

MITRE ATT&CK Framework

Digital and Cyber Railway Engineering and Operations Center (DCREOC)

Nii O. Attoh-Okine, PhD., P.E., F. ASCE

Professor and Chair

Department of Civil and Environmental Engineering

University of Maryland

College Park, MD



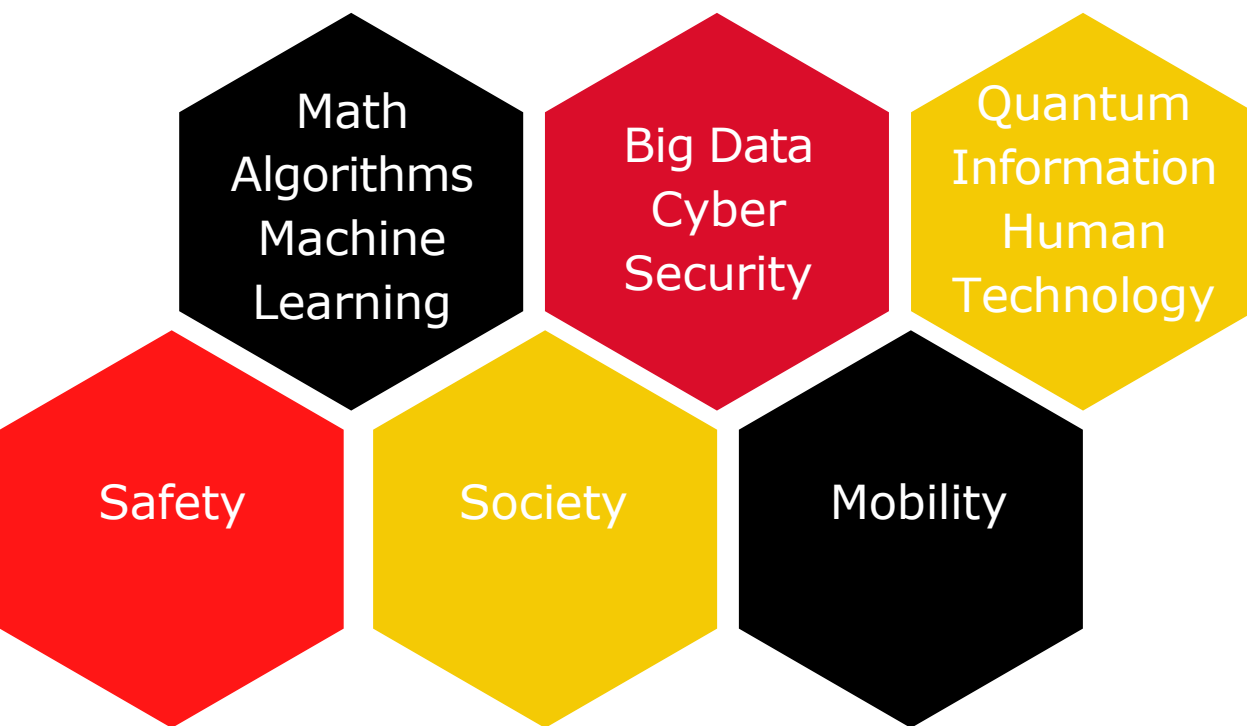
UNIVERSITY OF
MARYLAND

A. JAMES CLARK
SCHOOL OF ENGINEERING

Digital and Cyber Railway Engineering and Operations Center

Mission: Advancement of Digital and Cyber Issues in Railway Engineering and Operations

Fundamental Research

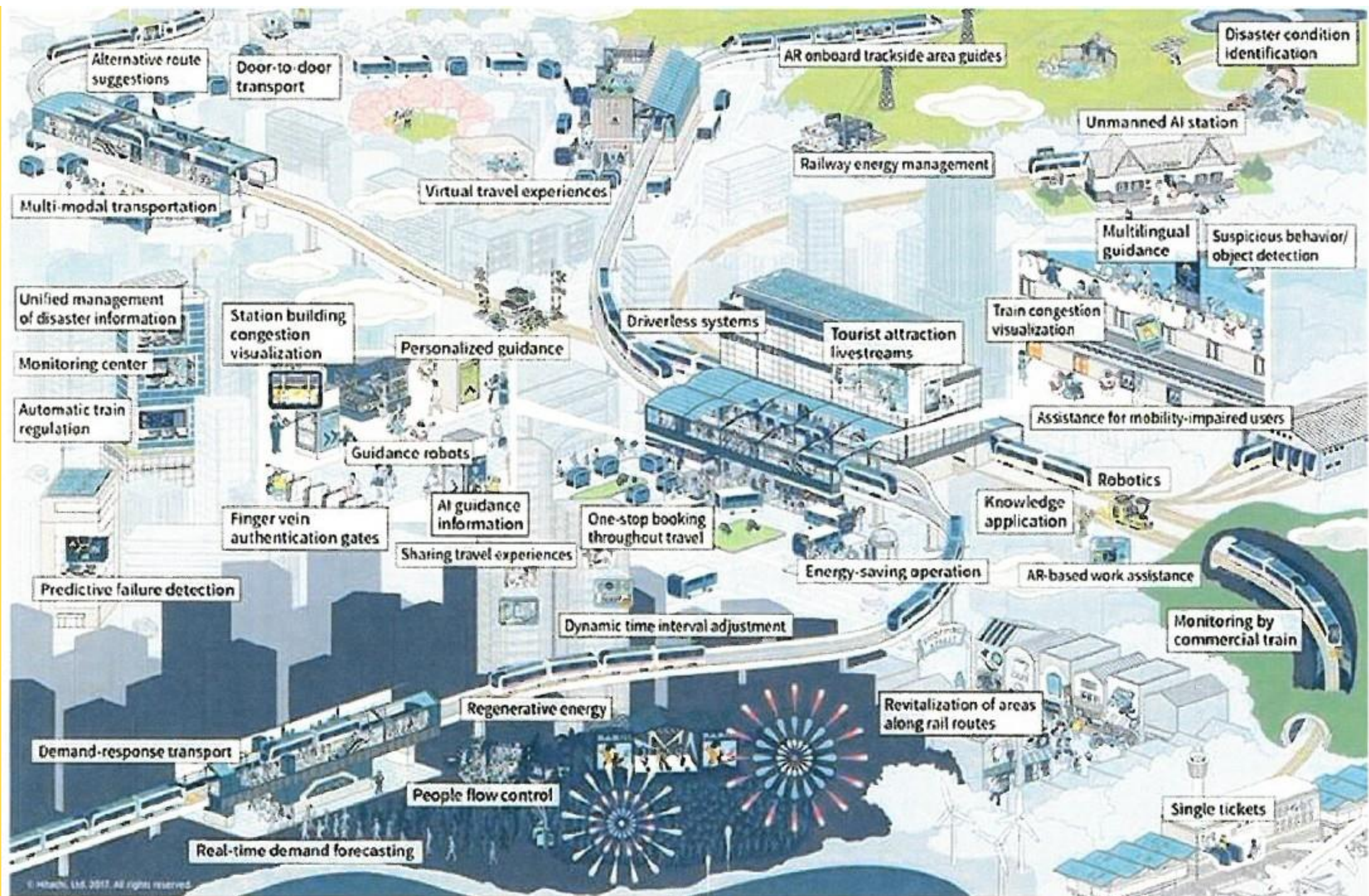


Applied Research

- Research-Railway Track Engineering
- Railway Operations (including ticketing)
- Safety and Security
- Blockchain in Railway Operations
- Quantum Information

Education

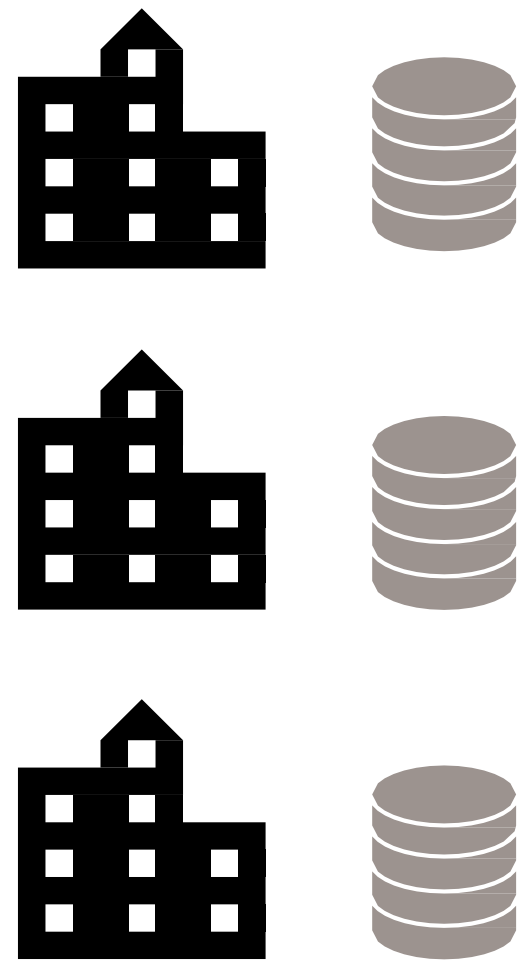
- Training of Students and Railway Professionals in the Area of Digital and Cyber Issues
- Short Courses in Digital and Cyber Railway Issues



Our Objective

How to **effectively** and **securely** utilize **distributed data** of railway agencies without exposing sensitive information?

