KEY TERMS

The following key terms are found in one or more MITRE Engage ™ offering. These terms and definitions represent a composite of the terms and definitions commonly used in the adversary engagement community.

Criteria for inclusion in Engage:

- Term is used across multiple papers/textbooks/resources (i.e., usage isn't limited to one source)
  - Except for words that capture a unique concept or summarize a common concept with unique clarity & brevity

- Term specifically deals with adversary engagement or can be applied in an adversary engagement context

Criteria for exclusion:

- Though used in an adversary engagement context, this term does not add any domain-specific knowledge
  - For example: Preconception – an opinion or conception formed in advance of actual knowledge
    While "preconception" may be used within deception communities, the inclusion of this definition would add no domain-specific knowledge, and therefore would contribute to bloat.
  - Other examples include phishing or virus

- Term is shadowed by another term that means the same thing
  - In this case, the less-commonly-used-word may be listed as a synonym of the more-commonly-used-word, but will not be given its own entry

A-Type (Ambiguity-Type) Deception

The purposeful intent to increase ambiguity by surrounding a target with irrelevant information, or to cause confusion based on a lack of certainty. The aim is to keep the target unsure of one's true intentions. A number of alternatives are developed for the target's consumption, built on misinformation that is both plausible and sufficiently significant to cause the target to expend resources to cover it. [1]

After-Action Review

Review of operational activities.

Analysis System

The set of systems used to review and analyze data collected in the collection system.

Anchoring Bias

The tendency to favor first learned or pre-existing information to drive motivation and decision making; for example, the defender needs to have applications on the desktop to cause the attacker to believe they have penetrated a viable target.

Application Diversity

Present the adversary with a variety of installed applications and services.

Artifact Diversity

Present the adversary with a variety of network and system artifacts.

Attack Vector Migration

Move a malicious link, file, or device from its intended location to an engagement system or network for execution/use.

Bait

A type of lure that is intended to draw the adversary's attention towards a specific artifact or system.

Baseline

Identify key system elements to establish a baseline and be prepared to reset a system to that baseline when necessary.

Breadcrumb

A type of lure that leads an adversary in a specific direction.

Burn-In

Exercise a target system in a manner where it will generate desirable system artifacts.

Cognitive Bias

The influence of an individual's subjective view of reality onto their perception of the actual reality.

Collection System

The set of systems used to gather artifacts and other data from an operation to monitor the engagement. Collection systems are necessary for the defender to see, and thus understand, the adversary's actions.

Concealment

Protection from observation or surveillance. [1]

Concept of Operations (CONOP)

A planning document that outlines of assumptions and intent for one or more operations. CONOPs should outline goals, objectives, and methodologies. It must contain the appropriate context to guide team coordination and delegation of responsibilities. CONOPs should also be structured in a way to validate current capabilities and assess their ability to complete the outlined operations. [3]

Contextual Bias

Domain-irrelevant environmental or emotional pressures that influence an individual's observations, interpretations, and inferences. External forces or information can lead an adversary to make incorrect decisions when they fall subject to Contextual Bias.

Counterdeception

The act of detecting, characterizing, and penetrating adversarial deception operations. This includes the process of discerning the adversary's real capabilities and intentions to assess what is real, and to determine what the adversary is trying to make you believe in order to understand what the adversary wants you to do. Counterdeception is characterized by three dimensions of action: (1) awareness; (2) detection and exposure; and (3) discovery and penetration. [1]

Cyber Threat Intelligence

The process of analyzing actionable knowledge about adversaries and their malicious activities, enabling defenders and their organizations to reduce harm through better security decision-making.

Deception

Reveal, conceal, or otherwise manipulate facts and fictions to mislead or confuse an adversary so that behave in a way that is beneficial to the deceiver.

Decoy

A type of lure that imitates a real artifact or system and is intended to divert the adversary's attention, disrupt their reconnaissance efforts, or otherwise move the adversary away from real artifacts or systems.

