Cyber Kill Chains

Adversarial Behaviours

Cyber Kill Chains

Adversarial Behaviours

- **Kill Chains** are a military concept, that are used to determine the anatomy of an attack.
- Researchers and companies have adapted them for cyber security in the form of **cyber kill chains**.
- Cyber kill chains supports organisations and individuals in formulating the **anatomy of an attack** as well as considering defences.

Cyber Kill Chains

Adversarial Behaviours

- Many different forms, the process we are going to consider models a scenario where the attacker identifies, compromises and exploits.
- Model not always optimal for all attacks or adversarial behaviours, need to adapt or utilise another approach.
- Specifically the model is optimal for **intrusions**, arguably for other types of attacks the approach is not optimal.

Phases

Phases

Hutchins *et al.* Cyber Kill Chain Model

Reconnaissance

Cyber Kill Chain Phases

- Attacker determines viable targets to focus energy on. Diverse set of approaches could be used by the attacker:
  - purchase email lists.
  - social media.
  - vulnerabilities in prospective systems (e.g. open ports).

Weaponisation

Cyber Kill Chain Phases

- Development of the payload or instrument to support attack. This could be to develop a new instruction (e.g. programatically) or utilise existing instrument. Examples:
  - potentially insert malware into a benign payload.
  - deactivate controls to deal with malicious payloads.

Delivery

Cyber Kill Chain Phases

- Delivery of the payload or instrument in preparation to exploit vulnerability.
- Attacker could have great weapon, but pointless if unable to deliver it. For example:
  - potentially via USB.
  - email attachment.

Exploitation

Cyber Kill Chain Phases

- Vulnerability exploited within the system.
- Actual payload executes and gains minimum foothold to access target environment.

Installation

Cyber Kill Chain Phases

- Malicious instrument or software downloaded and insert into the machine of the victim.
- Install remote administration software, remote access trojan (RAT).
- May also expand across the network of systems.

Command and Control

Cyber Kill Chain Phases

- Attack establishes contact with the instrument or software and then exerts control across organisation.
- Initiate attack commands or begin exfiltration of data.

Actions on Objectives

Cyber Kill Chain Phases

- Perform objective, this could be profit immediately or extract information to perform other attacks.

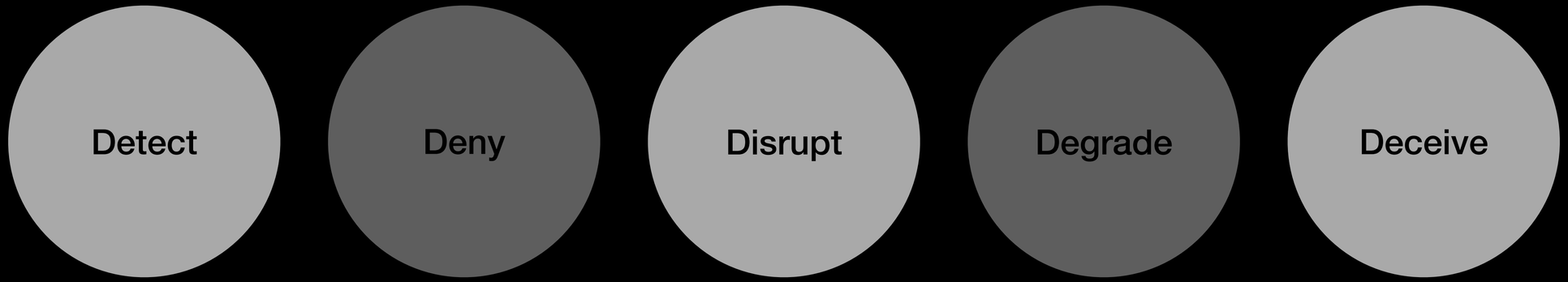
Phases

Hutchins *et al.* Cyber Kill Chain Model

Defensive steps

Defensive steps

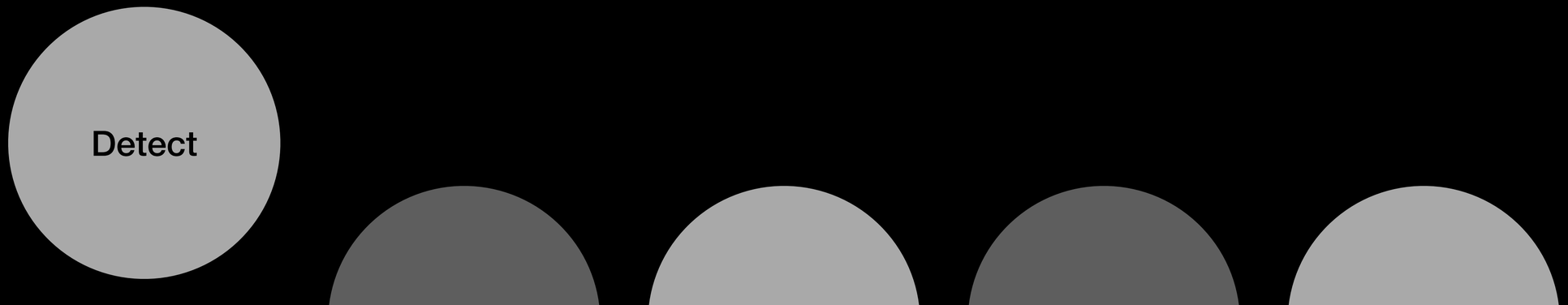
Hutchins et al. Cyber Kill Chain Model



Detect

Hutchins et al. Cyber Kill Chain Model

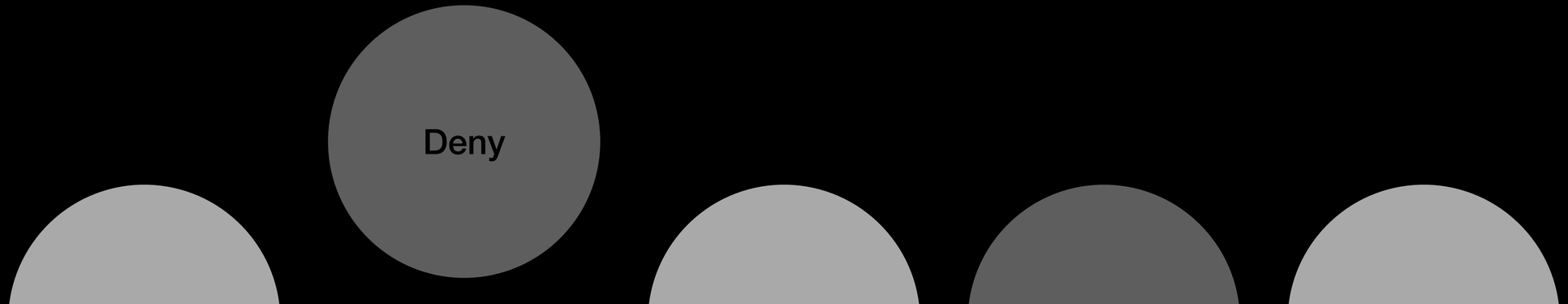
- Identify attackers exploring the network or accessing systems.



