MITRE ATT&CK Framework

Digital and Cyber Railway Engineering and Operations Center (DCREOC)

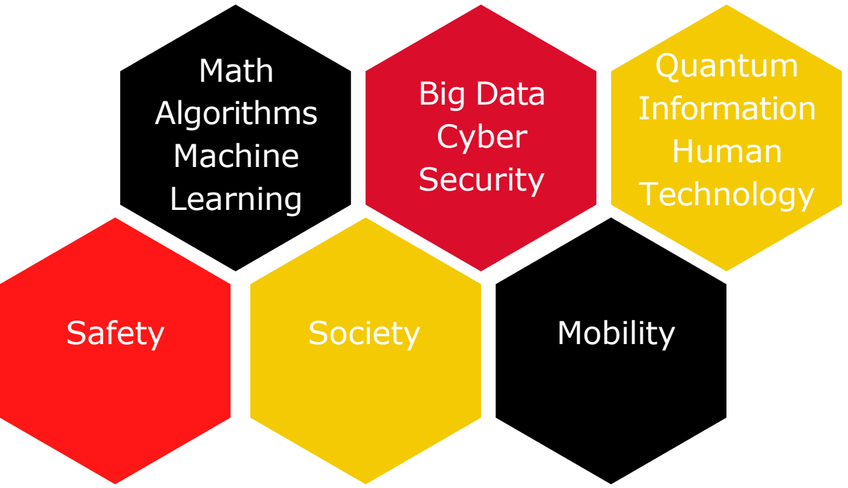
Nii O. Attoh-Okine, PhD., P.E., F. ASCE
Professor and Chair
Department of Civil and Environmental Engineering
University of Maryland
College Park, MD

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

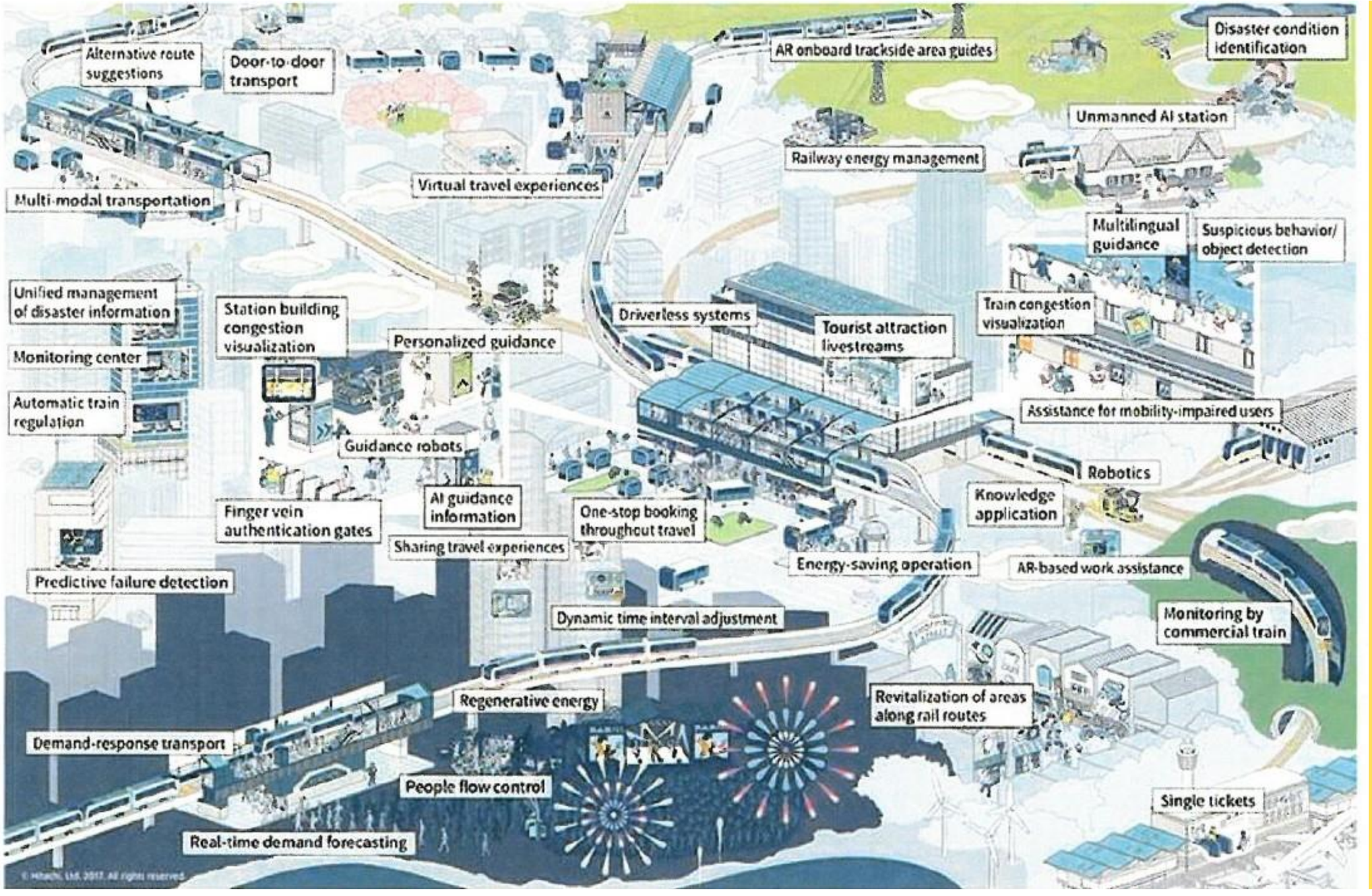


Applied Research

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

Education

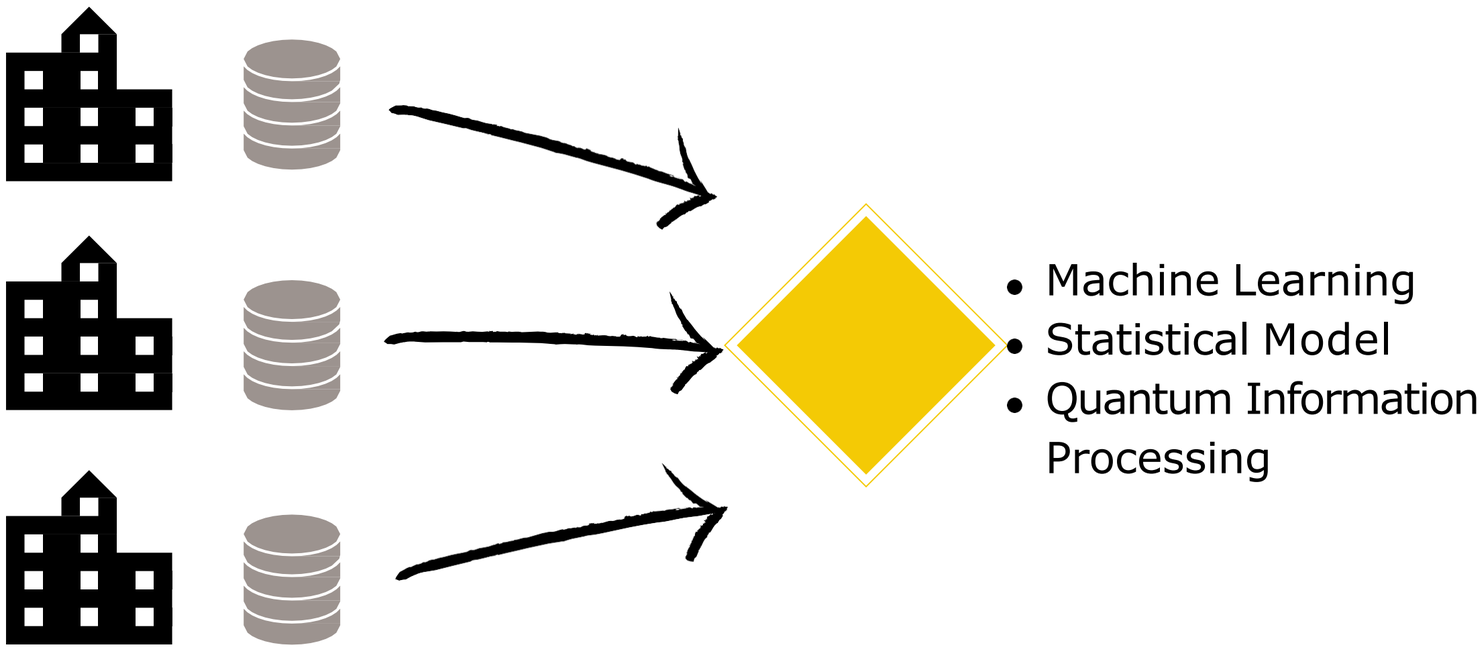
- Training of Students and Railway Professionals in the Area of Digital and Cyber Issues
- Short Courses in Digital and Cyber Railway Issues