Defensive Cyberspace Operations (DCO)

Missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. [2]

Demonstration

A show of force where a decision is not sought and no contact with the adversary is intended. A demonstration's intent is to cause the adversary to select an unfavorable course of action (COA). It is similar to a feint but no actual contact with the adversary is intended. See also Diversion. [1]

Denial

Denial is the ability and effort to prevent or impair the collection of intelligence by the enemy. Denial most often involves security and concealment to prevent collection (e.g., by foreign agents, photographic surveillance, electronic monitoring, or even the media) from detecting and collecting information on secretive diplomatic or military matters. [1]

Desired Perception

In military deception, desired perception is what the deception target must believe for it to make the decision that will achieve the deception objective. [1]

Disinformation

The deliberate spreading of false information to mislead the adversary or conceal one's true activities. [1]

Display

The static portrayal of an activity, artifact, or system intended to deceive the adversary's observations. Displays have the opposite objective from concealments in that they are intended to draw the adversary's attention to mislead. Displays often serve to help tell the engagement narrative. [1]

Diversion

The act of drawing the attention and forces of the adversary from the point of the principal operation; an attack, alarm, or feint that diverts enemy attention. See also Demonstration. [1]

Email Manipulation

Modify the flow of email in the environment.

Engagement Environment

Design the systems and network for the operation.

Engagement Narrative

The cover story explaining the fictitious purpose of the adversary engagement environment and how it came to be.

Essential Elements of Deception Information (EEDI)

EEDI are revealed fictions that are an essential basis for creating false perceptions. [1]

Essential Elements of Friendly Information (EEFI)

EEFI are the critical aspects of a friendly operation that, if known by the enemy would subsequently compromise, lead to failure, or limit success of the operation, and therefore, must be protected from enemy detection. [1]

Feedback

Information collected on the friendly and enemy situation that reveals how well the engagement narrative is being portrayed by the friendly side and other channels of cover story information, if the deception target is responding to the deception cover story information and portrayals, and if the deception plan is working to get the adversary to act as desired by the friendly side, thus accomplishing the deception objective. [1]

Gating Criteria

Define the set of events that would lead to the unnegotiable pause or conclusion to the operation.

Hardware Manipulation

Alter the hardware configuration of a system to limit what an adversary can do with the device.

High Value Target (HVT)

Any individual in your organization designated as a priority for internal and external cyber threats.

High Value Technology (HVTC)

Any technology or class of technologies in your organization designated as a priority for internal or external cyber threats.

Honeypot

A type of low interaction, often low fidelity, engagement environment. Uses intentional vulnerabilities to attract adversaries and motivate activity. Has no legitimate use case besides attracting and exposing adversaries.

Honeytoken

False information intended to allow defenders to learn more about a data compromise such as who the data was stolen from, the extent of data stolen, or how it was leaked.

Information Manipulation

Conceal and reveal both facts and fictions to support a deception story

Introduced Vulnerabilities

Intentionally introduce vulnerabilities into the environment for the adversary to exploit.

Isolation

Configure devices, systems, networks, etc. to contain activity and data, thus preventing the expansion of an engagement beyond desired limits.

Lures

Deceptive systems and artifacts intended to serve as decoys, breadcrumbs, or bait to elicit a specific response from the adversary.

M-Type (Mislead-Type)

M-Type, or misleading, deception involves achieving a reduction of ambiguity, as perceived by the intended target, by building up attractiveness of a wrong alternative. This may be more difficult than A-type deception because it requires time and carefully orchestrated resources to build a series of misleading false signals. [1]

Malware Detonation

Execute malware under controlled conditions to analyze its functionality.

Military Deception (MILDEC)

Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions or inactions that will contribute to the accomplishment of the friendly mission. Also called MILDEC. Form of Soviet Active Measures (aktivnye meropriyatiya). Military deception

(maskirovka) includes camouflage, concealment, deception, imitation, disinformation, secrecy, security, feints, diversions, and simulations in aid of attaining military surprise. [1]

Network Analysis

Analyze network traffic to gain intelligence on communications between systems.

Network Diversity

Use a diverse set of devices on the network to help establish the legitimacy of a deceptive network.

Network Manipulation

Make changes to network properties and functions to achieve a desired effect.