Deny

Hutchins et al. Cyber Kill Chain Model

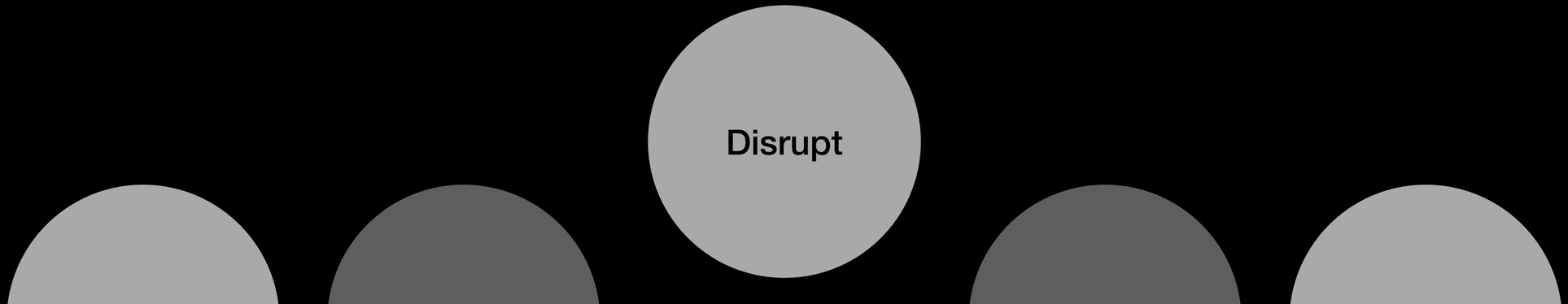
- Attempts to access resources and interference with data.



Disrupt

Hutchins et al. Cyber Kill Chain Model

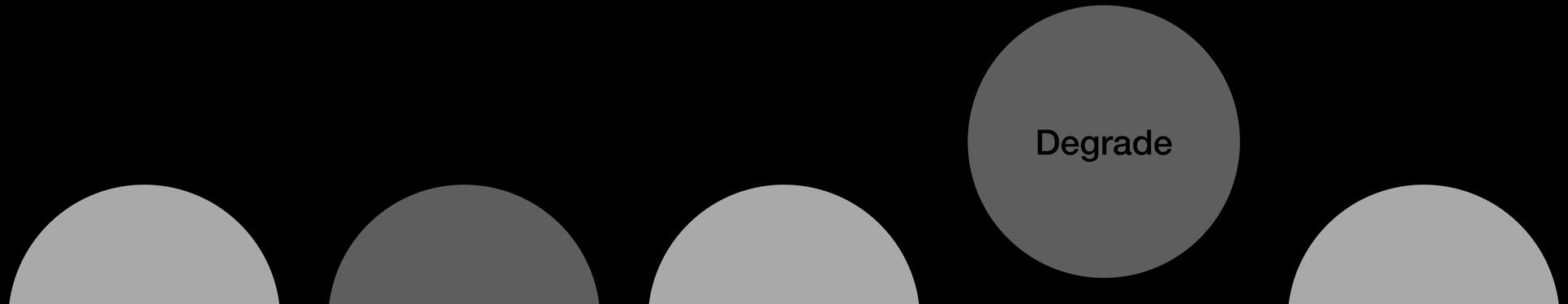
- Any attempt to alter outbound transfer or to transmit data outside organisation if deemed a concern.



Degrade

Hutchins et al. Cyber Kill Chain Model

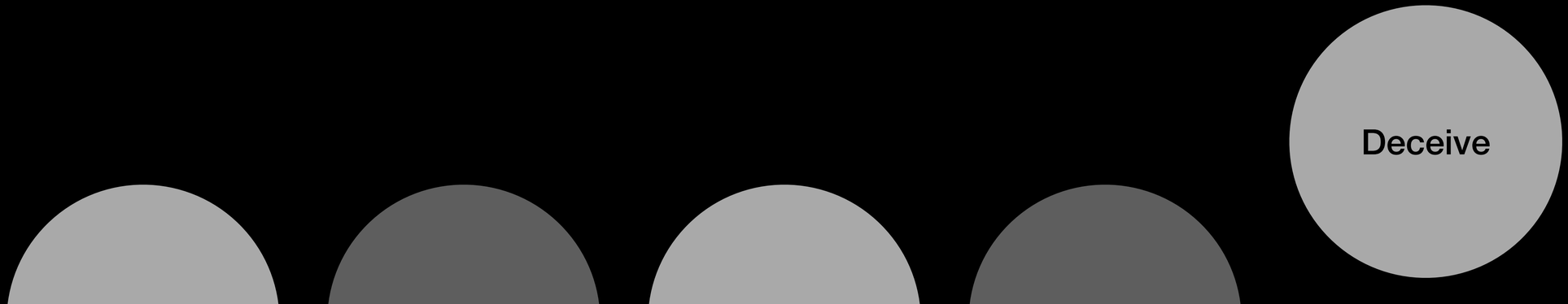
- Attack the structure attacker, attempt to reduce impact on organisation.



Deceive

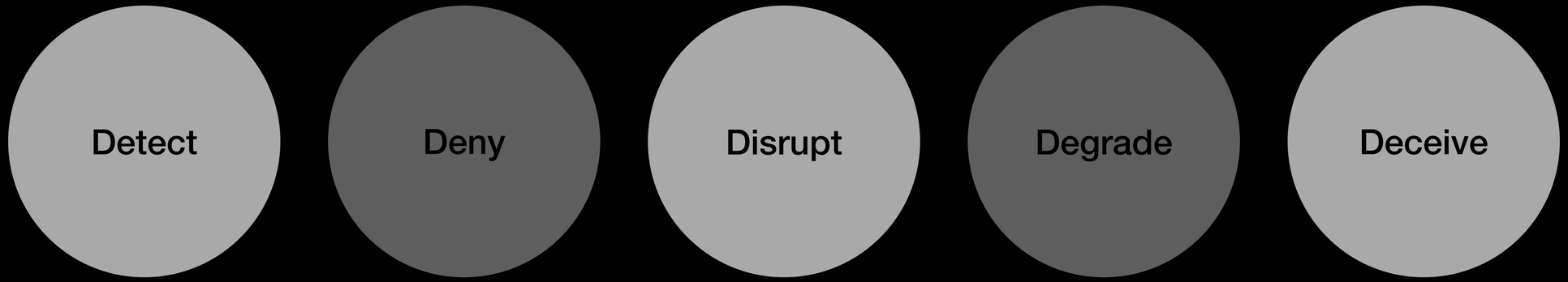
Hutchins et al. Cyber Kill Chain Model

- Interfere with data released in attack to gain deeper insight into attacker.