Alternative route suggestions
Door-to-door transport
AR onboard trackside area guides
Disaster condition identification
Unmanned AI station
Railway energy management
Virtual travel experiences
Multi-modal transportation
Multilingual guidance
Suspicious behavior/ object detection
Unified management of disaster information
Station building congestion visualization
Driverless systems
Tourist attraction livestreams
Train congestion visualization
Personalized guidance
Monitoring center
Automatic train regulation
Assistance for mobility-impaired users
Guidance robots
Robotics
Knowledge application
AI guidance information
Finger vein authentication gates
One-stop booking throughout travel
Sharing travel experiences
Energy-saving operation
AR-based work assistance
Predictive failure detection
Dynamic time interval adjustment
Monitoring by commercial train
Regenerative energy
Revitalization of areas along rail routes
Demand-response transport
People flow control
Single tickets
Real-time demand forecasting

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

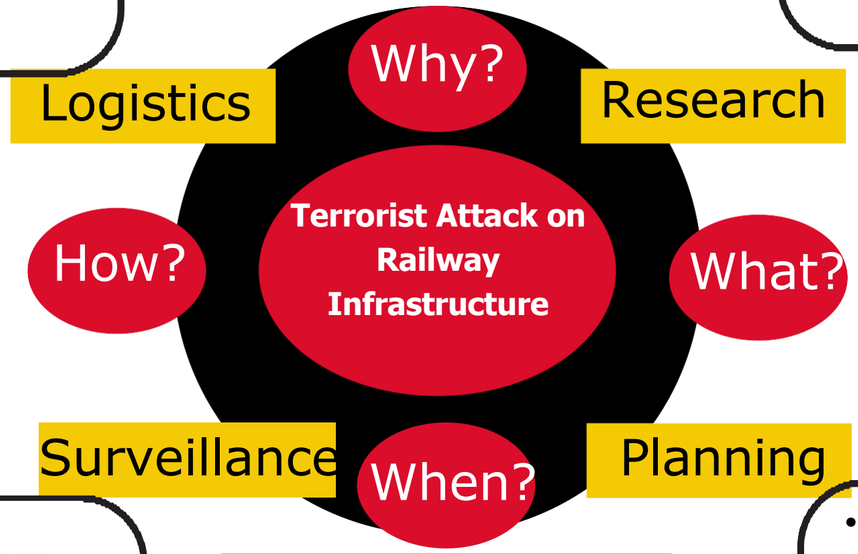
General Goal

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



- Equipment
- Weaponry
- Uniforms
- Special vehicles
- Data access
- Maps and plans
- Google Earth

- Perceived response to overseas engagement
- Religious motives
- Political motives
- Solo attacker aggrieved by social position
- Radicalised (young) people

- Target identification
- critical infrastructure
- attack technologies
- attack methods (explosives, CBRM, etc.)
- IT technologies (cyber)
- Terrorist education and training

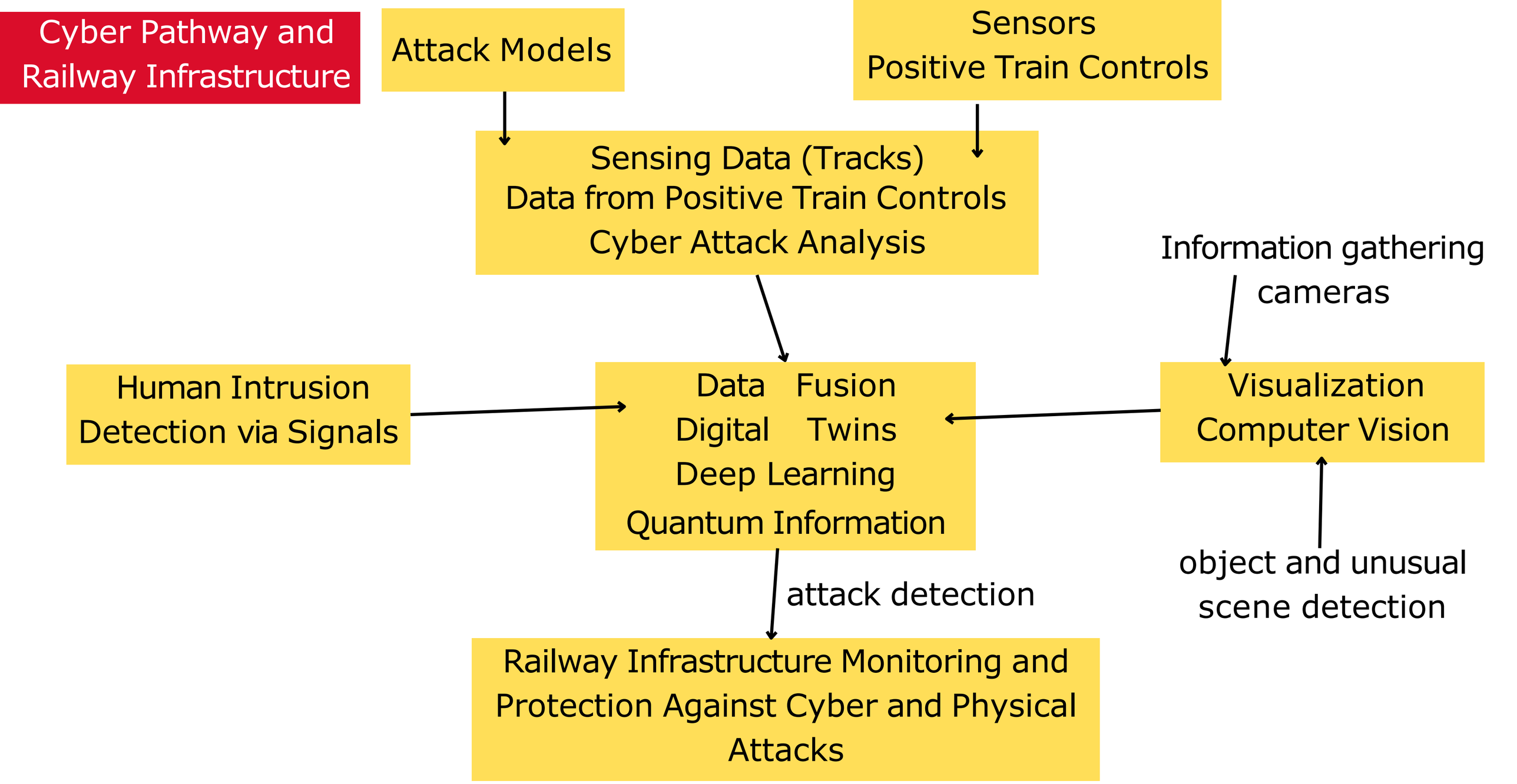
- Physical (IED, suicide attack, explosion on timer)
- Cyber (SCADA, computer operating system)
- CBRN (toxic substance, gas)
- Facility damage to SPOFs