Data, distributed in a cross-silo setting



- Machine Learning
- Statistical Model
- Quantum Information Processing

Needs:

- Causal
- Digital Twins
- Cyber Attacks
 - safety and security
 - performance

Difficulties:

- different data format
- difficulties of coordination
- isolated data servers - hard to do iterative communication
- privacy and security concerns

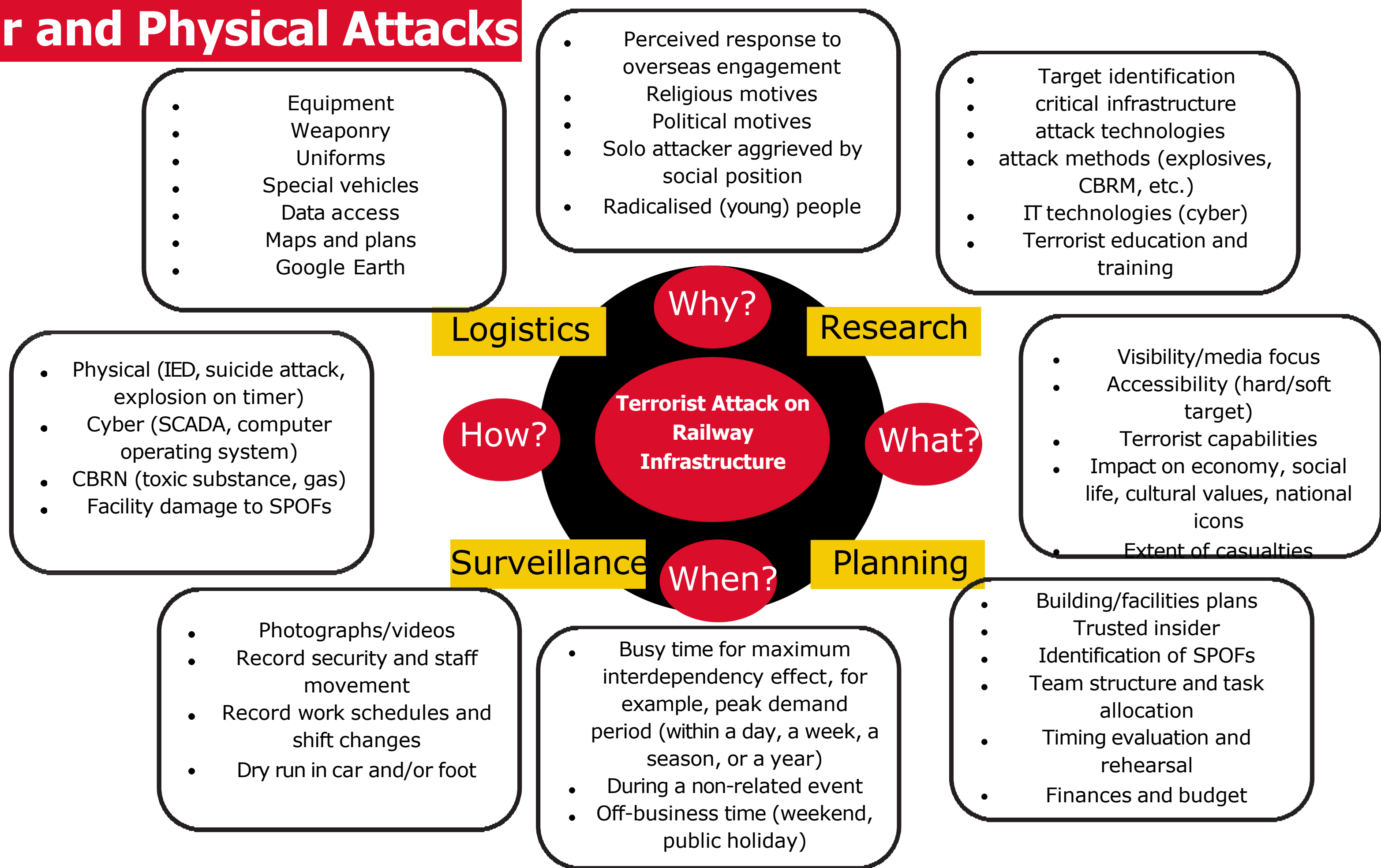
General Goal

Maximize the benefits of Digital Techniques and Cyber Issues in Railway Engineering and Operations, through research, education and policy working with diverse range of specialists and partners to facilitate change that will address appropriate maintenance techniques, operational efficiency, security and safety in Railway Engineering and Operations.

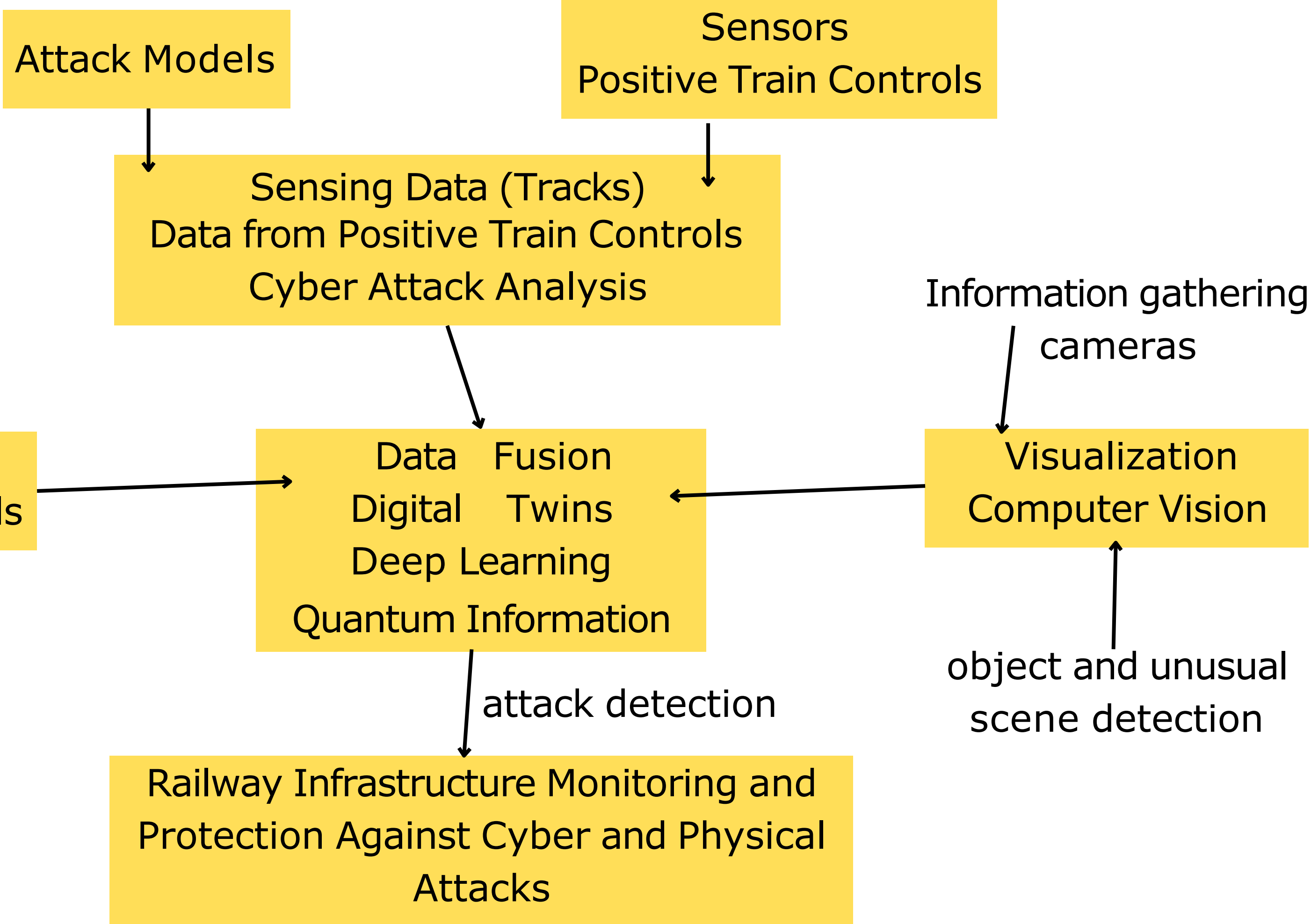
Concept

The future of Rail Transportation will be guided by the Digital and Cyber related issues. Fundamental changes such as data storage and sharing, data analysis, supply chain, cyber attacks and physical attacks will have enormous potential to transform passenger experience, shipping of goods, including hazardous materials and major economic development. Railway Engineering leadership research will guide this transformation. DCREOC is the focal point to guide this new era of Railway Transportation.

Cyber and Physical Attacks



Cyber Pathway and Railway Infrastructure



Ongoing Projects/Past Projects

- Blockchain applications in track geometry modeling
- Covariate-Shift Generative Adversarial Network (COGAN) and Railway Track Images Analysis
- Hybrid reduction technique with covariate shift optimization in high dimensional track geometry
- Approximate Bayesian computation for railway track geometry parameter estimation
- Theory Guided Track Geometry and Defect modeling

- Developing a new track quality index using adaptive methods
- Graphical methods and hazardous materials by rail tank car
- Performance of pantograph operations
- Future of liquid natural gas by rail tank car

Capabilities

The center is led by DCREOC at the University of Maryland, College Park, MD. The University has authoritative programs in Transportation Engineering, Artificial Intelligence and the home of over dozen centers in Quantum Computing.

Partners: University of Tsukuba Center for Artificial Intelligence, Tsukuba, Japan; Railway Engineering Program at Delft University, Netherlands.

MITRE ATT&CK Framework

On-Going Research

ATT&CK evolved...

Adversarial Tactics, Techniques, and Common Knowledge

Framework for aligning defensive strategy to the adversary's playbook of tactics, techniques and procedures.

ATT&CK is...

Adversarial Tactics, Techniques, and Common Knowledge

Based on real-world observations of malicious cyber activity

Knowledge-base of cyber adversary behavior and relationships

Taxonomy for adversarial actions across the attack lifecycle

ATT&CK use...

Adversarial Tactics, Techniques, and Common Knowledge

**Blueprint for the development of
specific threat models and
methodologies**

ATT&CK use...

Adversarial Tactics, Techniques, and Common Knowledge

Model and analyze threats

Assess risk

Plan attack simulations

Evaluate defense

**Attack detection, prediction, prevention,
mitigation**

ATT&CK Framework...

Adversarial Tactics, Techniques, and Common Knowledge

3 Technology Domains

Platforms

Tactics

Techniques/Sub-techniques

Mitigations

Threat groups

Software

Campaigns

ATT&CK Domains...

Adversarial Tactics, Techniques, and Common Knowledge

3 Technology Domains:

Enterprise – *most extensive*

Mobile

Industrial Control Systems (ICS)

**Represent fundamentally different
system/device types and adversaries
objectives**

**Each domain is associated with different
tactics, techniques, and procedures (TTPs)**

ATT&CK Matrix...