Defensive steps

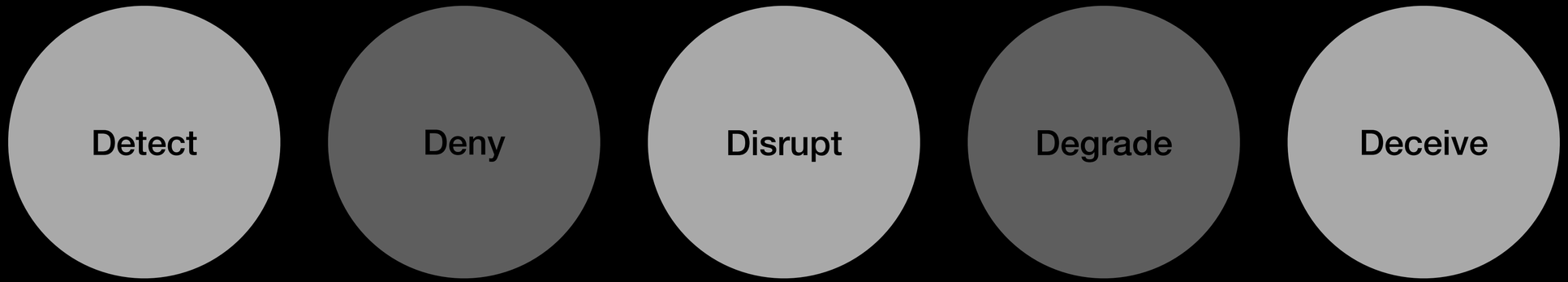
Hutchins et al. Cyber Kill Chain Model



Course of Action (CoA) Matrix

Phases

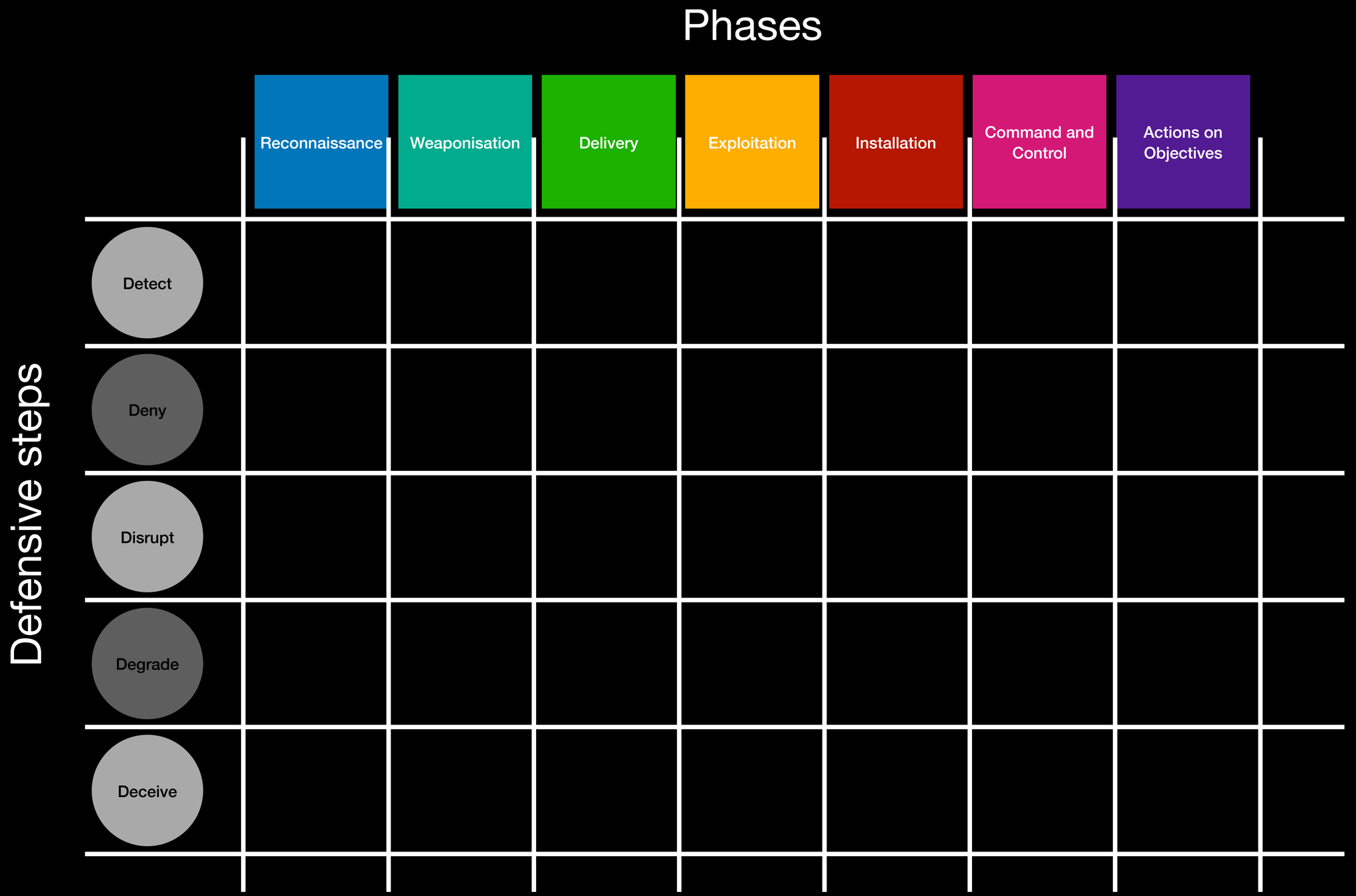
Defensive steps

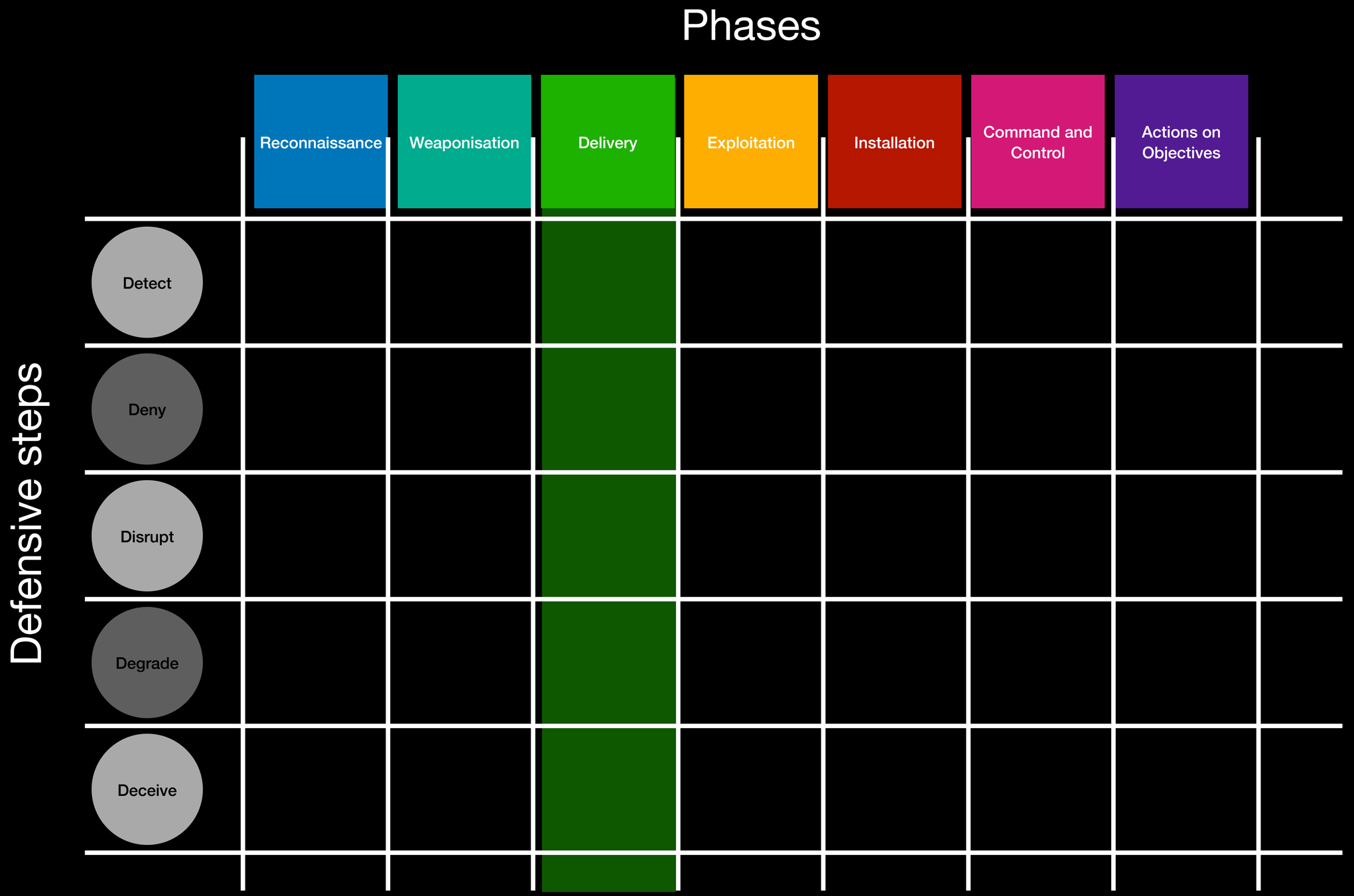


Phases

Defensive steps

- Detect
- Deny
- Disrupt
- Degrade
- Deceive

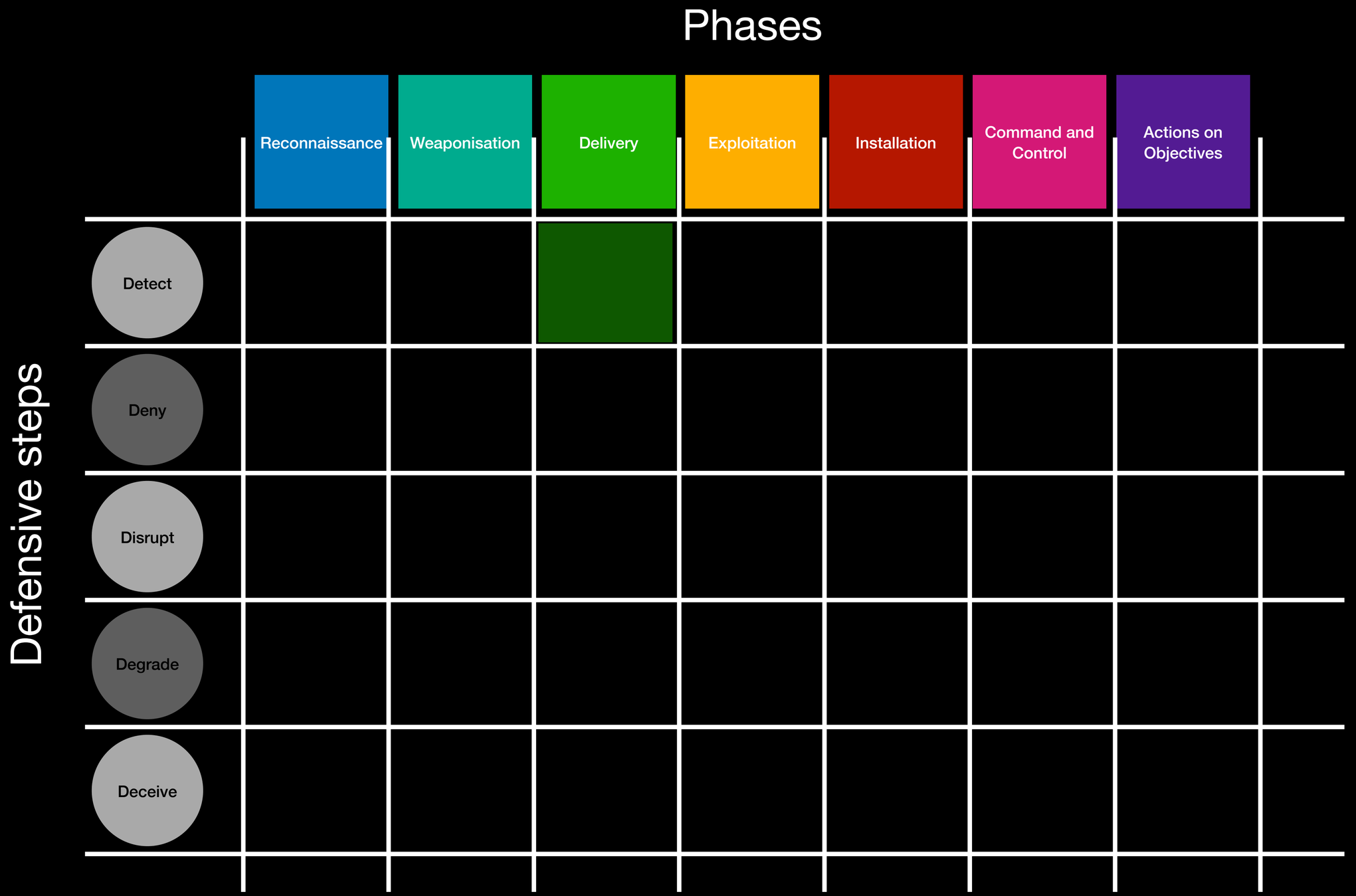

Phases
