not be discounted. We propose to continue this work through the development of a Cyber Denial and

Deception capability suite for Nuclear and Radiological Domains with an associated training and education program to help our partner nations to approach this exciting cyber defensive capability.

Acknowledgements

The authors would like to express appreciation to the U.S. Department of Energy, National Nuclear Security Administration, Office of International Nuclear Security for their support of this work. Idaho National Laboratory is operated by Battelle Energy Alliance for the U.S. Department of Energy under contract DE-AC07-05ID14517. Pacific Northwest National Laboratory is operated by Battelle Memorial Institute for the U.S. Department of Energy under contract DE-AC05-76RL01830.