Adversarial Tactics, Techniques, and Common Knowledge

Condensed representation of framework

Updated twice a year – reflects evolving threat landscape

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

layout: flat show sub-techniques hide sub-techniques help

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques

Mobile Matrix

Below are the tactics and techniques representing the two MITRE ATT&CK® Matrices for Mobile. The Matrices cover techniques involving device access and network-based effects that can be used by adversaries without device access. The Matrix contains information for the following platforms: Android, iOS.

layout: flat show sub-techniques hide sub-techniques help

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
7 techniques	4 techniques	7 techniques	3 techniques	16 techniques	5 techniques	8 techniques	2 techniques	13 techniques	9 techniques	2 techniques	10 techniques

ICS Matrix

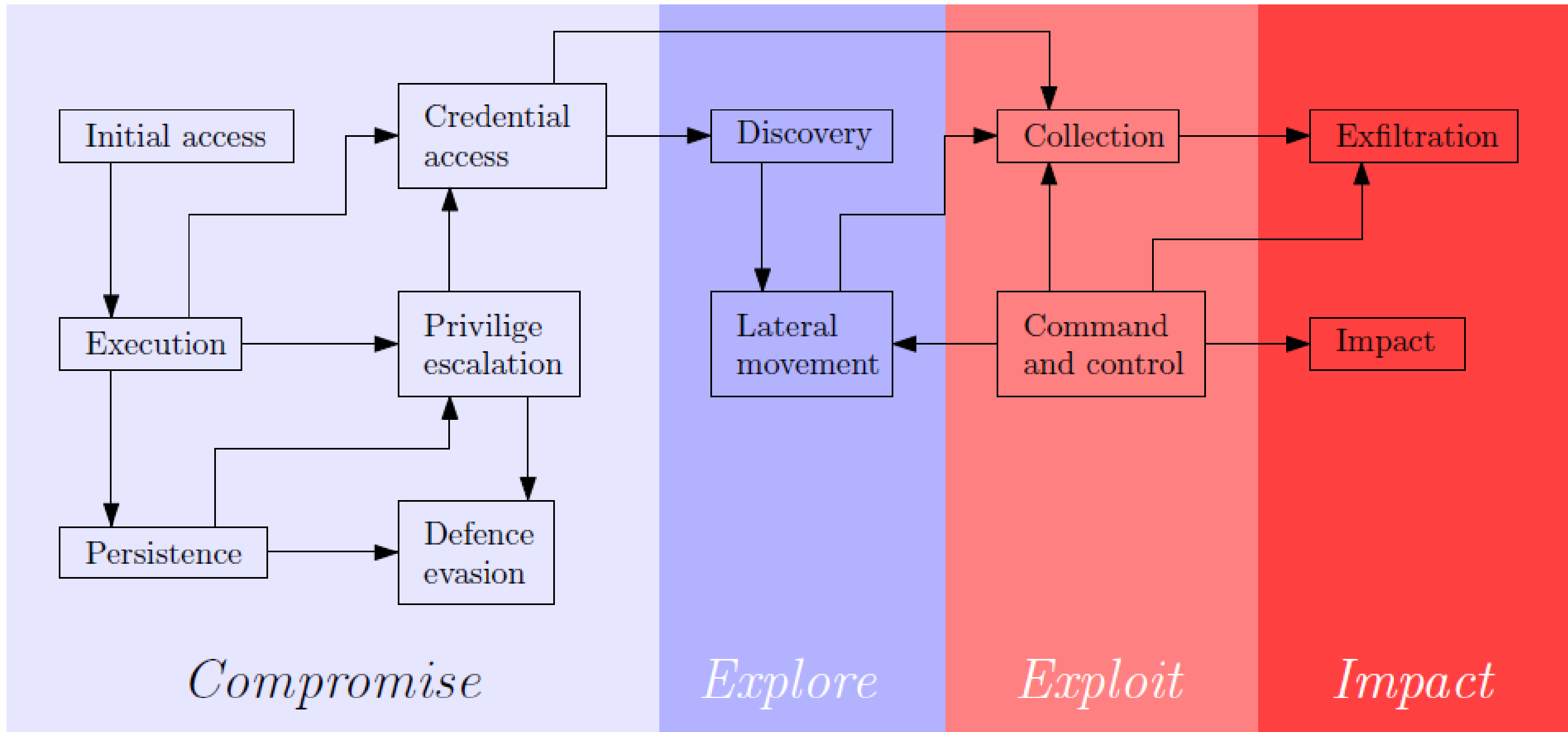
Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

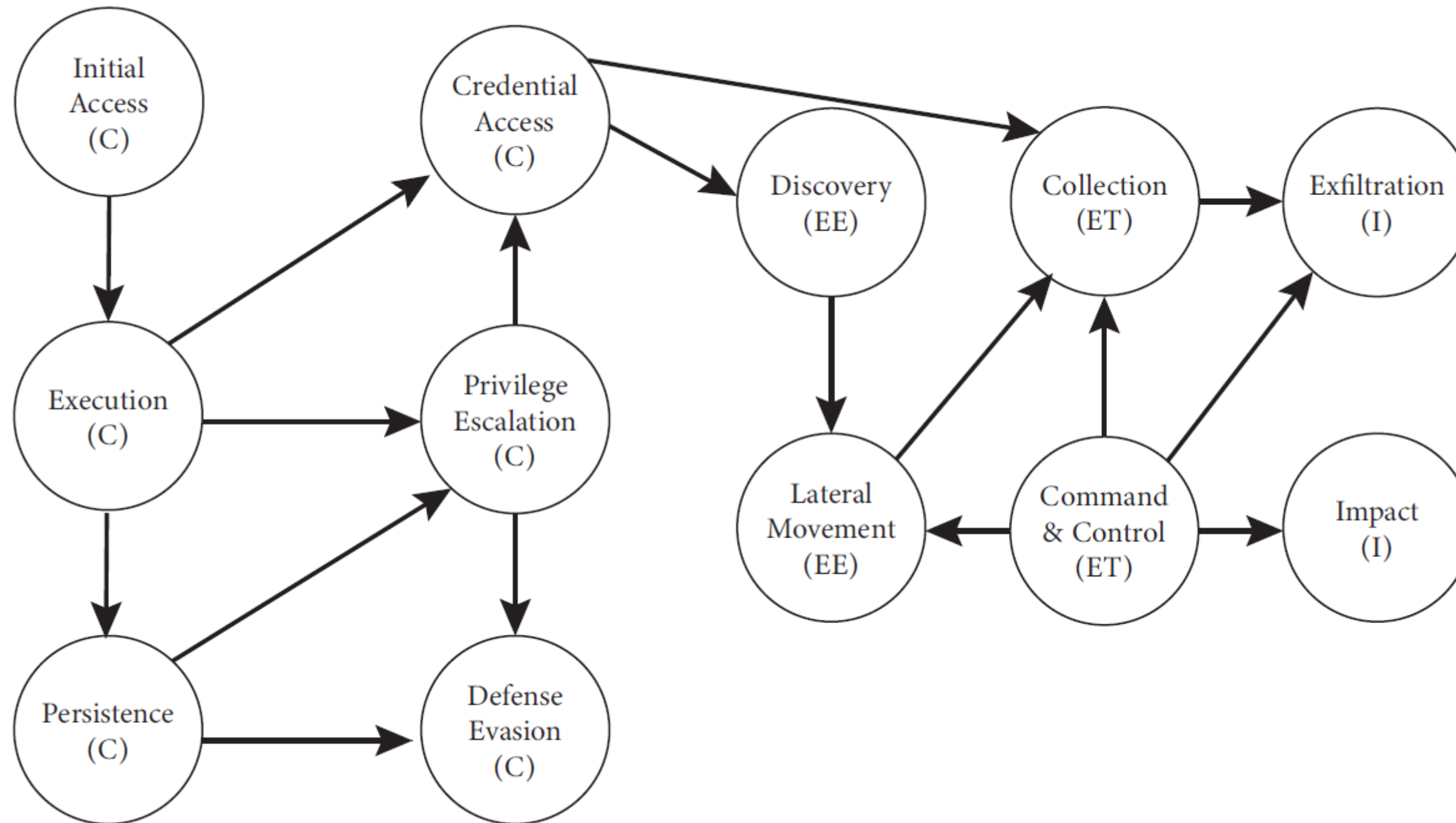
Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage Proper
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availa
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Contro
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Produ
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protec
	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
	Scripting								Device Restart/Shutdown		Loss of
									Manipulate I/O Image		Loss of