Reconnaissance
Weaponisation
Delivery
Exploitation
Installation
Command and Control
Actions on Objectives
Defensive steps
Detect
Deny
Disrupt
Degrade
Deceive

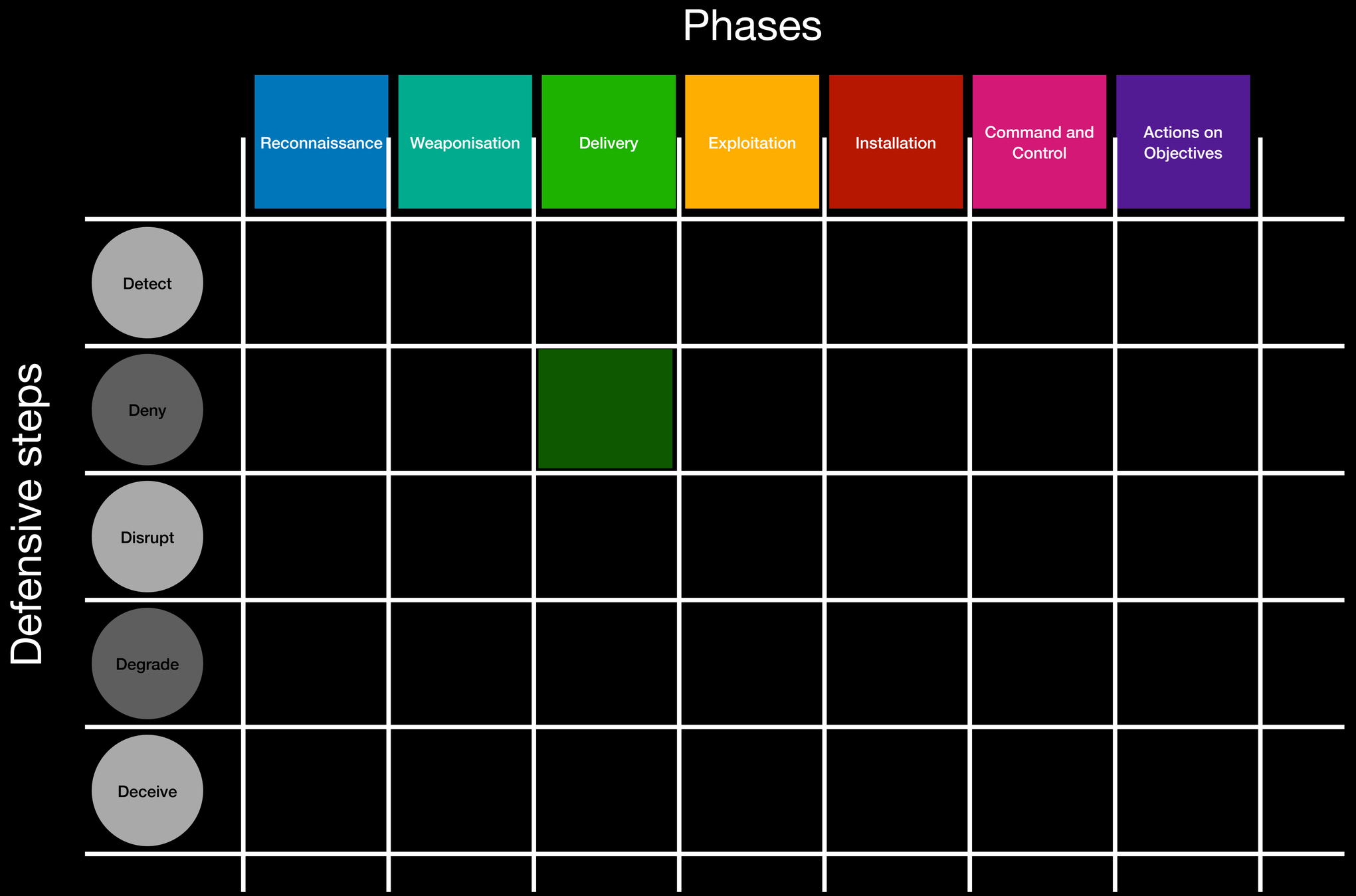

Phases
Reconnaissance
Weaponisation
Delivery
Exploitation
Installation
Command and Control
Actions on Objectives
Defensive steps
Detect
Deny
Disrupt
Degrade
Deceive