- Visibility/media focus
- Accessibility (hard/soft target)
- Terrorist capabilities
- Impact on economy, social life, cultural values, national icons
- Extent of casualties

- Photographs/videos
- Record security and staff movement
- Record work schedules and shift changes
- Dry run in car and/or foot

- Busy time for maximum interdependency effect, for example, peak demand period (within a day, a week, a season, or a year)
- During a non-related event
- Off-business time (weekend, public holiday)

- Building/facilities plans
- Trusted insider
- Identification of SPOFs
- Team structure and task allocation
- Timing evaluation and rehearsal
- Finances and budget


Cyber Pathway and Railway Infrastructure
Attack Models
Sensors
Positive Train Controls
Sensing Data (Tracks)
Data from Positive Train Controls
Cyber Attack Analysis
Information gathering
cameras
Human Intrusion
Detection via Signals
Data Fusion
Digital Twins
Deep Learning
Quantum Information
Visualization
Computer Vision
attack detection
object and unusual
scene detection
Railway Infrastructure Monitoring and
Protection Against Cyber and Physical
Attacks

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)

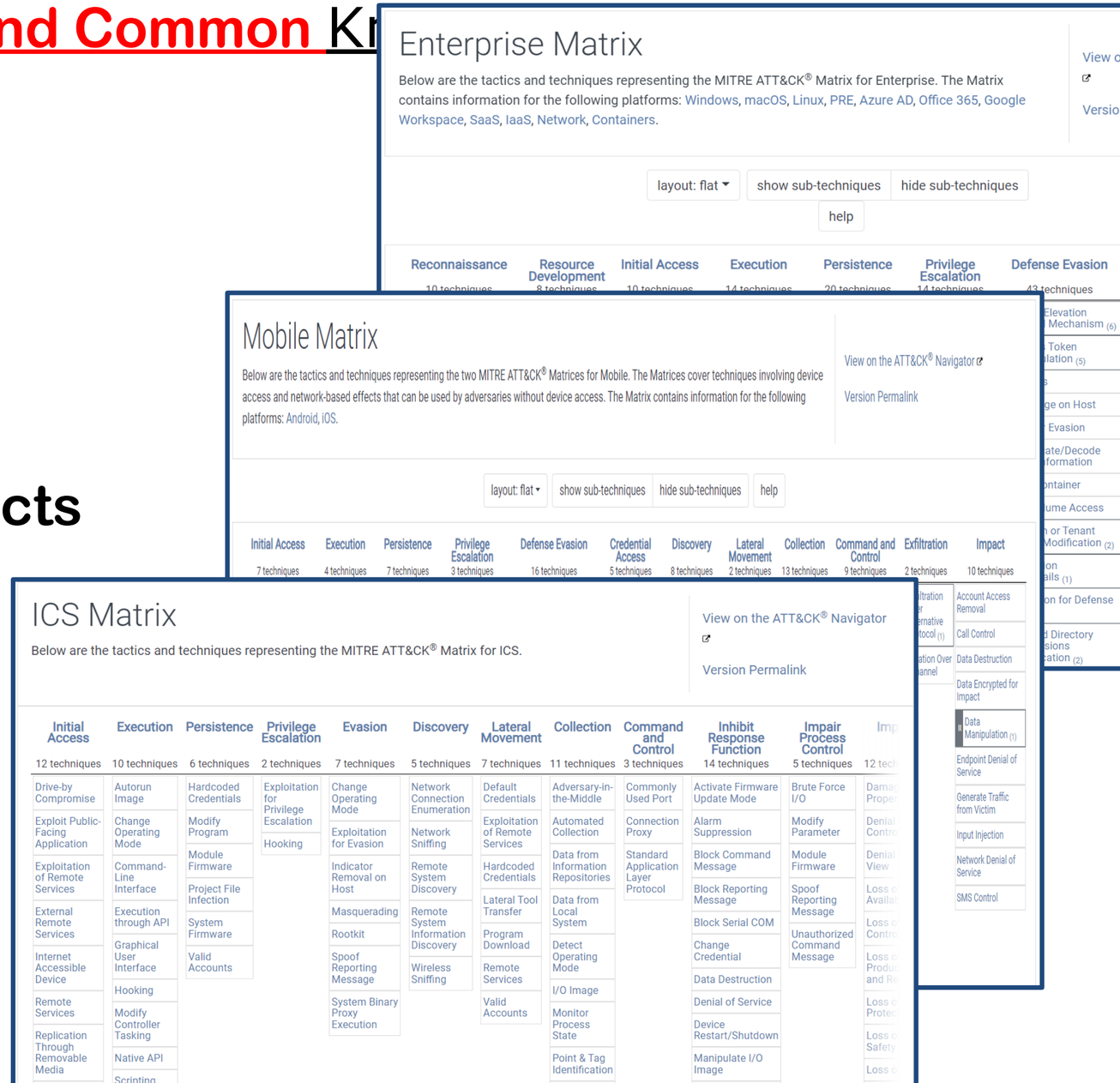
Represent fundamentally different system/device types and adversaries objectives
Each domain is associated with different tactics, techniques, and procedures (TTPs)