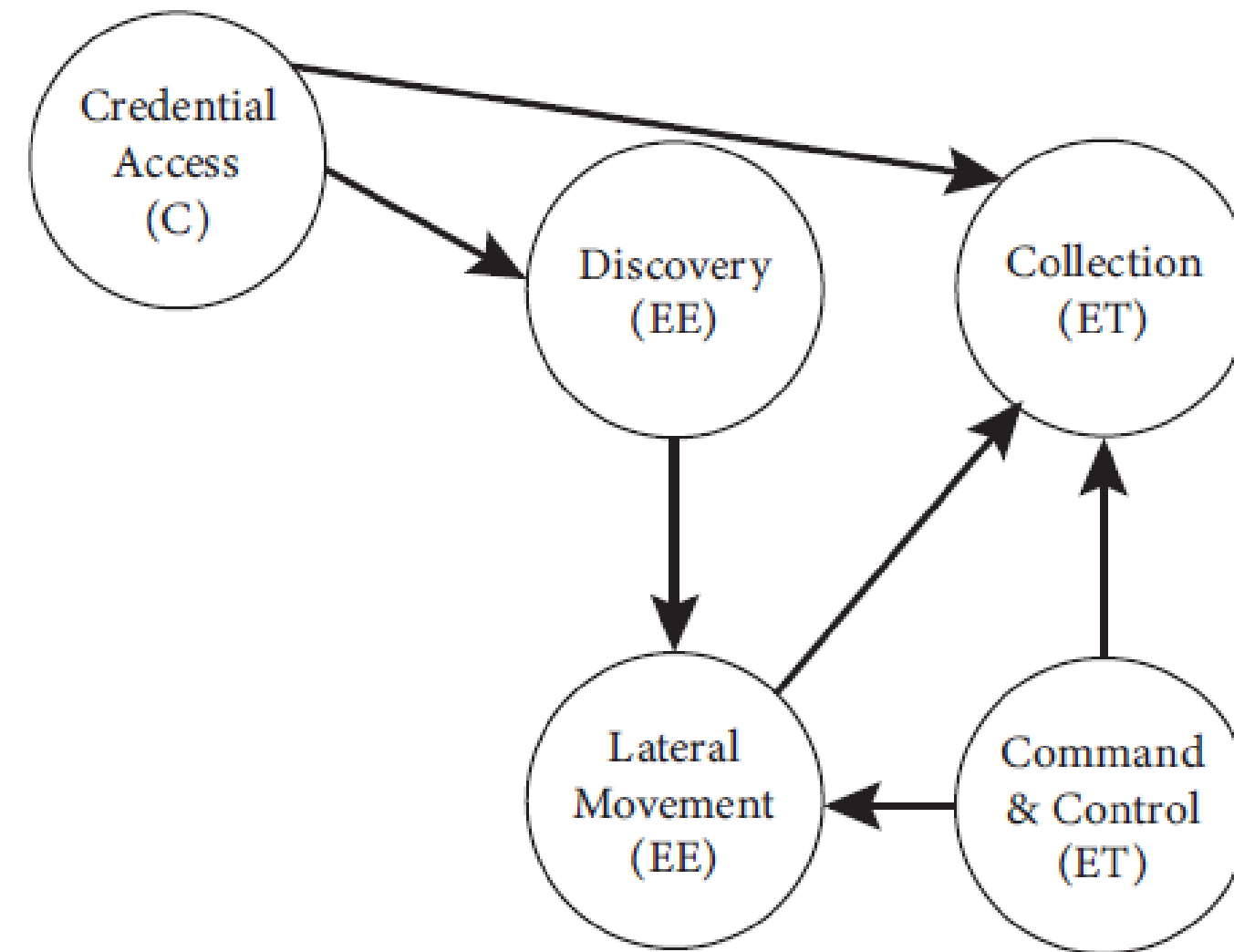


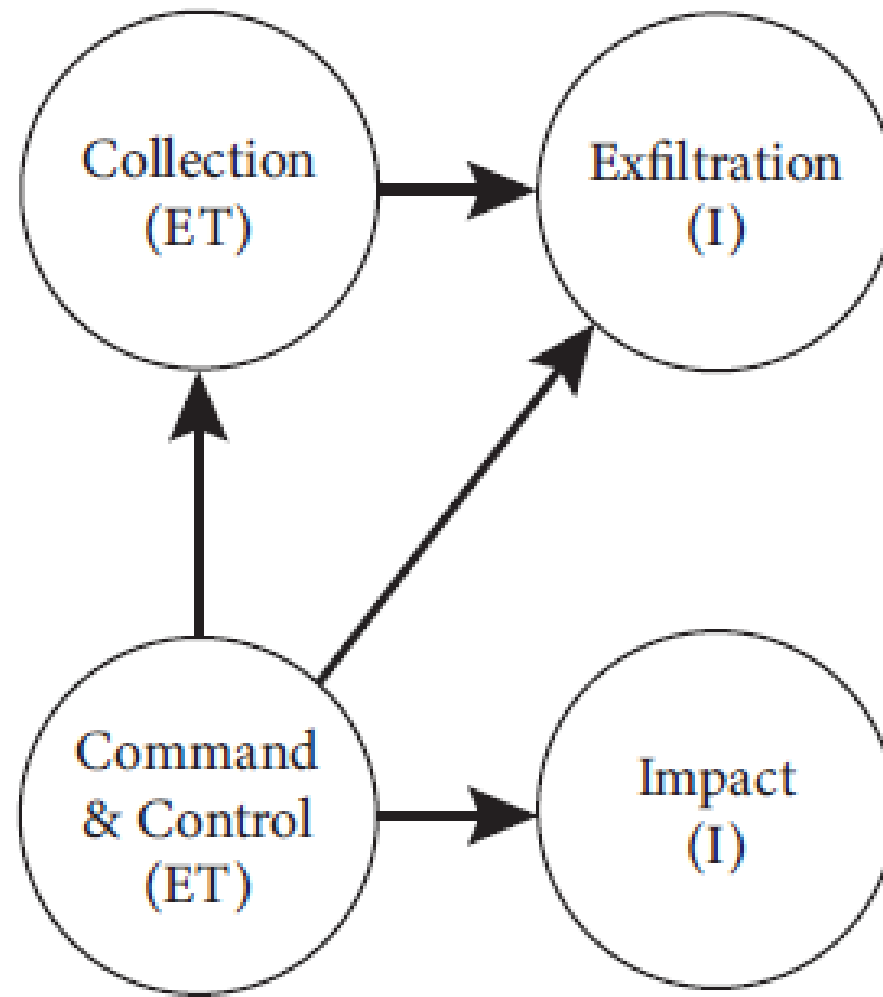
**Tactics = Columns
Left to right
Represent potential
phases of attack**

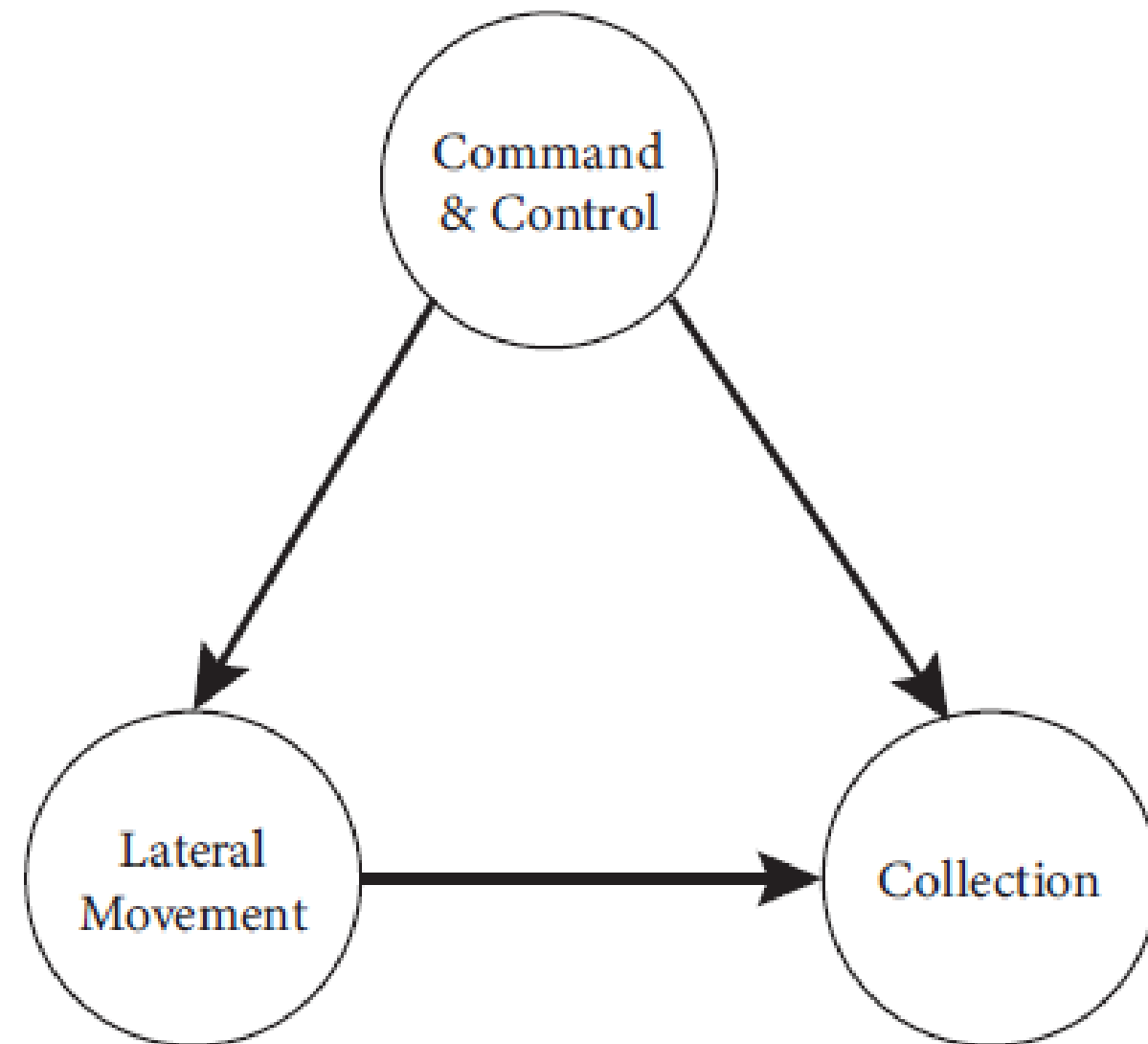
Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (6)	Access Token Manipulation (5)	Brute Force (4)	Application Web Discovery
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Discovery
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Discovery
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Execution Guardrails (1)	Direct Volume Access	Modify Authentication Process (9)	Container and Discovery
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Escape to Host	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote	Event Triggered Execution (16)	Exploitation for Defense Evasion	File and Directory Permissions Modification (2)	Device Driver Discovery
			Software Deployment Tools			File and Directory Permissions Modification (2)		Domain Trust Discovery
								File and Directory Discovery
								Group Policy Discovery











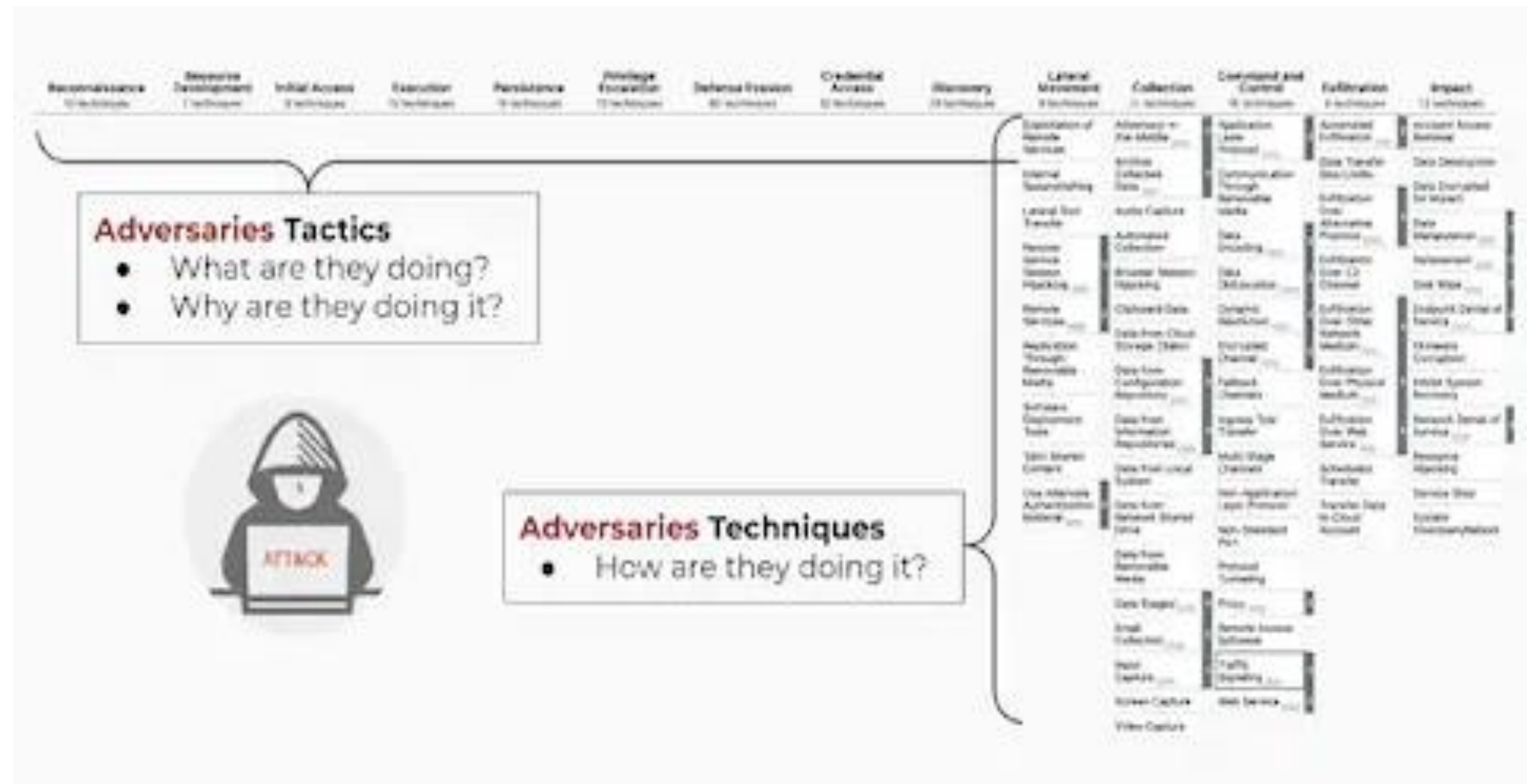
Node	Scenario 1	Scenario 2	Scenario 3
Command & Control	High	High	High
Lateral Movement	Medium	Low	High
Collection	Low	Medium	High