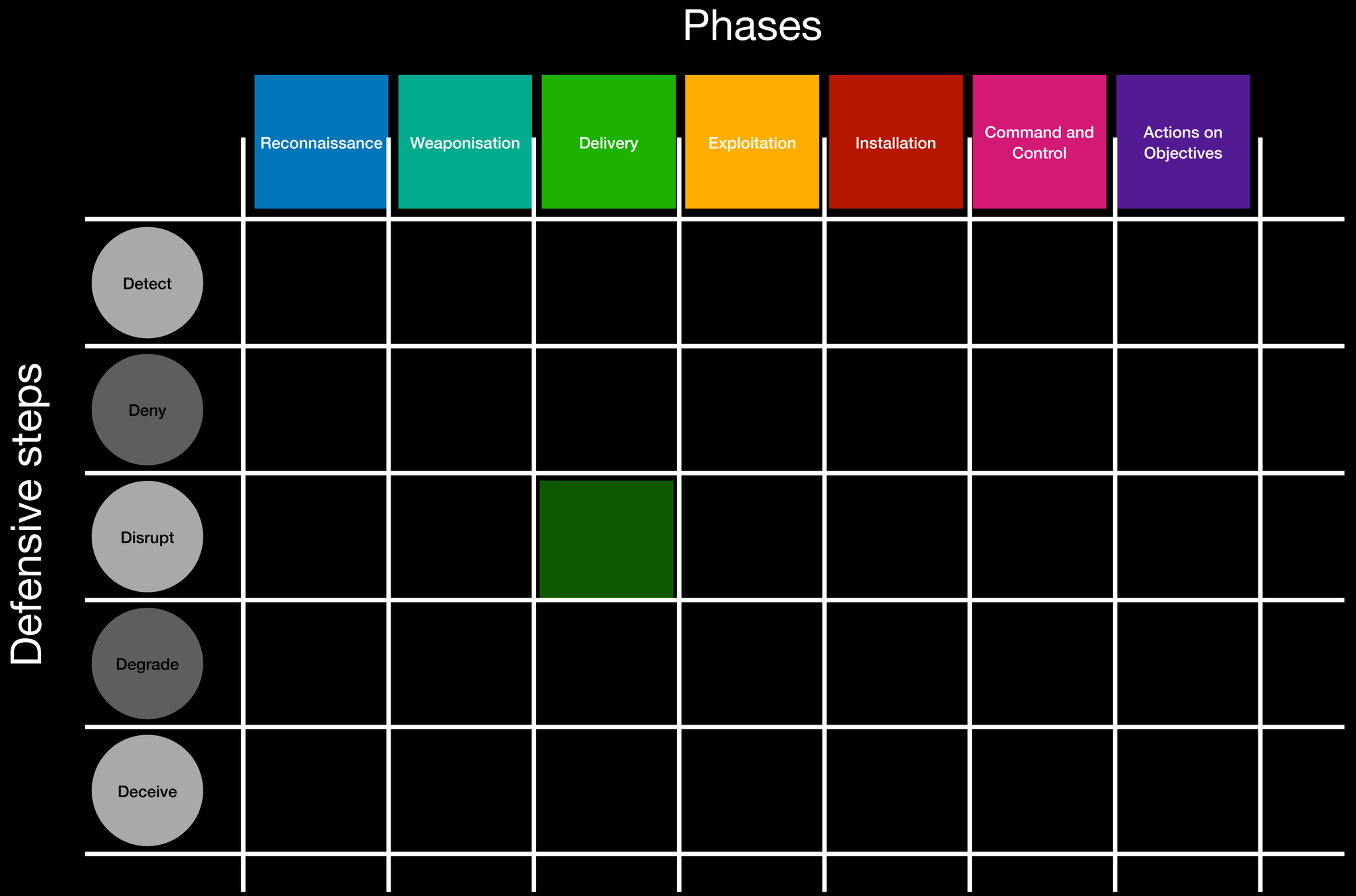
Delivery

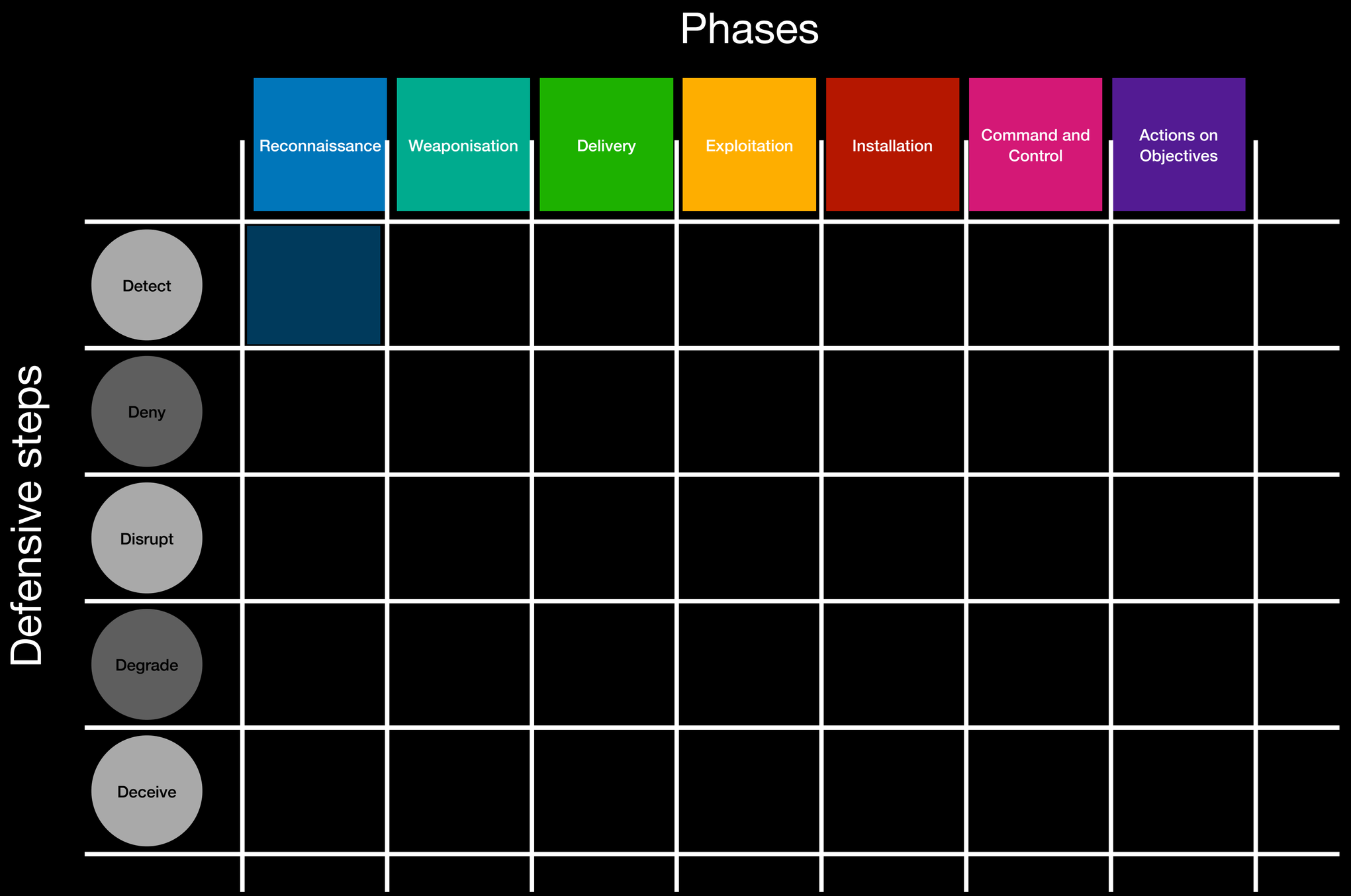
Cyber Kill Chain Phase

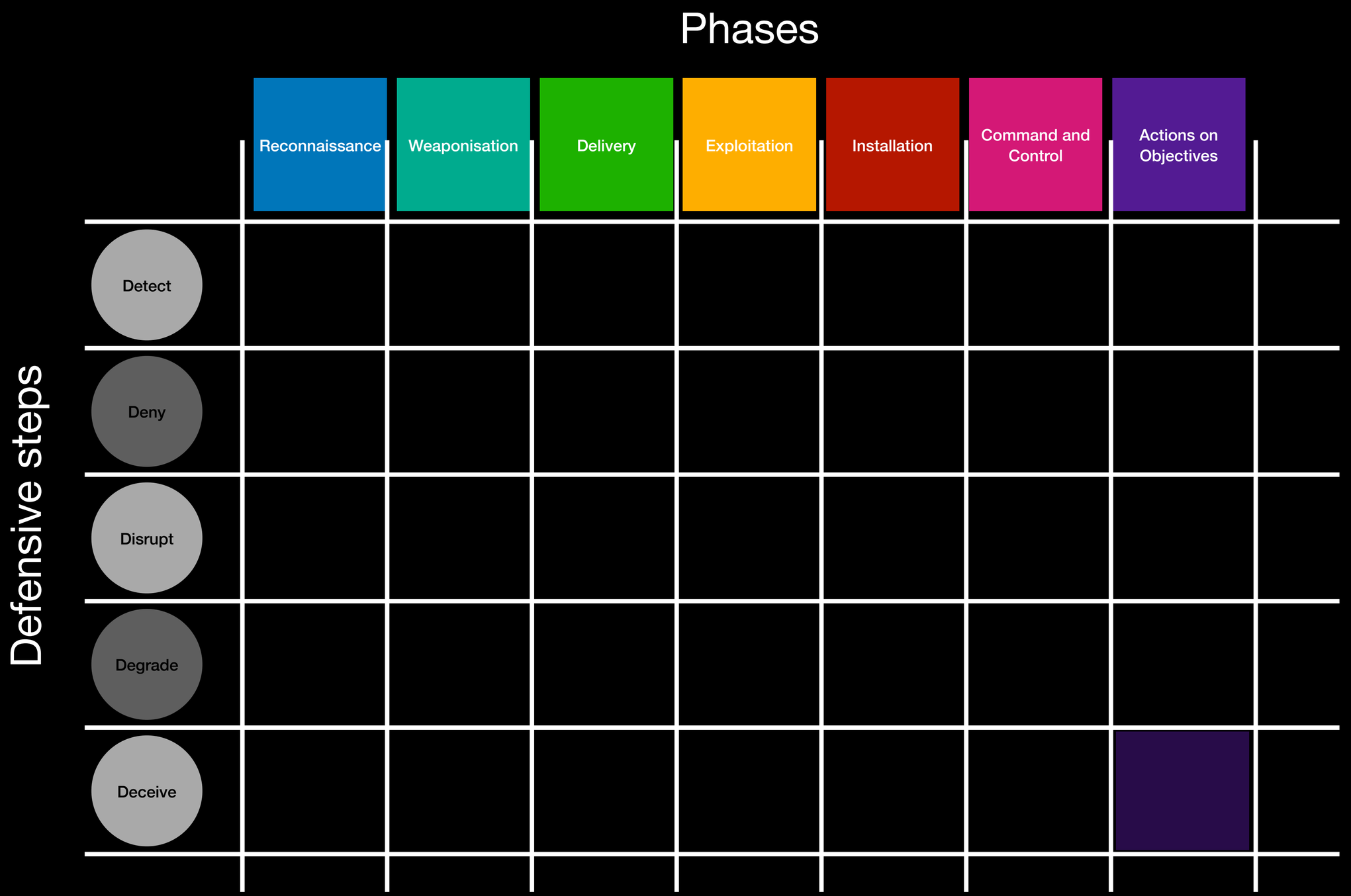
- **Phishing**, cast general net through various communication channels to obtain valuable information.
- **Spear-phishing**, target specific individual or user groups through various communication channels to obtain valuable information.
- **Malvertisement**, advertise on legitimate website but pulls users towards websites where malicious payload can be delivered.
- **Traffic distribution system**, redirect traffic from legitimate website to malicious website to deliver malicious payload.