ATT&CK Matrix…

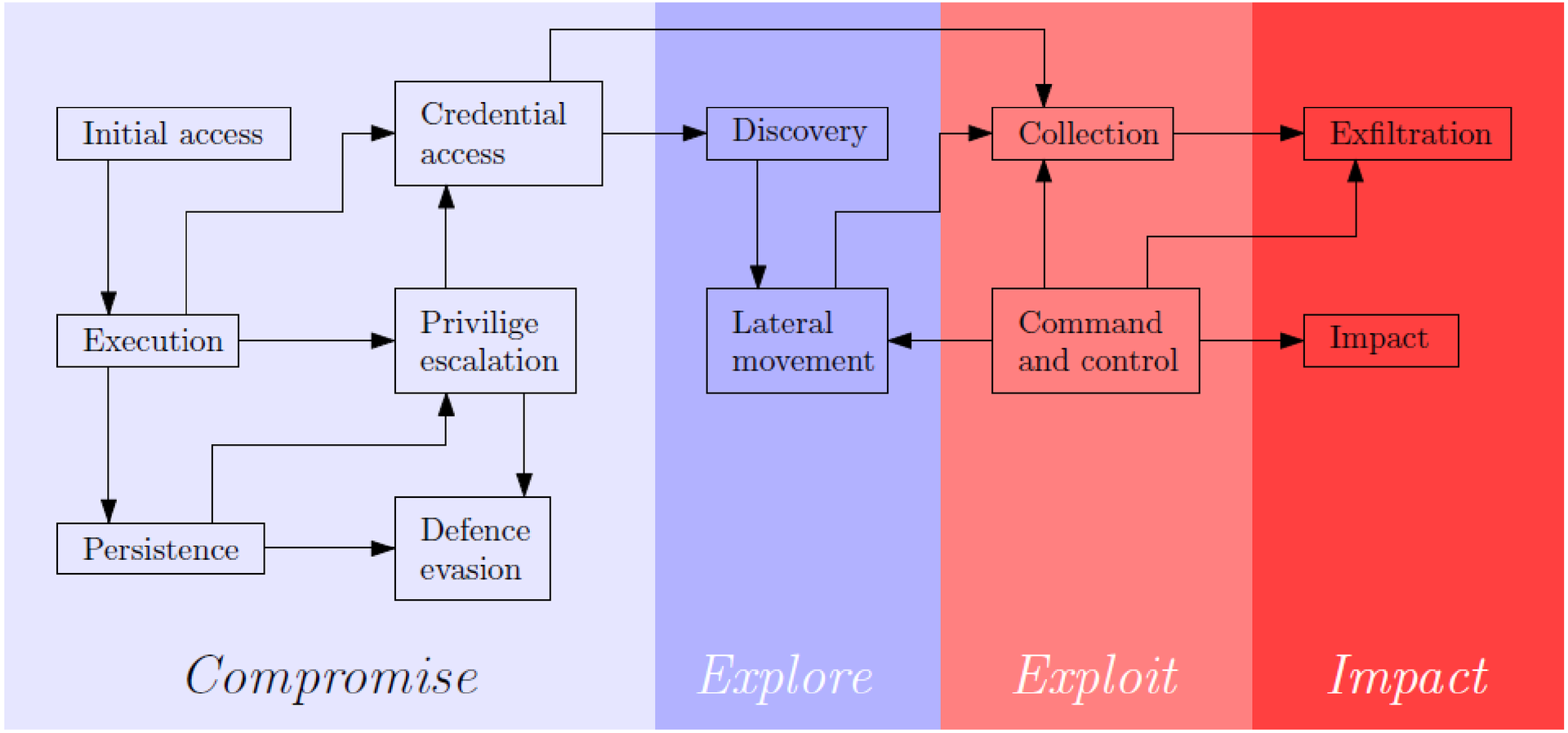
Adversarial Tactics, Techniques, and Common Kn

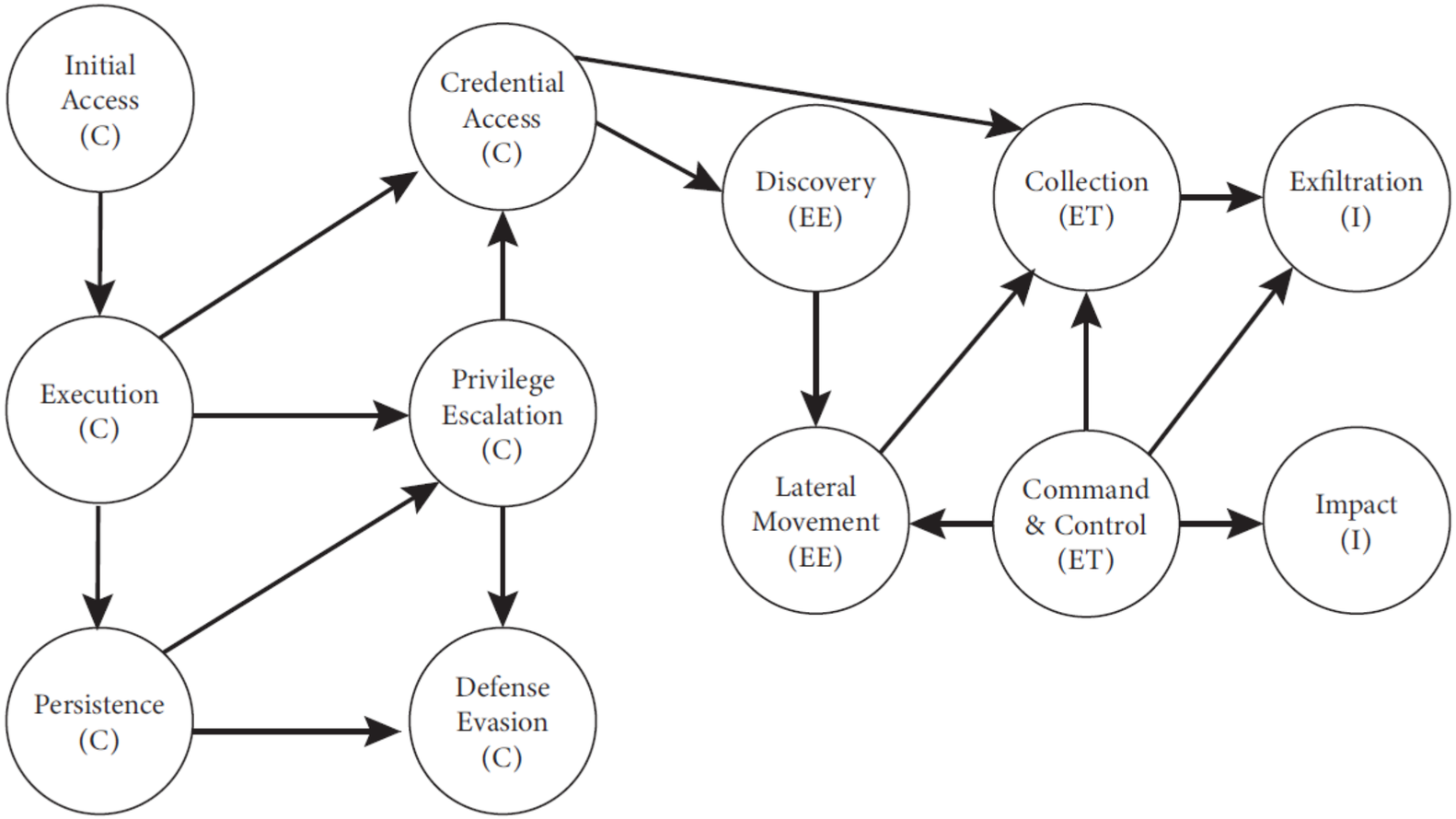
Condensed representation of framework

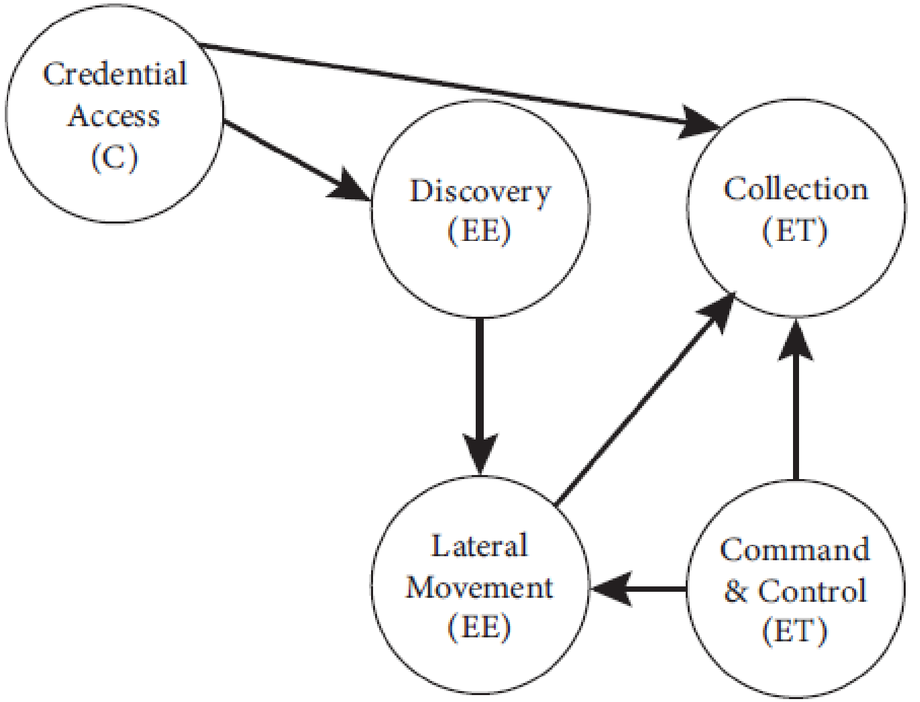
Updated twice a year – reflects evolving threat landscape