Adversary Tactical Goal

Tactics = “why”

Goal or Reason for performing an action



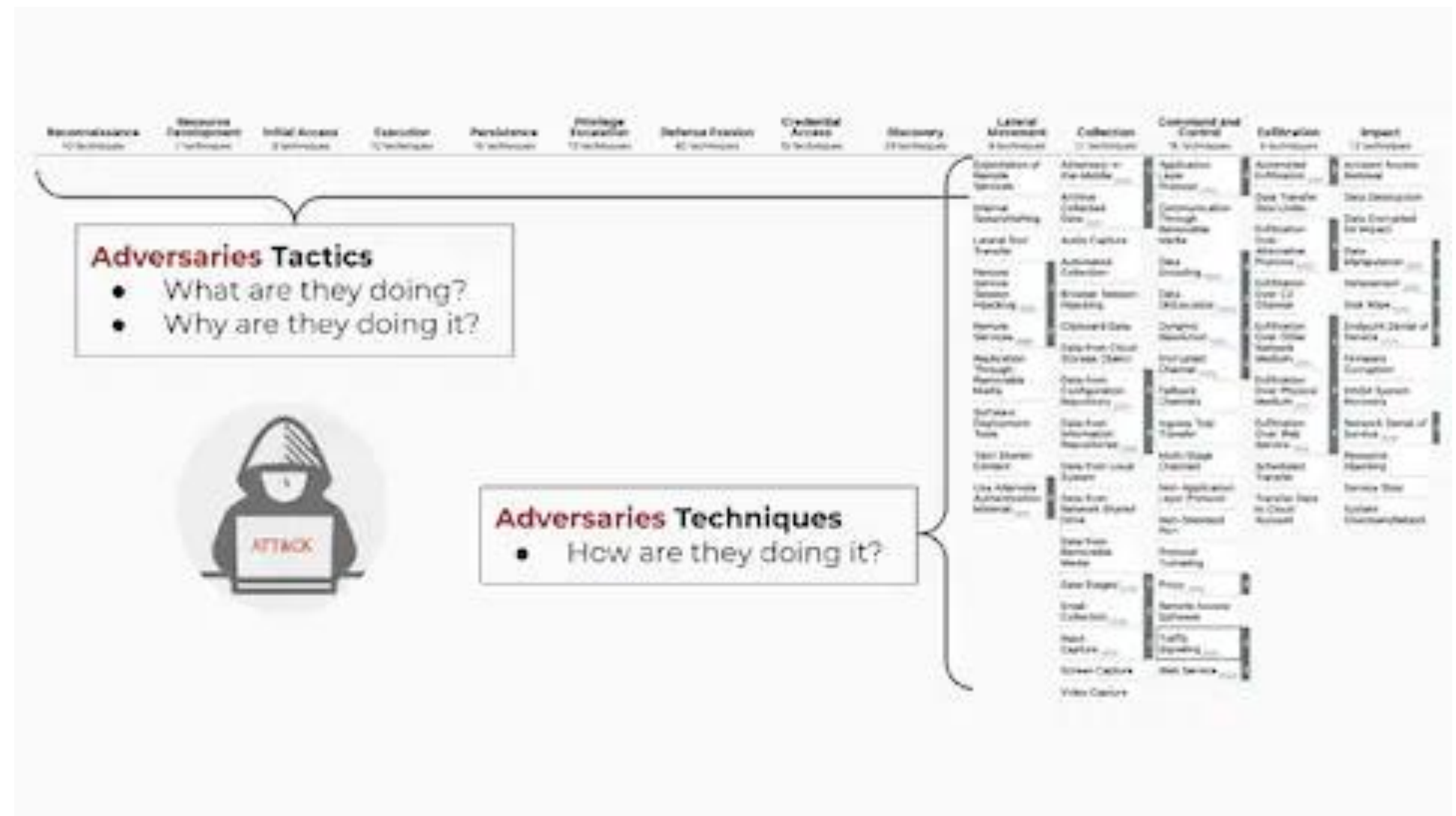
Techniques = Row items



Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (6)	Access Token Manipulation (5)	Brute Force (4)	Application Web Discovery
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Discovery
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Discovery
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Execution Guardrails (1)	Domain or Tenant Policy Modification (2)	Modify Authentication Process (9)	Container and Discovery
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Escape to Host	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Debugger Evasion
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote	Event Triggered Execution (16)	File and Directory Permissions Modification (2)		Device Driver Discovery
			Software Deployment Tools					Domain Trust Discovery
								File and Directory Discovery
								Group Policy Discovery

Adversary Techniques

Techniques = “how”
Actions, Methods employed to accomplish goals
Classified by tactics
Sub-techniques, more detailed



Sub-Techniques = More detailed

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (6)	Access Token Manipulation (5)	Brute Force (4)	Application Web Discovery
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Access Token Manipulation (5)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Account Manipulation (6)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Autostart Execution (14)	Debugger Evasion	Forced Authentication	Cloud Service Discovery
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Create or Modify System Process (5)	Deploy Container	Input Capture (4)	Cloud Storage Discovery
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Modify Authentication Process (9)	Container and Discovery
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Domain or Tenant Policy Modification (2)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote	Escape to Host	Execution Guardrails (1)	File and Directory Permissions Modification (2)	Device Driver Discovery
			Software Deployment Tools		Event Triggered Execution (16)	Exploitation for Defense Evasion		Domain Trust Discovery
						File and Directory Permissions Modification (2)		File and Directory Discovery
								Group Policy Discovery

Procedures

Sequence of malicious actions
 Lateral movement
 Same technique can be used to achieve multiple tactics
 Multiple techniques can be used to achieve one tactic

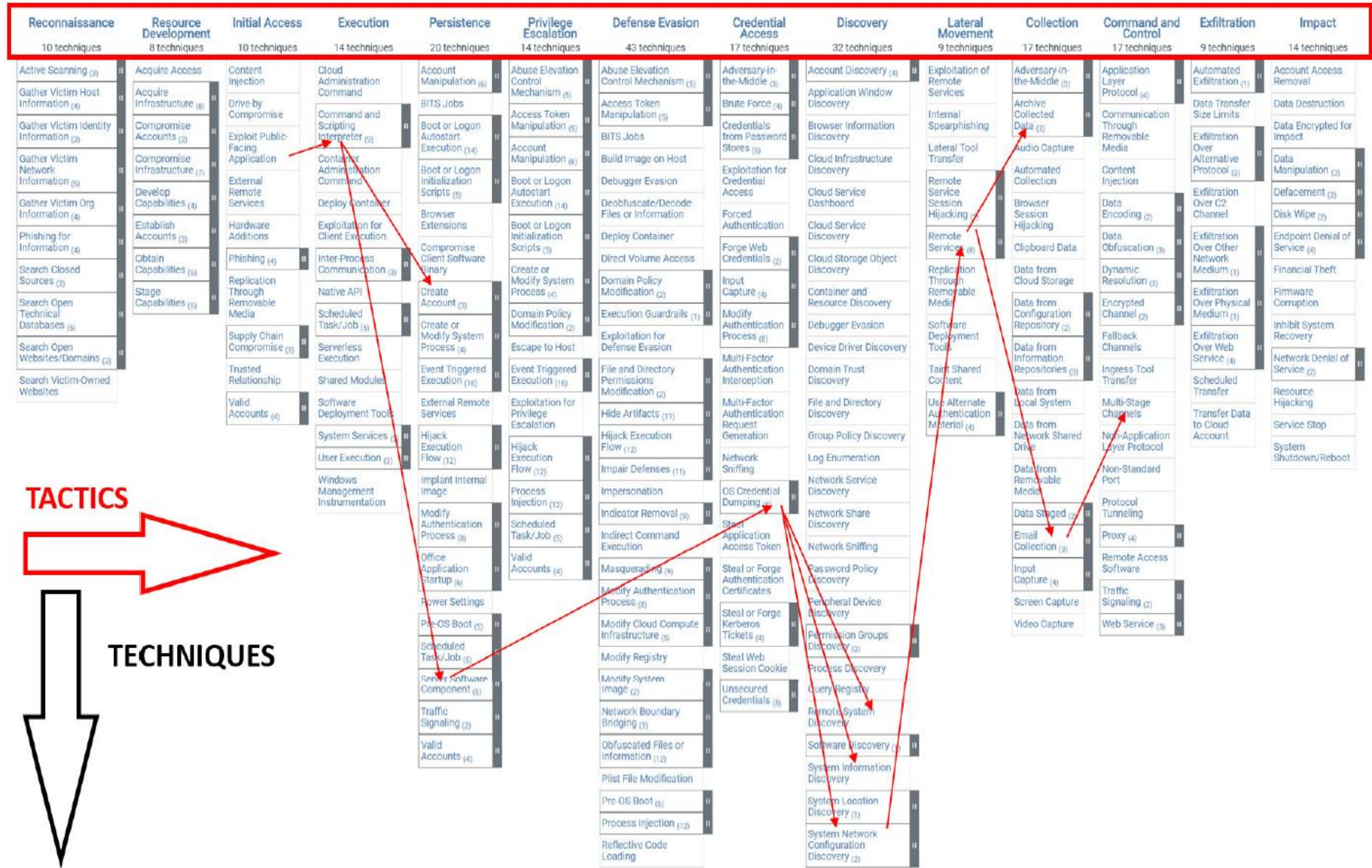
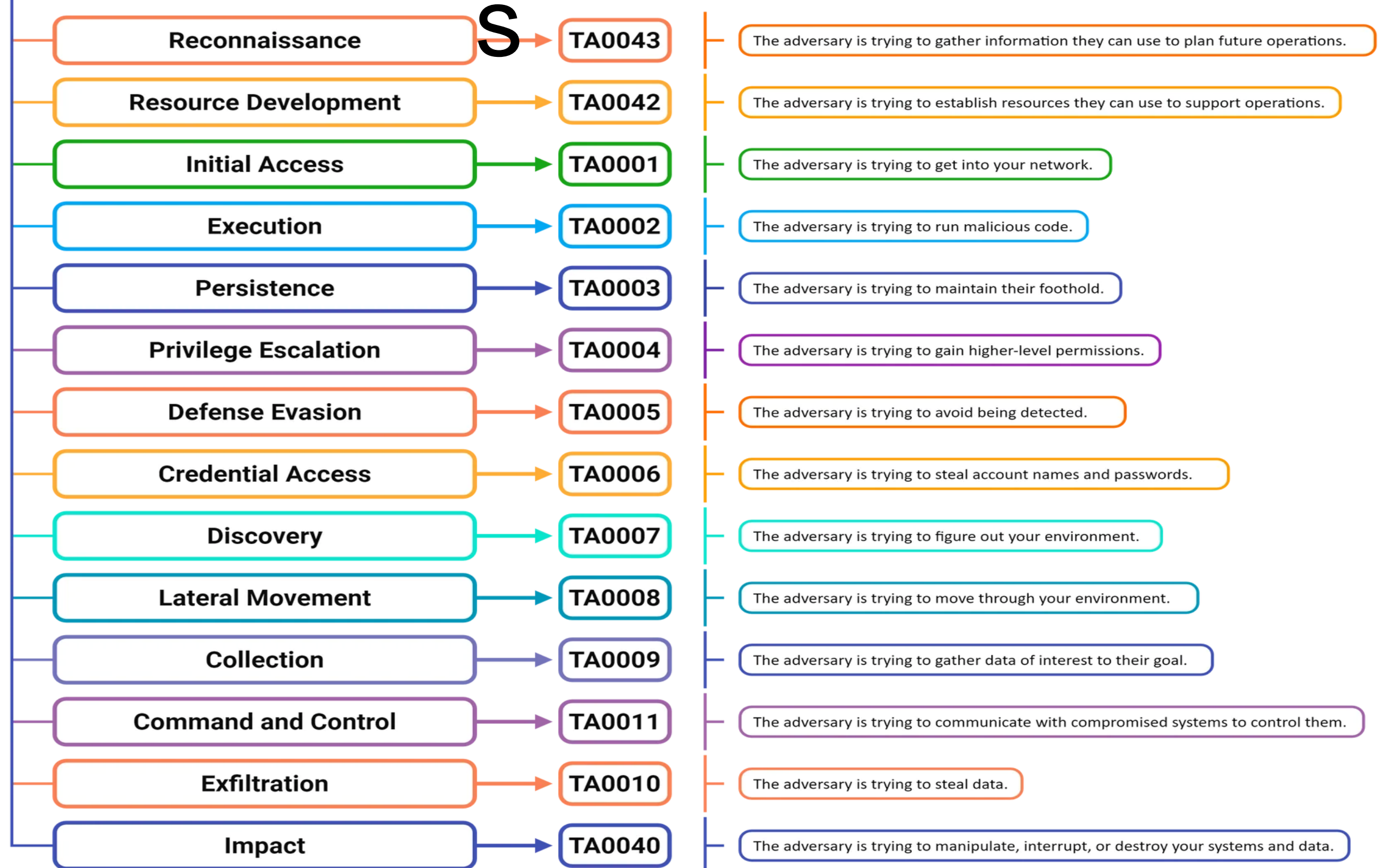