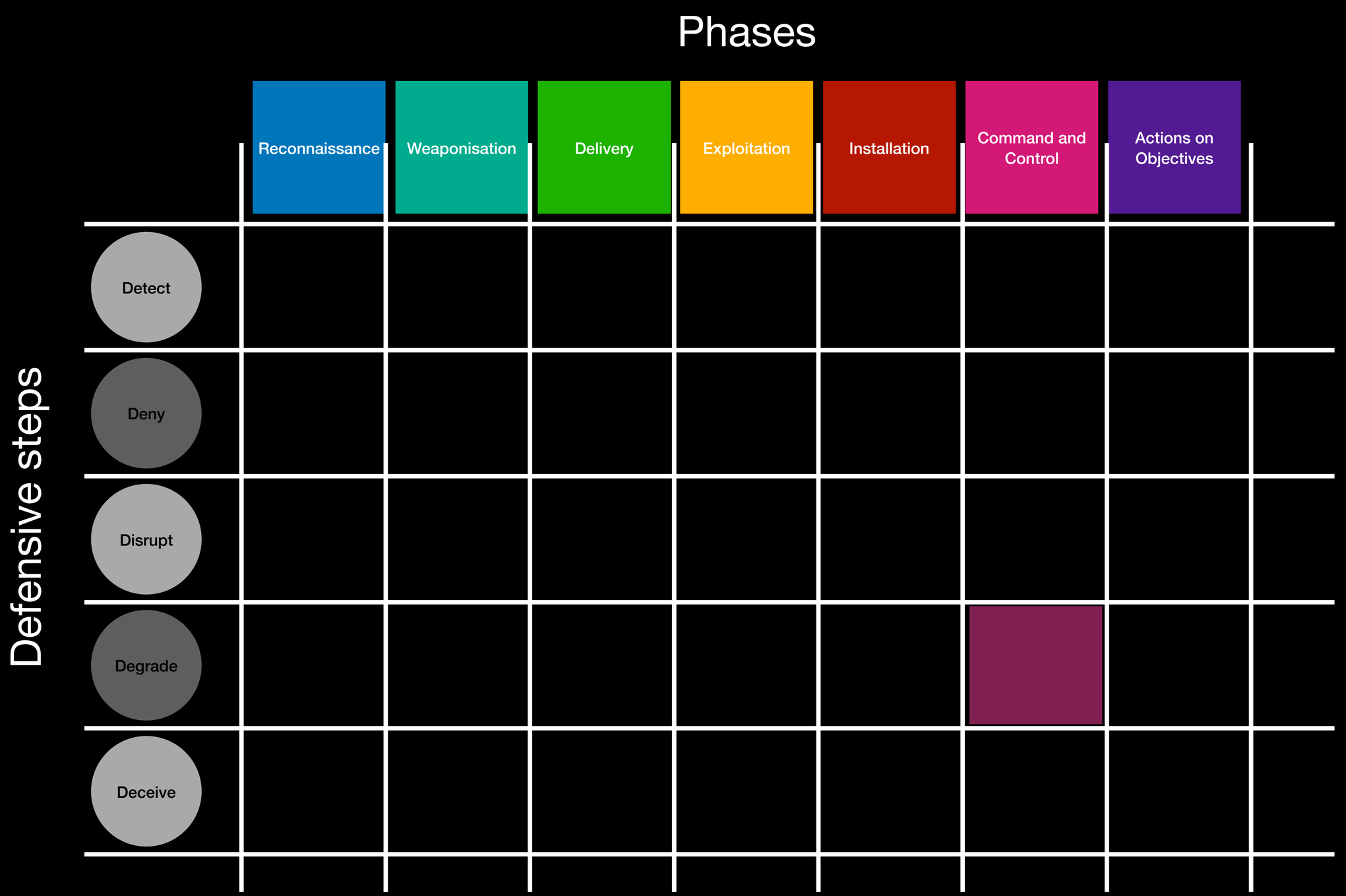

Phases
Reconnaissance
Weaponisation
Delivery
Exploitation
Installation
Command and Control
Actions on Objectives
Defensive steps
Detect
Deny
Disrupt
Degrade
Deceive

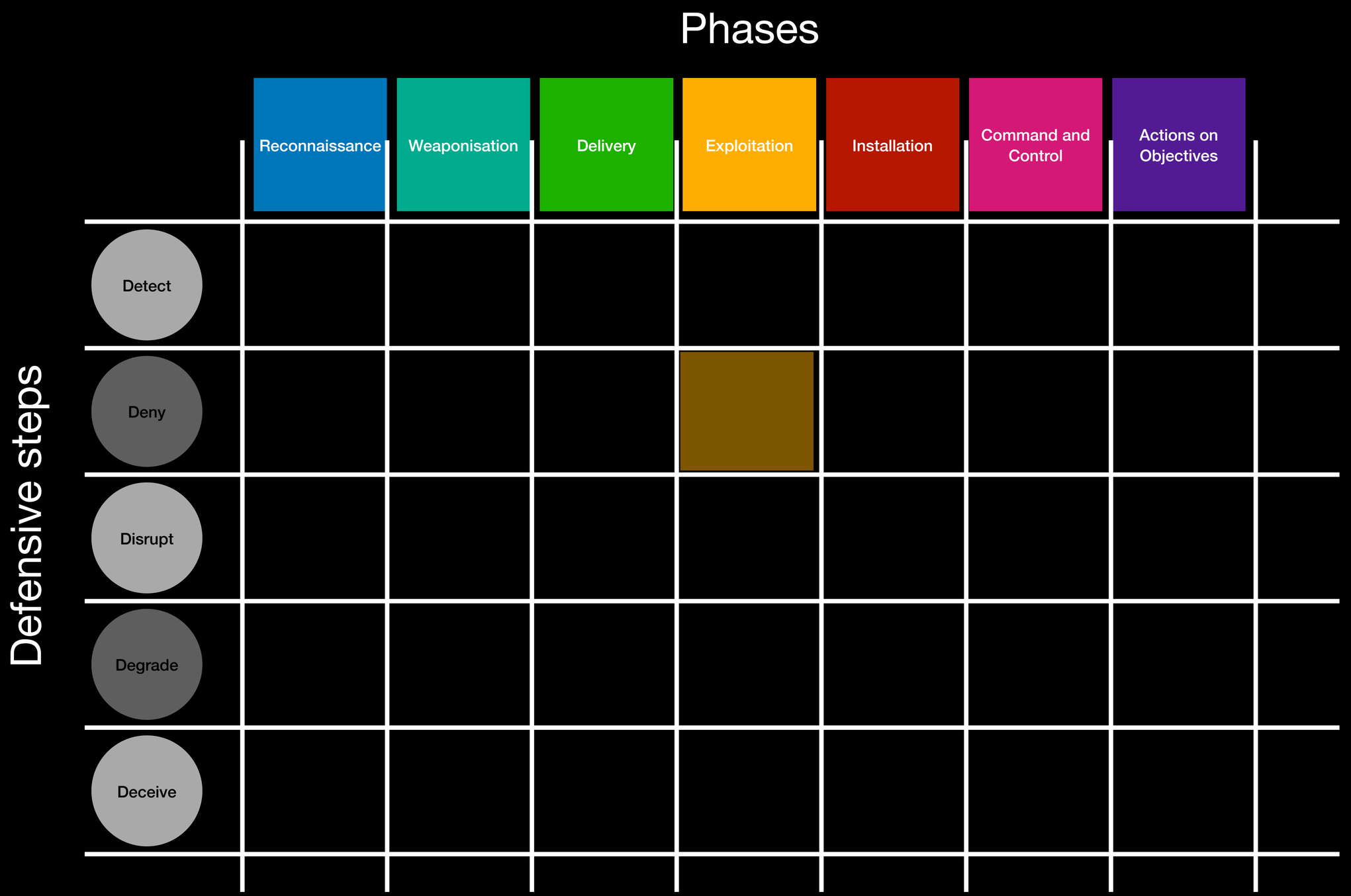

Phases
Reconnaissance
Weaponisation
Delivery
Exploitation
Installation
Command and Control
Actions on Objectives
Defensive steps
Detect
Deny
Disrupt
Degrade
Deceive