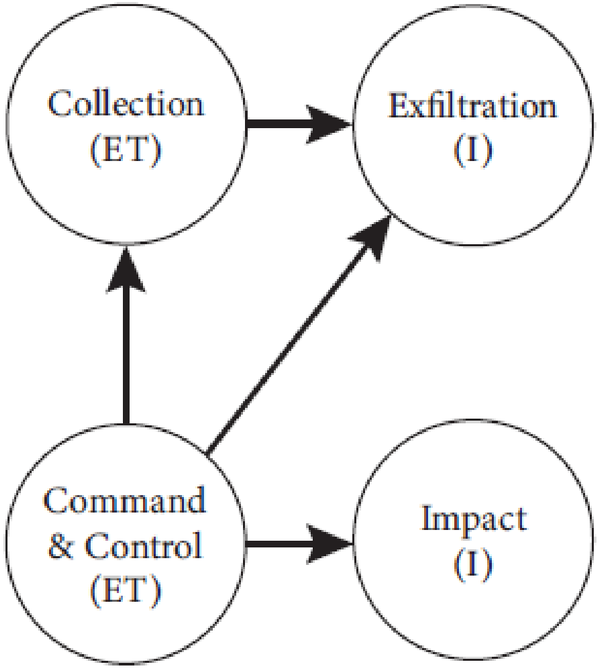


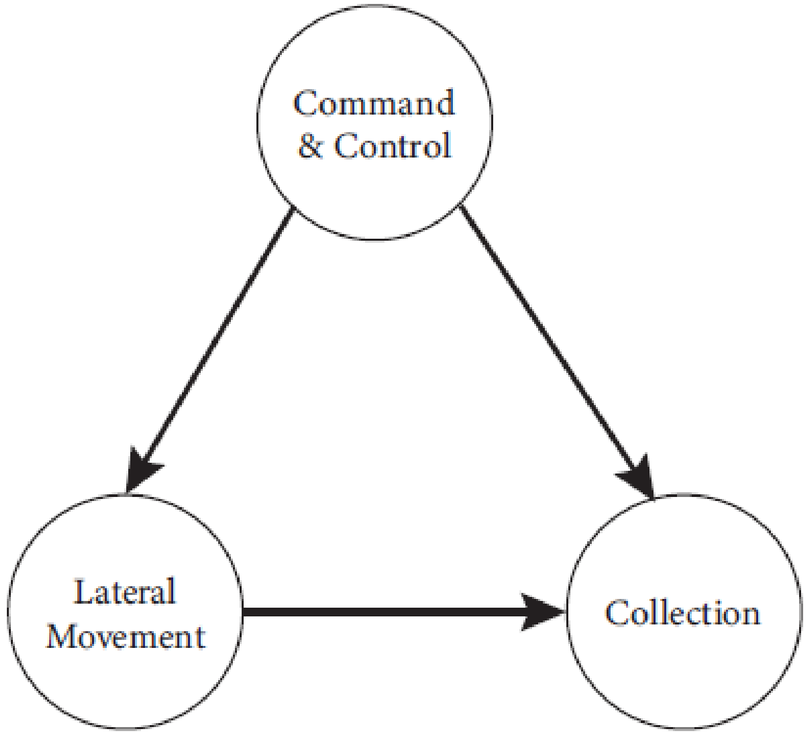
Tactics = Columns
Left to right
Represent potential phases of attack


Initial access
Credential access
Discovery
Collection
Exfiltration
Execution
Privilige escalation
Lateral movement
Command and control
Impact
Persistence
Defence evasion
Compromise
Explore
Exploit
Impact


Initial Access (C)
Credential Access (C)
Discovery (EE)
Collection (ET)
Exfiltration (I)
Execution (C)
Privilege Escalation (C)
Lateral Movement (EE)
Command & Control (ET)
Impact (I)
Persistence (C)
Defense Evasion (C)


Credential Access (C)
Discovery (EE)
Collection (ET)
Lateral Movement (EE)
Command & Control (ET)

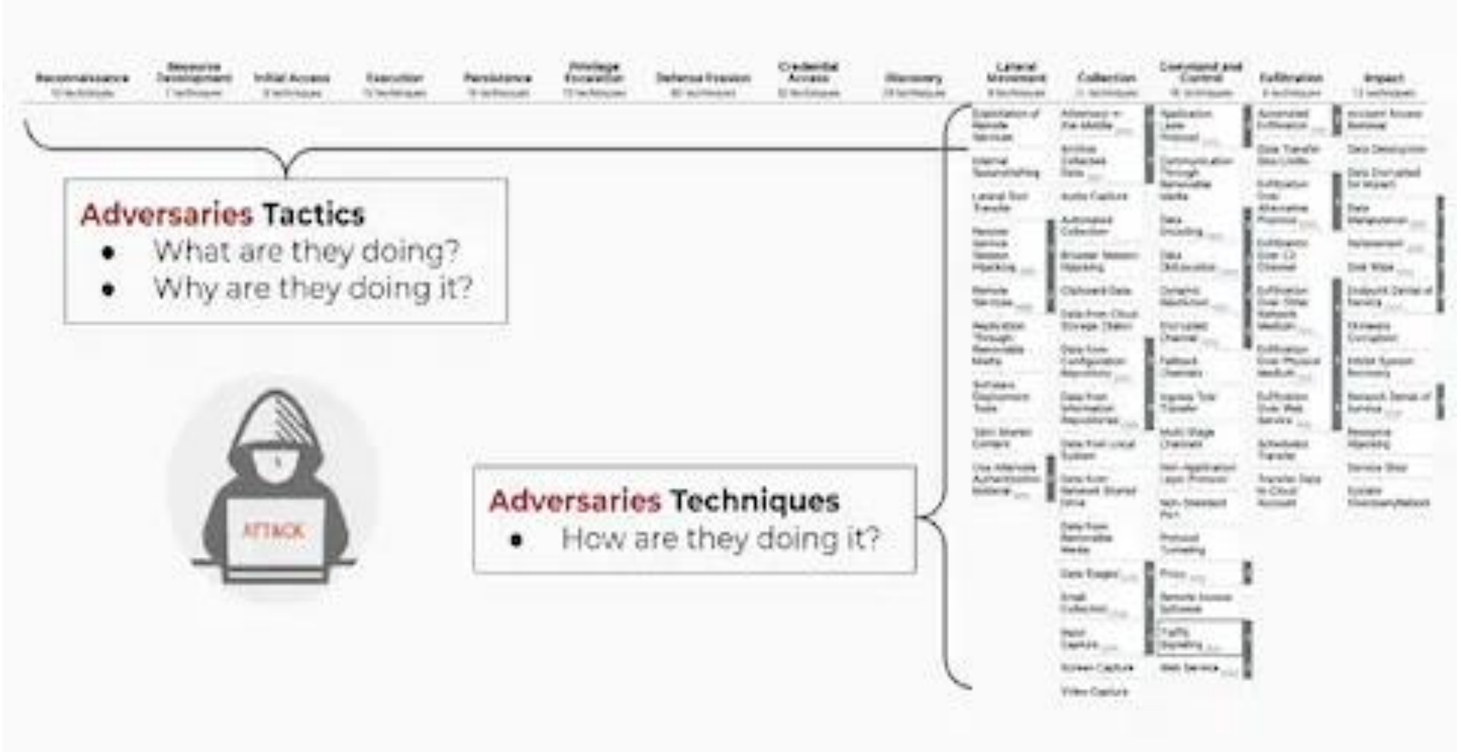

Collection
(ET)
Exfiltration
(I)
Command
& Control
(ET)
Impact
(I)