Network Monitoring

Monitor network traffic in order to detect adversary activity.

Notional

Adjective that is combined with other terms to indicate false objects or plans the friendly force wishes the opponent to accept as real. Notional describes a false activity or asset used to project the engagement narrative to the adversary. [1]

Operational Objective

Define the objective of the desired end-state of your adversary engagement operations.

Ostrich Bias

Willingness to put away doubts and avoid negative information if there is enough confirmation (bury your head in the sand).

Palter

Acting insincerely or misleadingly or deceiving by manipulation of the truth. Deceptive practices of fudging, twisting, shading, bending, stretching, slanting, exaggerating, distorting, whitewashing, and selective reporting of the truth to serve a deceptive purpose. The palter falls short of being an outright lie in two important dimensions. First, the palter may not be literally false. Second, the typical palter may seem less harmful or deceitful than the typical lie, while creating the same effect as an outright lie. [1]

Passive Deception

Allows a misleading interpretation of facts and fictions to go uncorrected. Passive deception misleads the opponent, preventing (e.g., through Operations Security) any actions that might reveal critical facts and fictions, and thus preventing the opponent from forming correct estimates or taking appropriate actions. Passive deception is primarily based on secrecy and

camouflage, on hiding and concealing one's intentions and/or capabilities from the adversary. [1]

Peripheral Management

Manage peripheral devices used on systems within the network for engagement purposes.

Persona Creation

Plan and create a fictitious human user through a combination of planted data and revealed behavior patterns.

Personas

Create fictitious human user(s) through a combination of planted data and revealed behavior patterns.

Pocket Litter

Data used to support the engagement narrative.

Portrayal

The presentation of artifacts or systems to represent nonexistent artifacts, systems, or activities. Although considered acts in themselves, portrayals usually include disguises and simulations. A form of Display. [1]

Pretexting

The manipulation of a target using an invented scenario with the purpose of performing some advantageous action. Attackers exploit processes of the target organization by contacting employees and posing as someone who should have access to sensitive information. [1]

Rules of Engagement (RoE)

The set of rules representing the actions that an adversary is not permitted to take in the environment or the required monitoring/logging that the analysts are required to maintain.

Ruse

A ruse is a trick of war designed to deceive the adversary, usually involving the deliberate exposure of false information to the adversary's intelligence collection system. A cunning trick designed to deceive the adversary to obtain friendly advantage. It is characterized by deliberately exposing false or confusing information for collection and interpretation by the adversary. [1]

Security Controls

Alter security controls to make the system more or less vulnerable to attack.

Signature Control

The manipulation of a system's emission and physical characteristics, such as network traffic patterns, to reduce an adversary's ability to detect, track, and or otherwise monitor or impact a system or network.

Simulation

The process of revealing fictions, or the essential elements of deception information (EEDI). Projections of objects or systems that do not actually exist. A form of Display. See Essential Elements of Deception Information (EEDI). [1]

Software Manipulation

Make changes to a system's software properties and functions to achieve a desired effect.

Storyboarding

Plan and create the deception story.

System Activity Monitoring

Collect system activity logs that can reveal adversary activity.

Target Adversary (TA)

The adversaries designated or prioritized as the focus for a given operation. This prioritization may be determined because the adversary regularly targets an organization or multiple organizations like the defender's own organization, has historically compromised the defender's organization, represents a gap in the defender's current intelligence, and/or targets employees identified as High-Value Targets (HVTs), or technologies identified as High-Value Technologies (HVTCs).

Threat Model

A risk assessment that models organizational strengths and weaknesses.

Works Cited

1. Heckman, K. E., Stech F. J., Thomas R. K, Schmoker B., & Tsow A. W. (2015). Cyber Denial, Deception, and Counter Deception: A Framework for Supporting Active Cyber Defense. New York: Springer International Publishing.
2. Joint Chiefs of Staff (2018, June 8). Joint Publication 3-12: Cyberspace Operations. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf
3. NIST (2020). Security and Privacy Controls for Federal Information Systems and Organizations. NIST Special Publication (SP) 800-53, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5