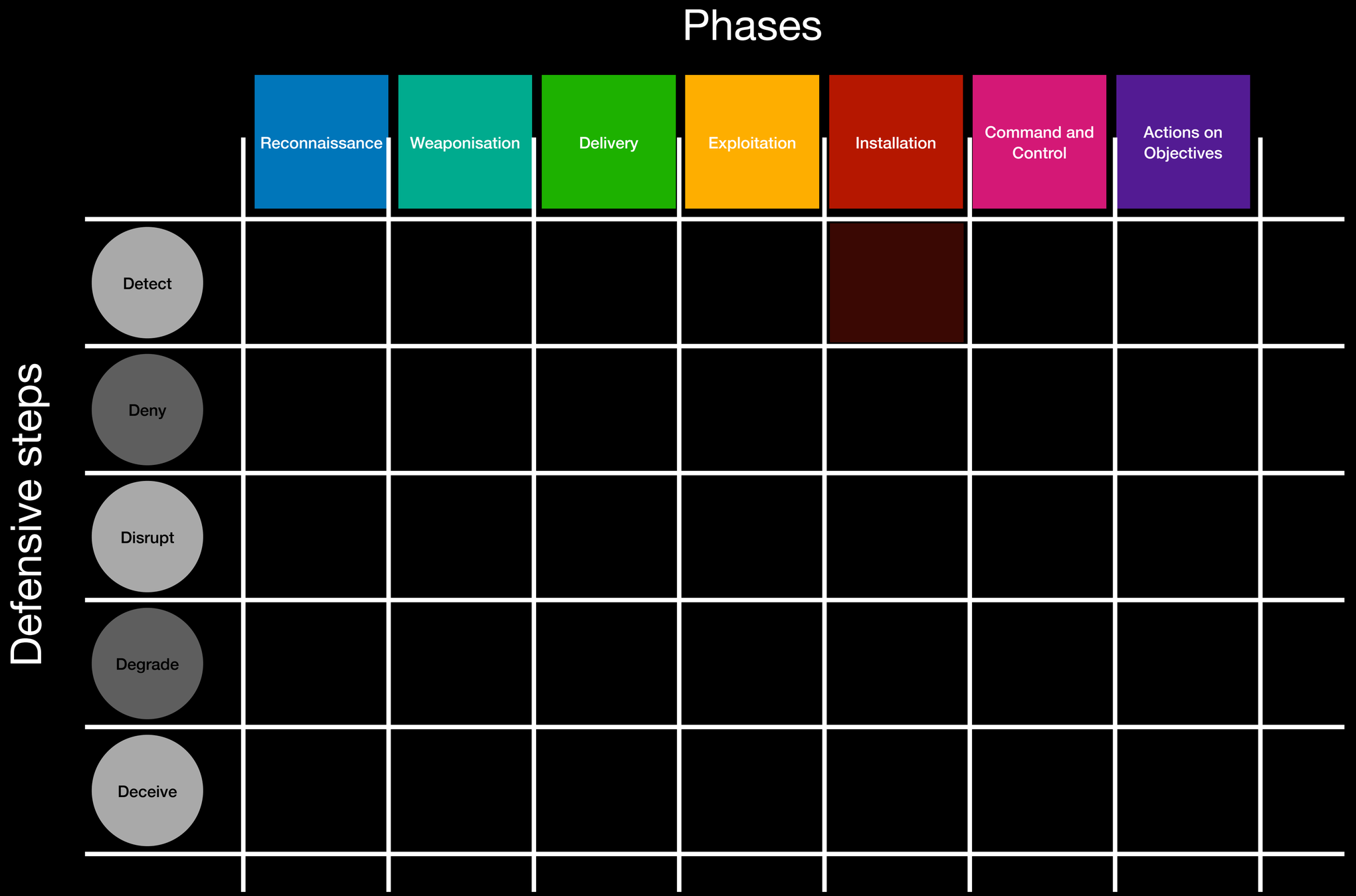

Phases
Reconnaissance
Weaponisation
Delivery
Exploitation
Installation
Command and Control
Actions on Objectives
Defensive steps
Detect
Deny
Disrupt
Degrade
Deceive

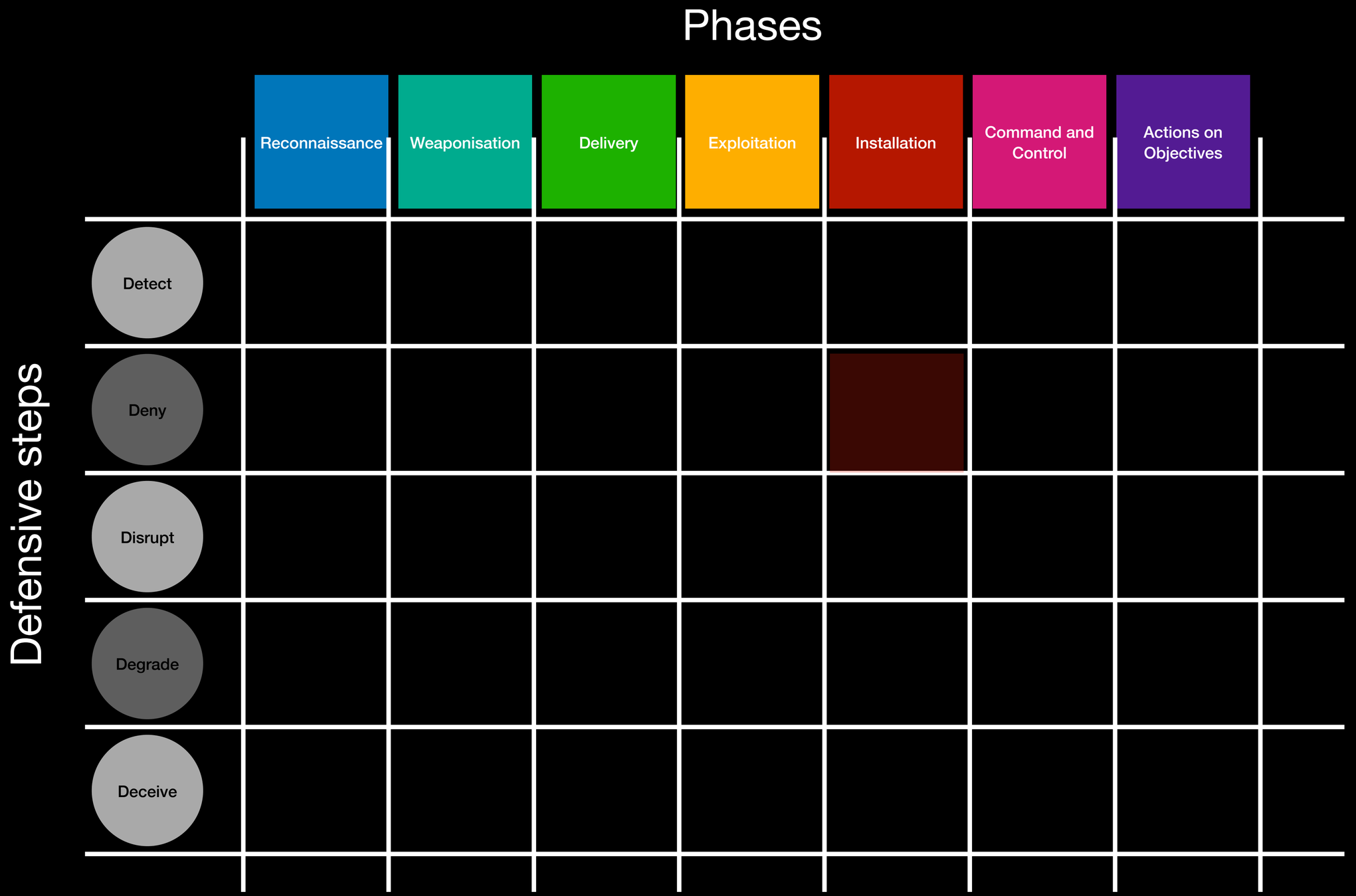

Phases
Reconnaissance
Weaponisation
Delivery
Exploitation
Installation
Command and Control
Actions on Objectives
Defensive steps
Detect
Deny
Disrupt
Degrade
Deceive


Phases
Reconnaissance
Weaponisation
Delivery
Exploitation
Installation
Command and Control
Actions on Objectives
Defensive steps
Detect
Deny
Disrupt
Degrade
Deceive


Phases
Reconnaissance
Weaponisation
Delivery
Exploitation
Installation
Command and Control
Actions on Objectives
Defensive steps
Detect
Deny
Disrupt
Degrade
Deceive


Phases
Reconnaissance
Weaponisation
Delivery
Exploitation
Installation
Command and Control
Actions on Objectives
Defensive steps
Detect
Deny
Disrupt
Degrade
Deceive


Phases
Reconnaissance
Weaponisation
Delivery
Exploitation
Installation
Command and Control
Actions on Objectives
Defensive steps
Detect
Deny
Disrupt
Degrade
Deceive


Phases
Reconnaissance
Weaponisation
Delivery
Exploitation
Installation
Command and Control
Actions on Objectives
Defensive steps
Detect
Deny
Disrupt
Degrade
Deceive

Cyber Kill Chains

Adversarial Behaviours

- Cyber kill chains supports organisations and individuals in formulating the **anatomy of an attack** as well as considering defences.
- Specifically the model considered is optimal for **intrusions**, arguably for other types of attacks the approach is not optimal.
- Not necessarily optimal for all types of intrusion attacks as the model is **fixated largely on external threats**.
- Consequently, may need to **adapt model** for some attacks as well as intrusion attacks, such as insider threats.

Cyber Kill Chains

Adversarial Behaviours