Command
& Control
Lateral
Movement
Collection

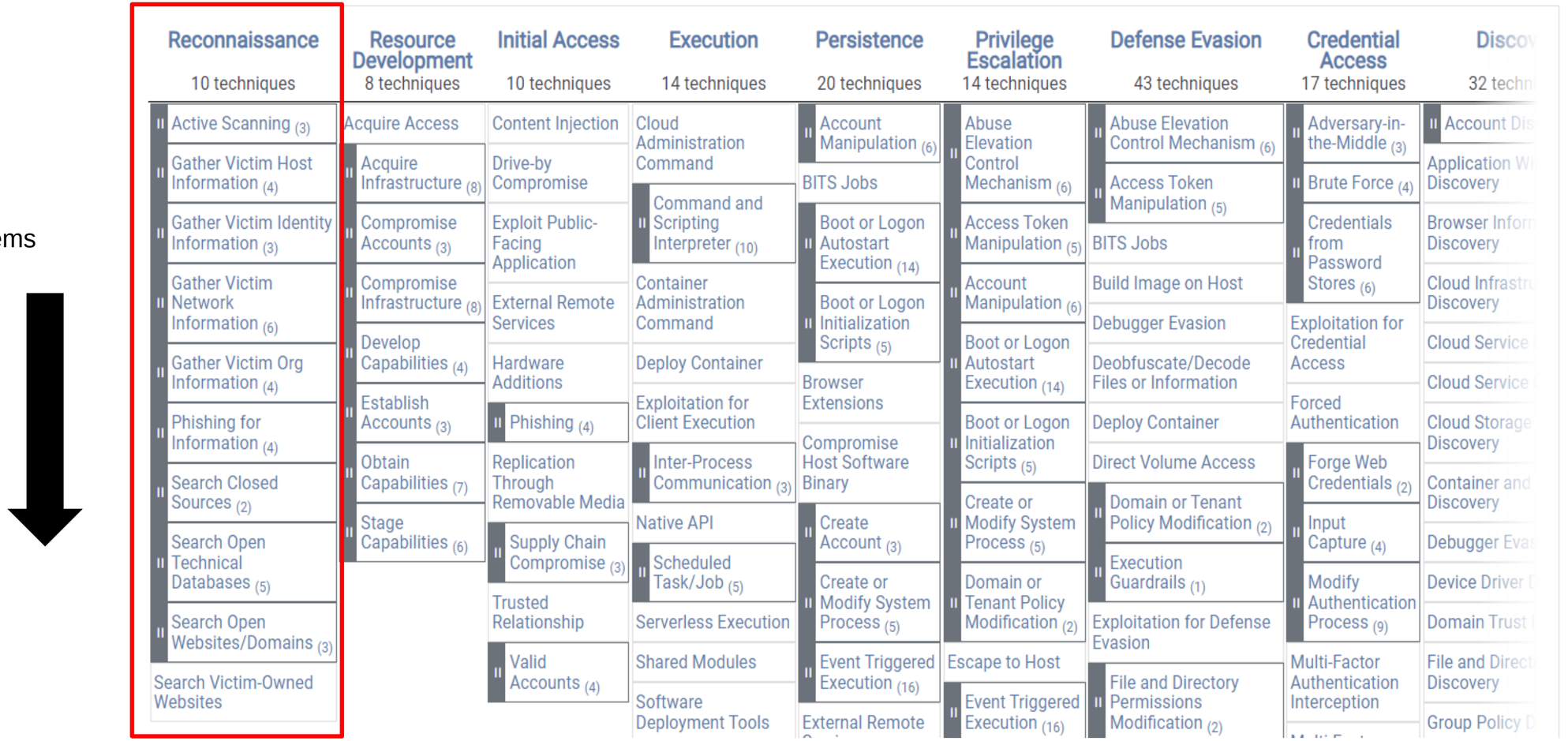
Node	Scenario 1	Scenario 2	Scenario 3
Command & Control	High	High	High
Lateral Movement	Medium	Low	High
Collection	Low	Medium	High