FIGURE 1. MITRE ATT&CK matrix lay-out for Enterprise domain: tactics are organized by columns while techniques by rows.

**MITRE ATT&CK
Framework
(Enterprise Matrix)**

Tactic



Mitigations

Security concepts/classes of technologies

Prevent successful execution of a
technique

43 Enterprise Mitigations

13 Mobile Mitigations

52 ICS Mitigations

Groups, Software

Tracked using various analytic methods

152 Groups (threat groups, threat actors)

Associated names

Techniques used

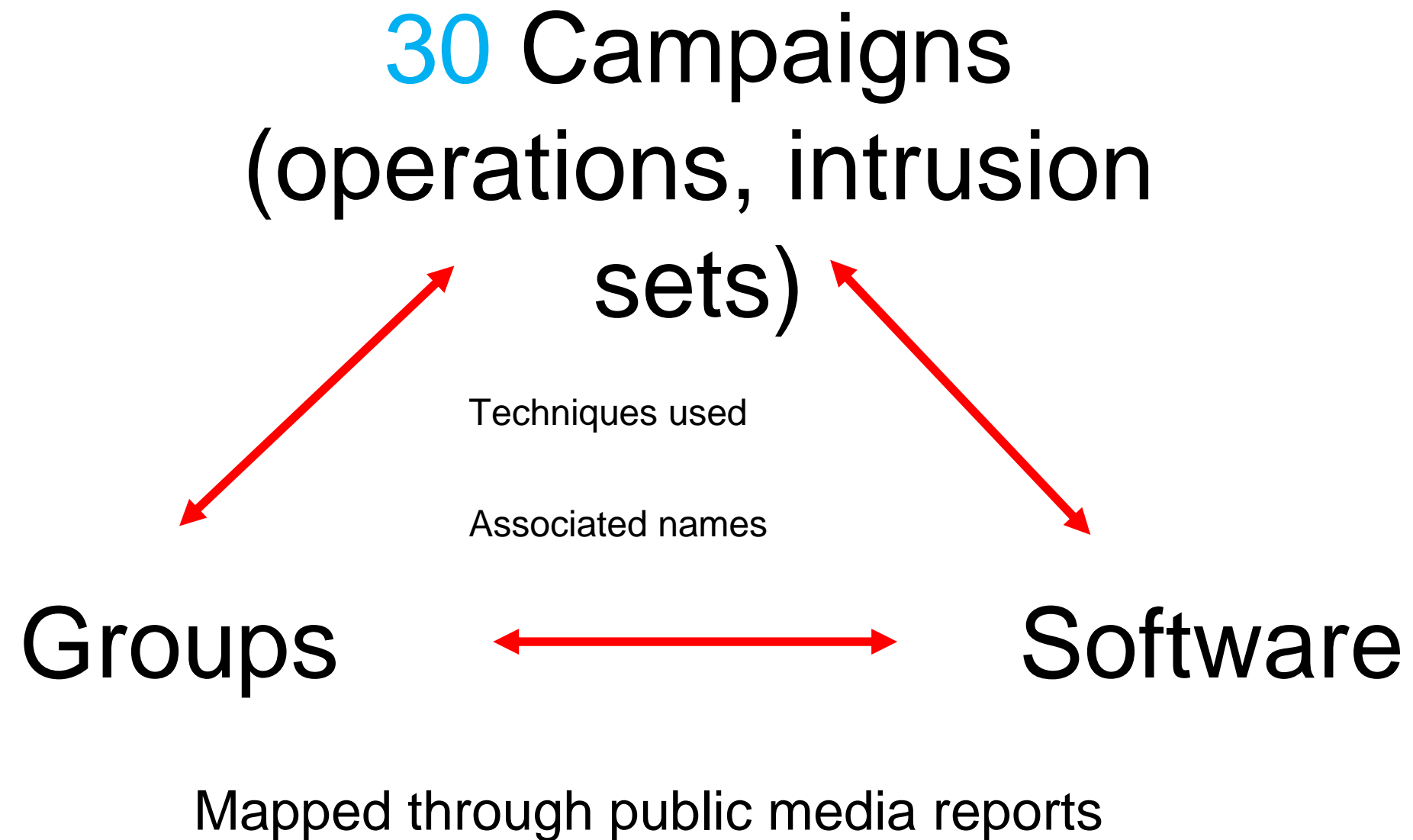


794 Software (Tools and Malware)

Mapped through public media reports

Campaigns

Tracked using various analytic methods



ATT&CK Navigator

Open-source tool to help explore ATT&CK knowledge base
Compare techniques used by two or more different Groups

The screenshot displays the ATT&CK Navigator interface with three tabs: FIN7, Leviathan, and FIN7 (RED) & LEVIATHAN (YELLOW). The interface is organized into columns representing different stages of an attack: Reconnaissance (10 techniques), Resource Development (8 techniques), Initial Access (10 techniques), Execution (14 techniques), Persistence (20 techniques), Privilege Escalation (14 techniques), Defense Evasion (43 techniques), Credential Access (17 techniques), Discovery (32 techniques), Lateral Movement (9 techniques), Collection (17 techniques), Command and Control (18 techniques), Exfiltration (9 techniques), and Impact (14 techniques). Each cell in the grid contains a technique name and a progress indicator (e.g., 0/3). Techniques are color-coded: red for techniques used by both groups, yellow for techniques used by one group, and green for techniques used by the other. The interface includes a top navigation bar with search and filter controls, and a bottom status bar with the text 'MITRE ATT&CK® Navigator v5.0.1' and a legend.

Reconnaissance (10 techniques)	Resource Development (8 techniques)	Initial Access (10 techniques)	Execution (14 techniques)	Persistence (20 techniques)	Privilege Escalation (14 techniques)	Defense Evasion (43 techniques)	Credential Access (17 techniques)	Discovery (32 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)	Command and Control (18 techniques)	Exfiltration (9 techniques)	Impact (14 techniques)
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/6)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (1/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Acquire Infrastructure (2/8)	Drive-by Compromise	Command and Scripting Interpreter (4/10)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Brute Force (0/4)	Communication Through Removable Media	Data Transfer Size Limits (0/3)	Data Destruction
Gather Victim Identity Information (1/3)	Compromise Accounts (2/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (2/14)	Account Manipulation (0/6)	BITS Jobs	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Credentials from Password Stores (0/6)	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/6)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Exploitation for Credential Access	Data Encoding (0/2)	Exfiltration Over C2 Channel (0/3)	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Develop Capabilities (1/4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Autostart Execution (2/14)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (3/8)	Forced Authentication	Data Obfuscation (0/3)	Exfiltration Over C2 Channel (0/3)	Defacement (0/2)
Phishing for Information (0/4)	Establish Accounts (2/3)	Phishing (2/4)	Inter-Process Communication (1/3)	Compromise Host Software Binary	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Forge Web Credentials (0/2)	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Obtain Capabilities (1/7)	Replication Through Removable Media	Native API	Create Account (0/3)	Boot or Logon Initialization Scripts (0/5)	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Input Capture (0/4)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Stage Capabilities (2/6)	Supply Chain Compromise (1/3)	Scheduled Task/Job (1/5)	Create or Modify System Process (1/5)	Create or Modify System Process (1/5)	Direct Volume Access	Modify Authentication Process (0/9)	Container and Resource Discovery	Taint Shared Content	Modify Authentication Process (0/9)	Data from Cloud Storage	Exfiltration Over Physical Medium (0/1)	Financial Theft
Search Open Websites/Domains (0/3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (2/16)	Domain or Tenant Policy Modification (0/2)	Domain or Tenant Policy Modification (0/2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Multi-Factor Authentication Interception	Data from Configuration Repository (0/2)	Exfiltration Over Physical Medium (0/1)	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (1/4)	Shared Modules	External Remote Services	Escape to Host (0/2)	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Multi-Factor Authentication Request Generation	Data from Information Repositories (0/3)	Exfiltration Over Web Service (1/4)	Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (0/13)	Event Triggered Execution (2/16)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Network Sniffing	Data from Local System	Exfiltration Over Web Service (1/4)	Network Denial of Service (0/2)
			System Services (0/2)	Implant Internal Image	Exploitation for Privilege Escalation	File and Directory Permissions Modification (0/2)	OS Credential Dumping (1/8)	File and Directory Discovery		OS Credential Dumping (1/8)	Data from Network Shared Drive	Scheduled Transfer	Resource Hijacking
			User Execution (2/3)	Modify Authentication Process (0/9)	Hijack Execution Flow (0/13)	Hide Artifacts (0/12)	Steal Application Access Token	Group Policy Discovery		Steal Application Access Token	Data from Network Shared Drive	Transfer Data to Cloud Account	Service Stop
			Windows Management Instrumentation	Office Application Startup (0/6)	Process Injection (1/12)	Hijack Execution Flow (0/13)	Steal or Forge Authentication Certificates	Log Enumeration		Steal or Forge Authentication Certificates	Data from Removable Media		System Shutdown/Reboot
				Power Settings	Scheduled Task/Job (1/5)	Impair Defenses (0/11)	Steal or Forge Kerberos Tickets (1/4)	Network Service Discovery		Steal or Forge Kerberos Tickets (1/4)	Data Staged (2/2)		
				Pre-OS Boot (0/5)	Valid Accounts (1/4)	Impersonation	Steal Web	Network Share Discovery		Steal Web	Email Collection (0/3)		
						Indicator Removal (0/9)		Network Sniffing			Input Capture (0/4)		
						Indirect Command Execution		Password Policy Discovery			Screen Capture		
						Masquerading (2/9)		Peripheral Device Discovery			Video Capture		
						Modify Authentication Process (0/9)		Permission Groups Discovery (1/3)					
						Modify Cloud Compute Infrastructure (0/5)		Process Discovery					