Adversary Tactical Goal

Tactics = “why”
Goal or Reason for performing an action

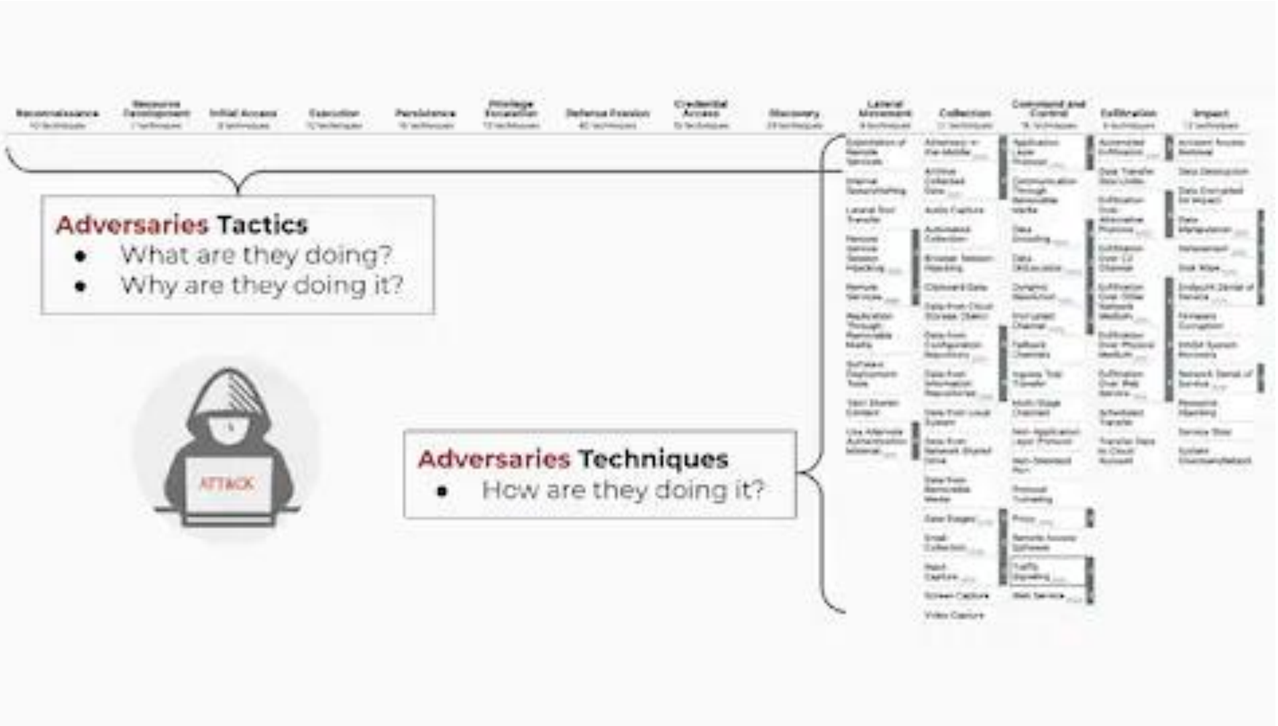


Techniques = Row items

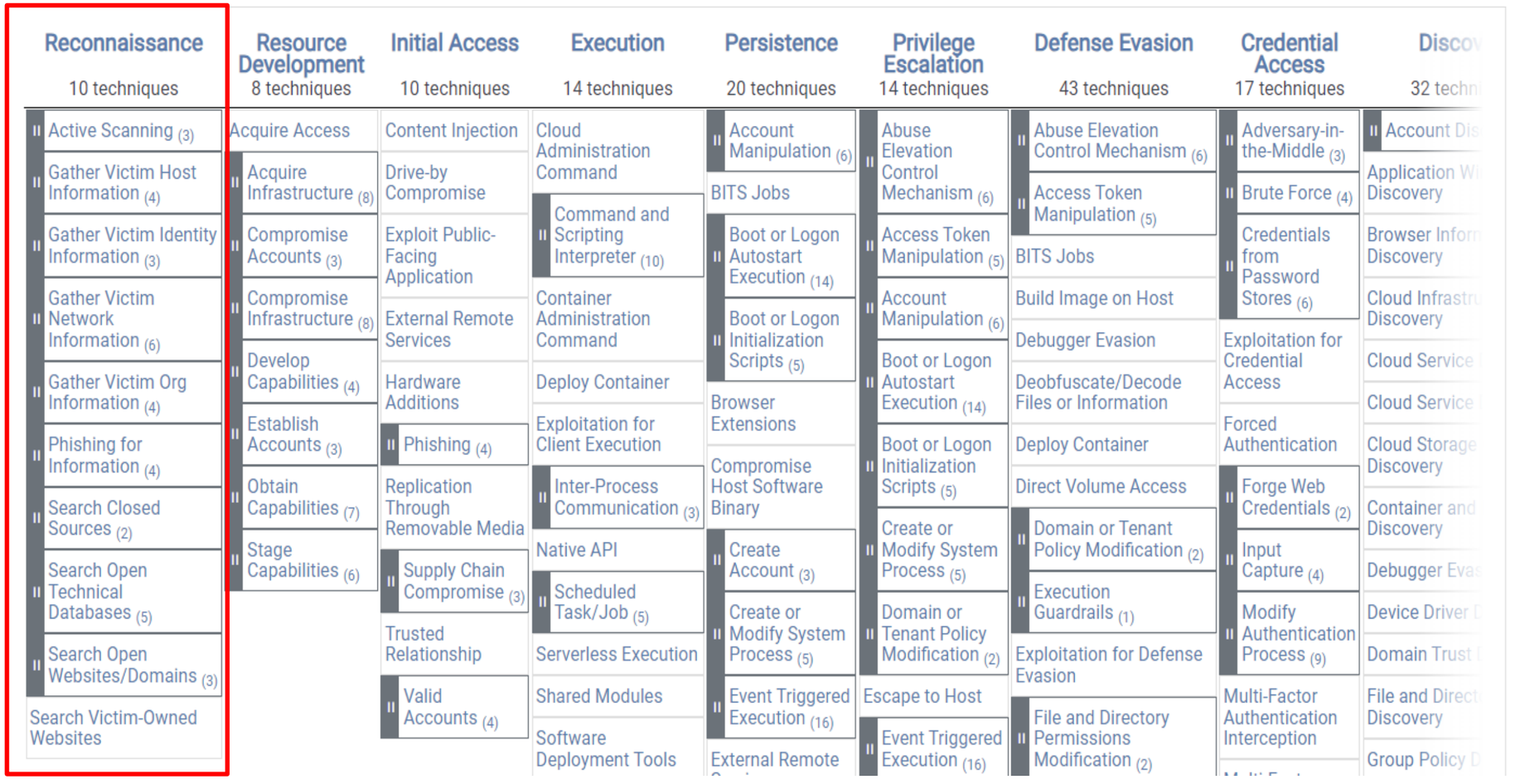


Adversary Techniques

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



Sub-Techniques = More detailed



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

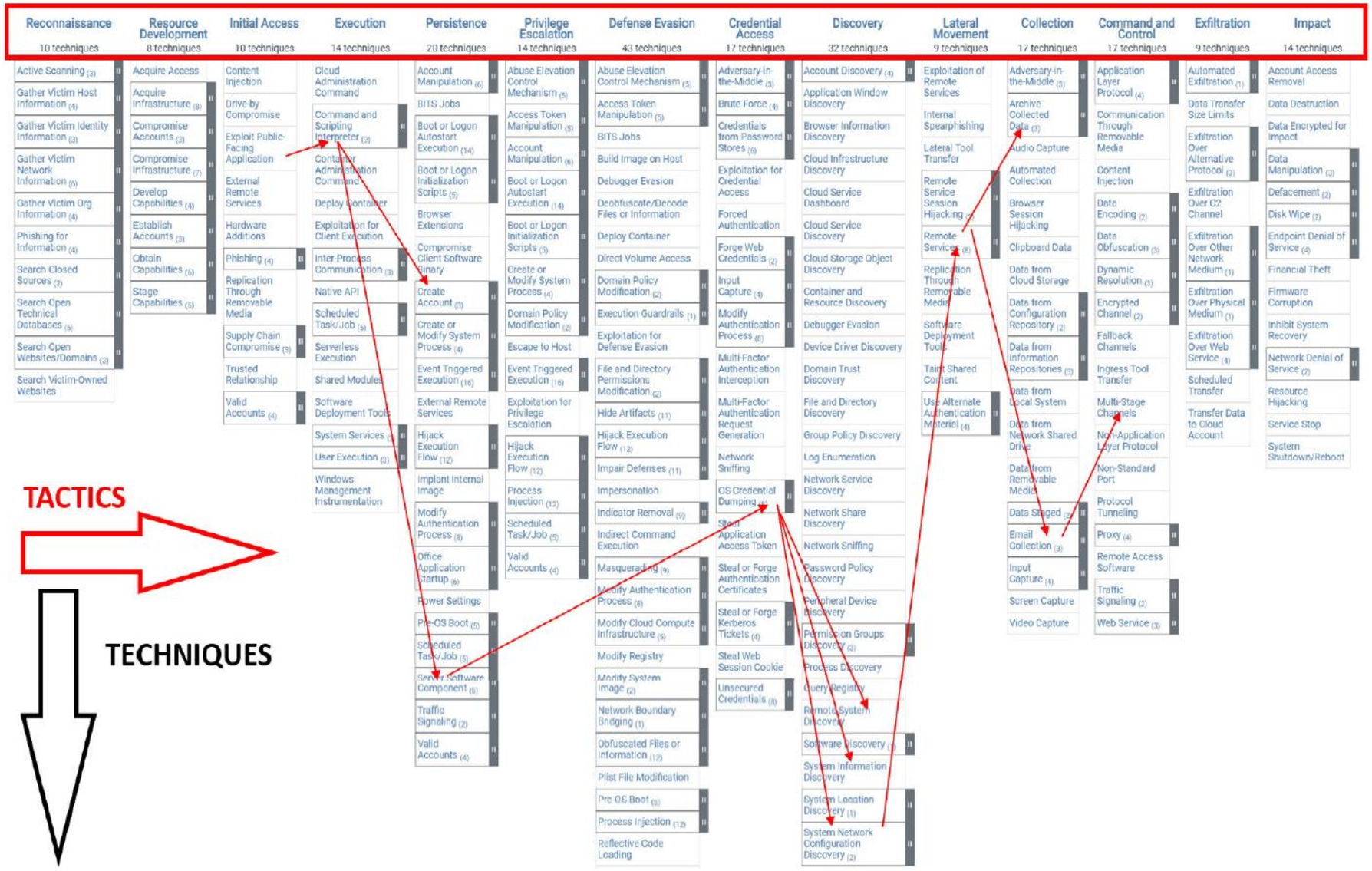