Potential targets for railway industry:

Signaling/switching

Dispatch

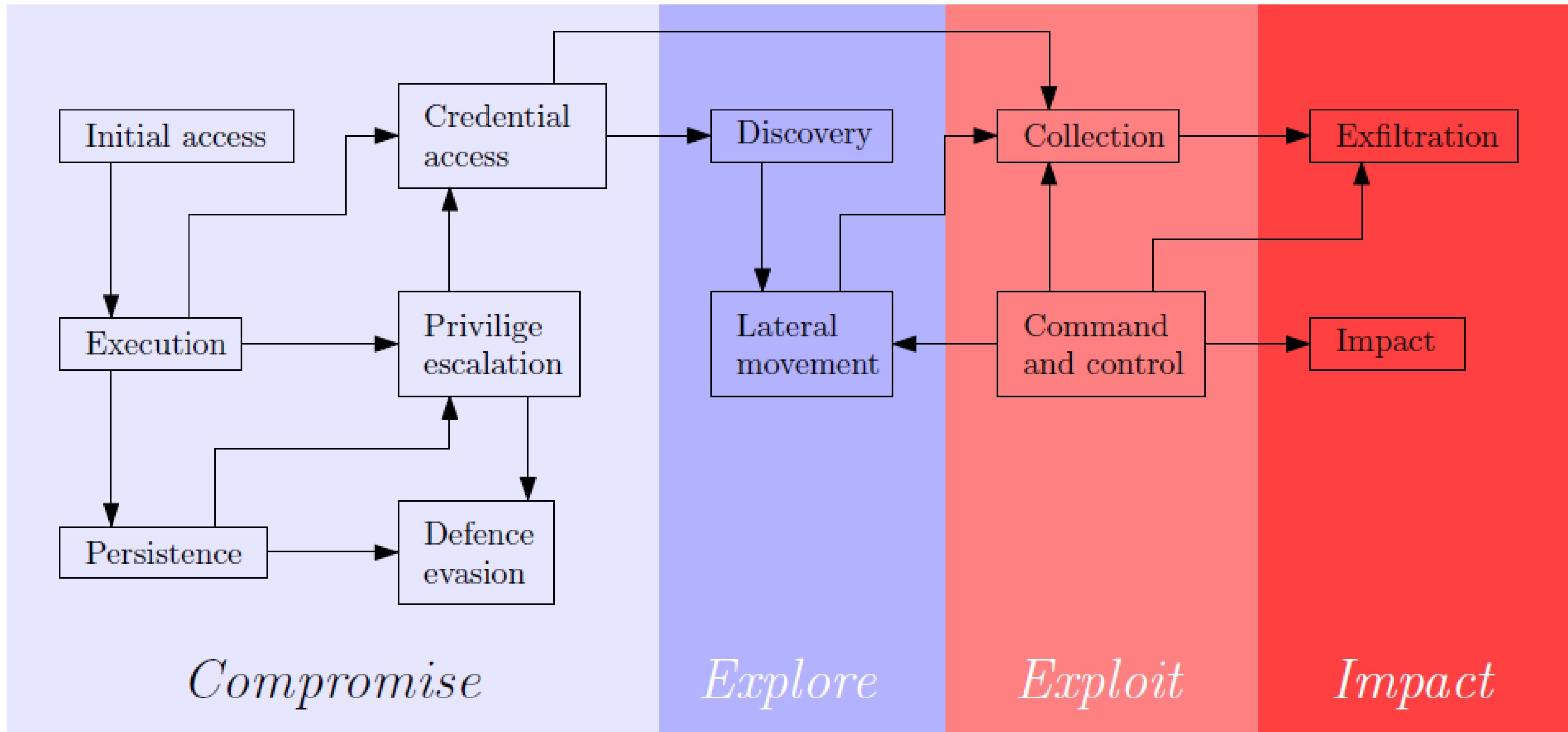
Locomotion

Ticketing

Data Collection

PTC

Utilities -



Bayesian Networks

Intersection between statistics, graph theory, and machine learning

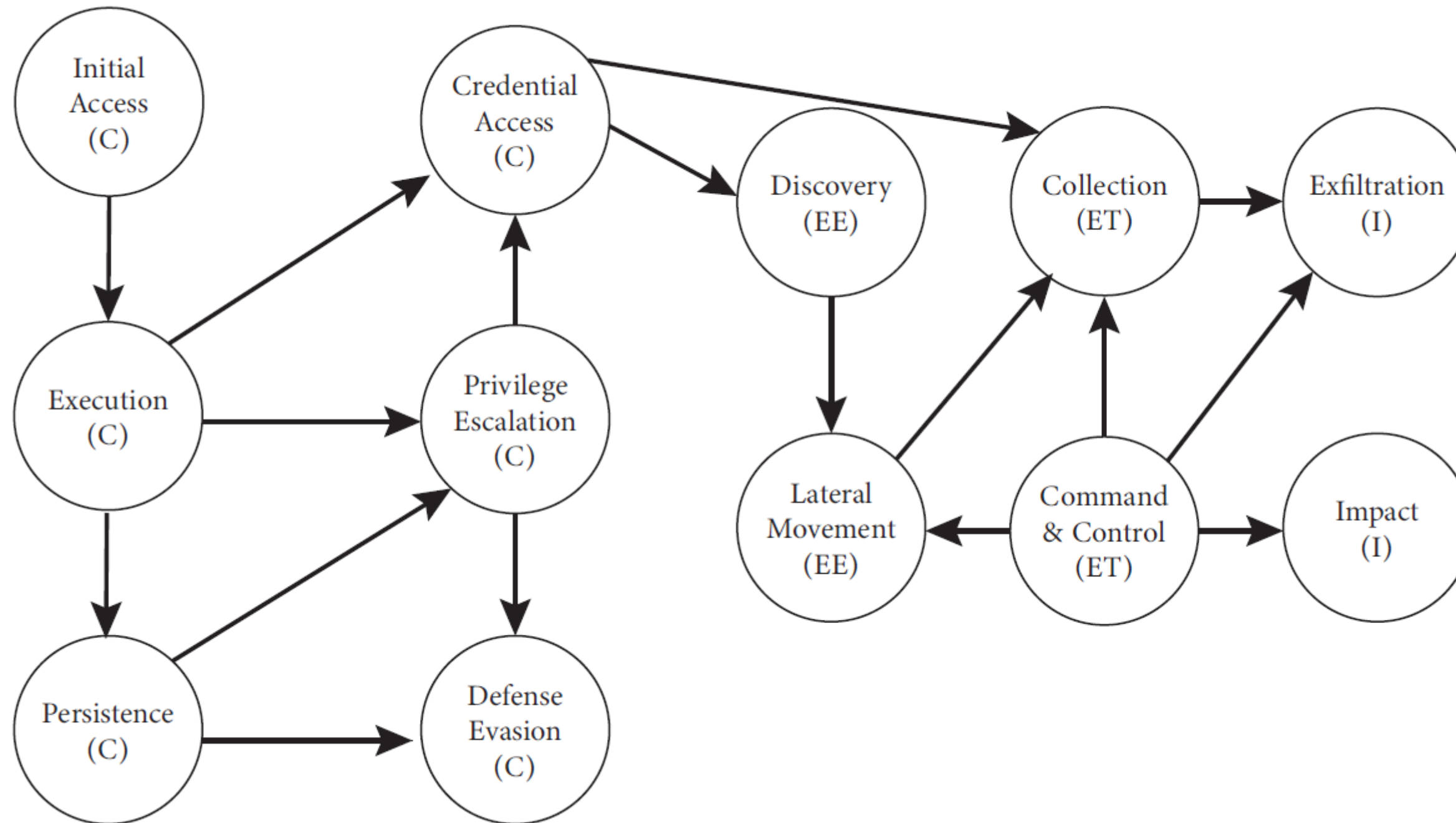
Consist of

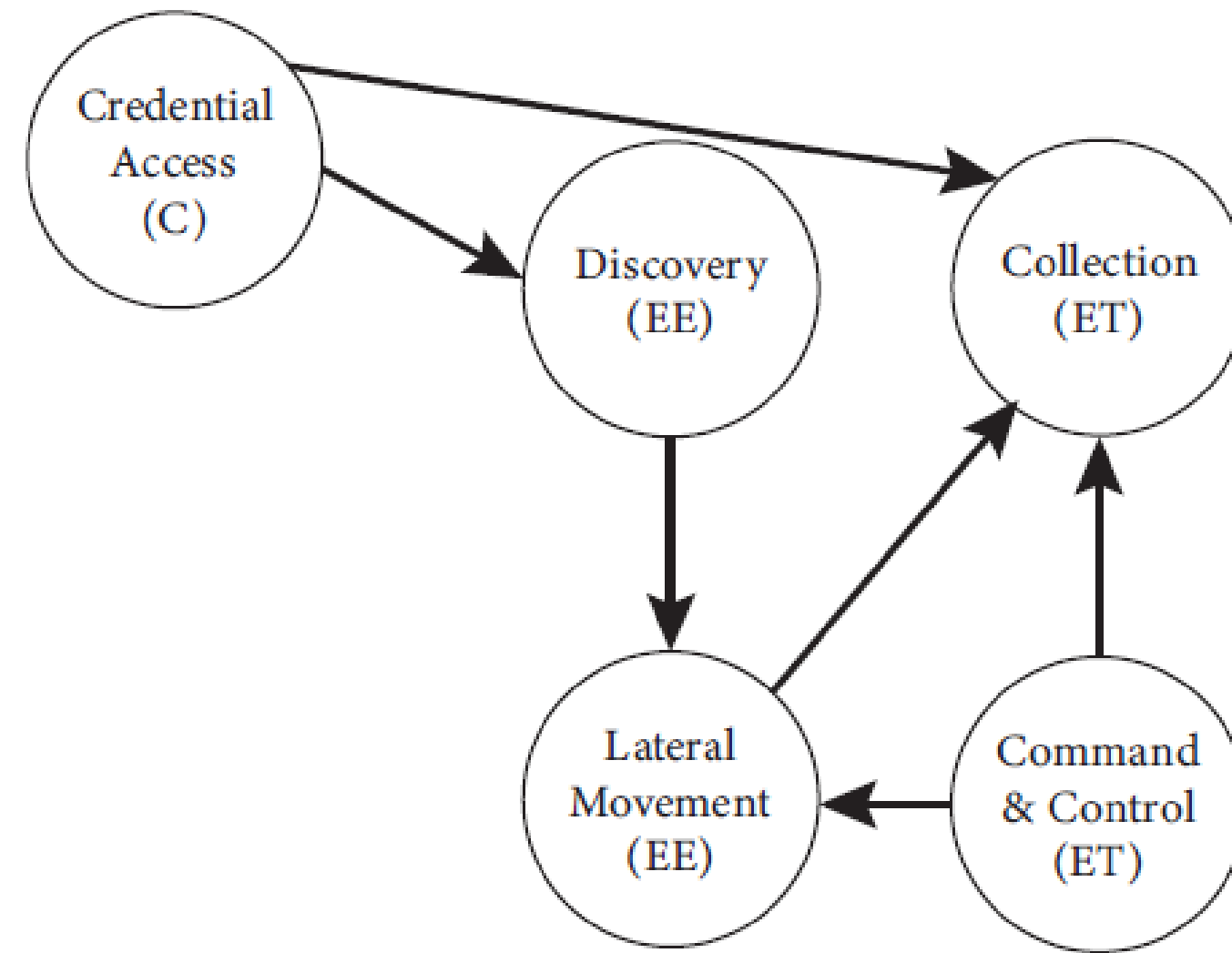
- **a set of nodes, corresponding to variables**
- **a set of edges, indicating dependency**
- **a set of functions defined on the graph that specify a probability distribution**

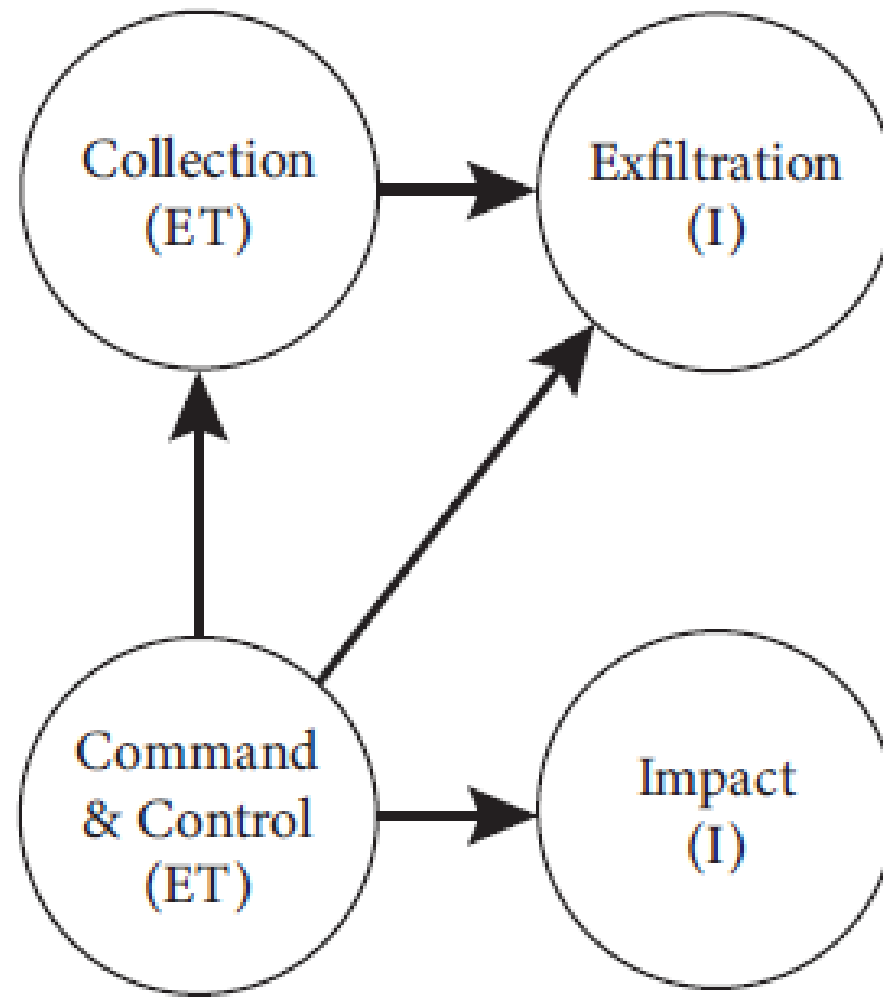
Bayesian Networks

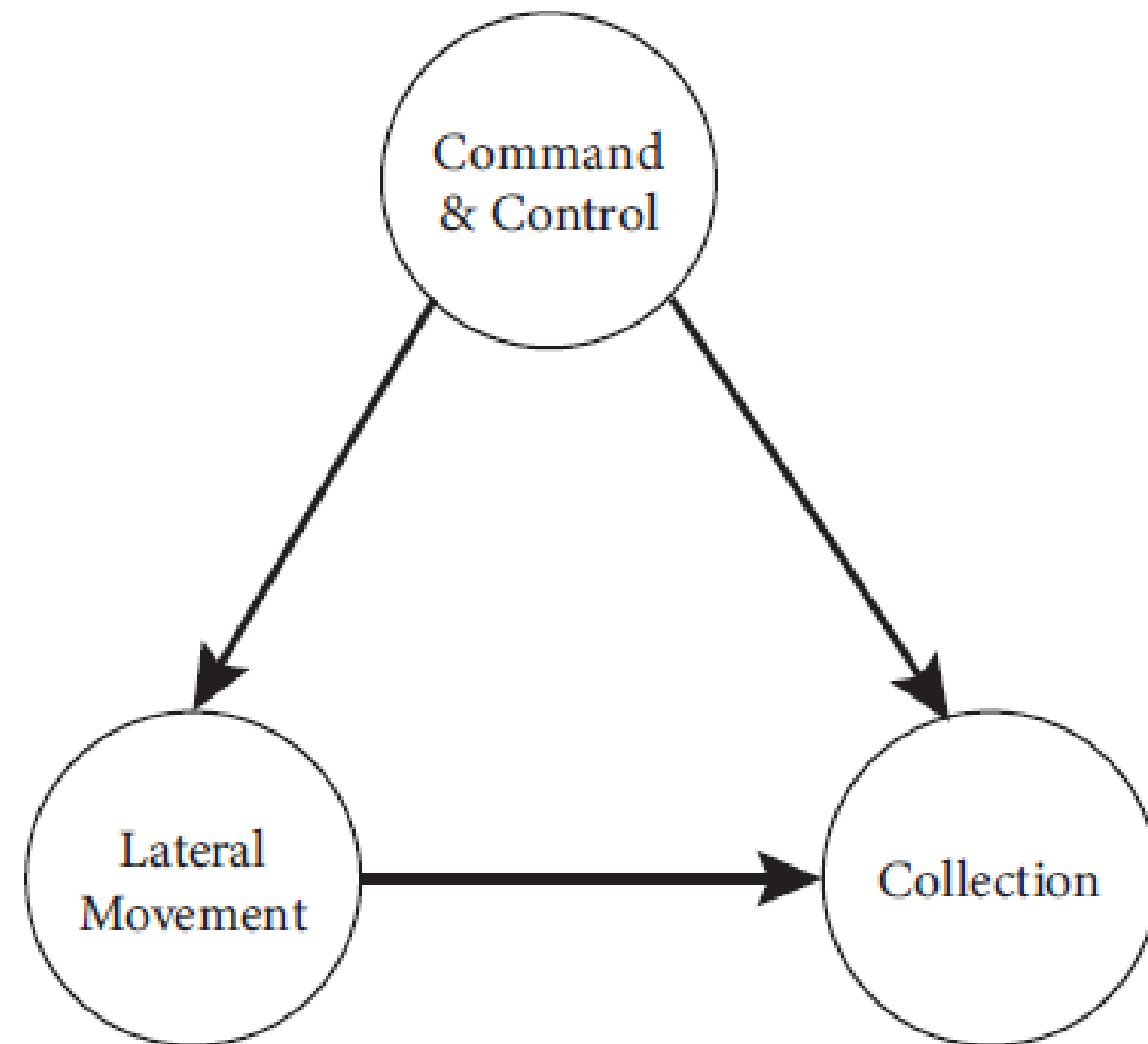
Intersection between statistics, graph theory, and machine learning

- *Data Gathering*
- *Probabilistic/Uncertainty*
- *What if –Scenarios*
- *Dynamic Bayesian Networks*









Node	Scenario 1	Scenario 2	Scenario 3
Command & Control	High	High	High
Lateral Movement	Medium	Low	High
Collection	Low	Medium	High



THANK YOU -

References

Maccarone T, Buede DM, Bowman ST, Burdick CD, Bracken MC, Jones JM, Weaver GA. Development of a Bayesian Network to Model Malicious Cyber-Activity in Operational Technology Environments. 16th Bayesian Modelling Applications Workshop. 2022

Xie P, Li JH, Ou X, Liu P, Levy R. Using Bayesian Networks for Cyber Security Analysis. 2010 IEEE/IFIP International Conf on Dependable Systems & Networks

Kim Y, Lee I, Kwon H, Lee K, Yoon J. BAN: Predicting APT Attack Based on Bayesian Network with MITRE ATT&ck Framework. IEEE 2023