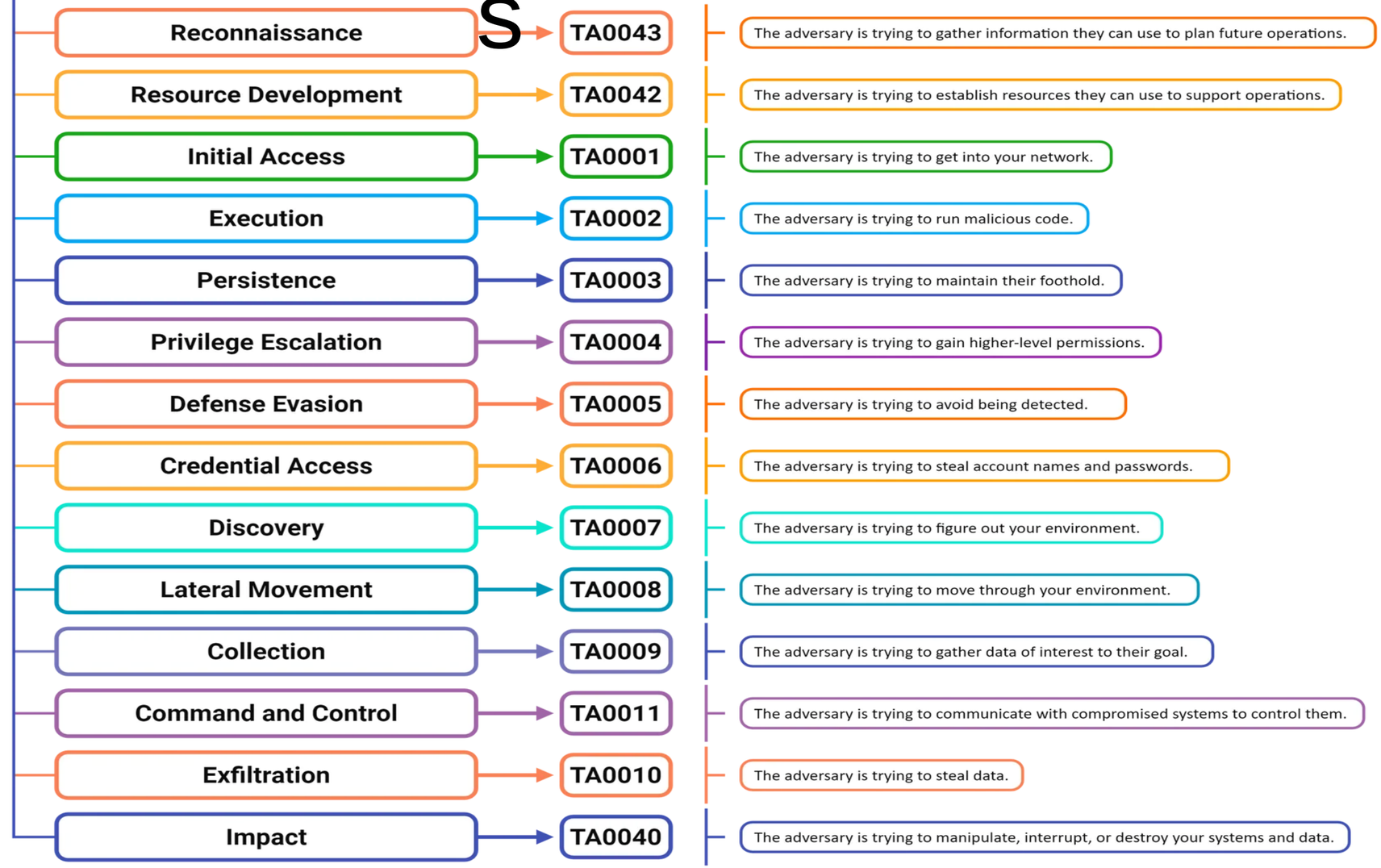


FIGURE 1. MITRE ATT&CK matrix lay-out for Enterprise domain: tactics are organized by columns while techniques by rows.

Tactics

MITRE ATT&CK Framework (Enterprise Matrix)



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

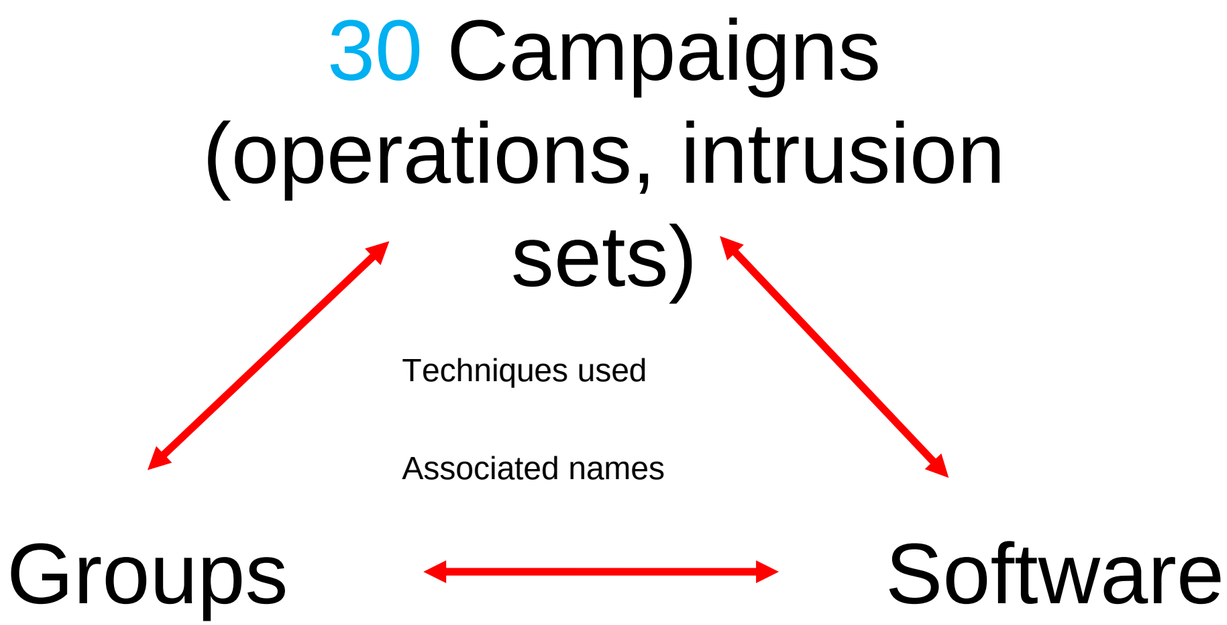
Techniques used

794 Software (Tools and Malware)

Mapped through public media reports

Campaigns

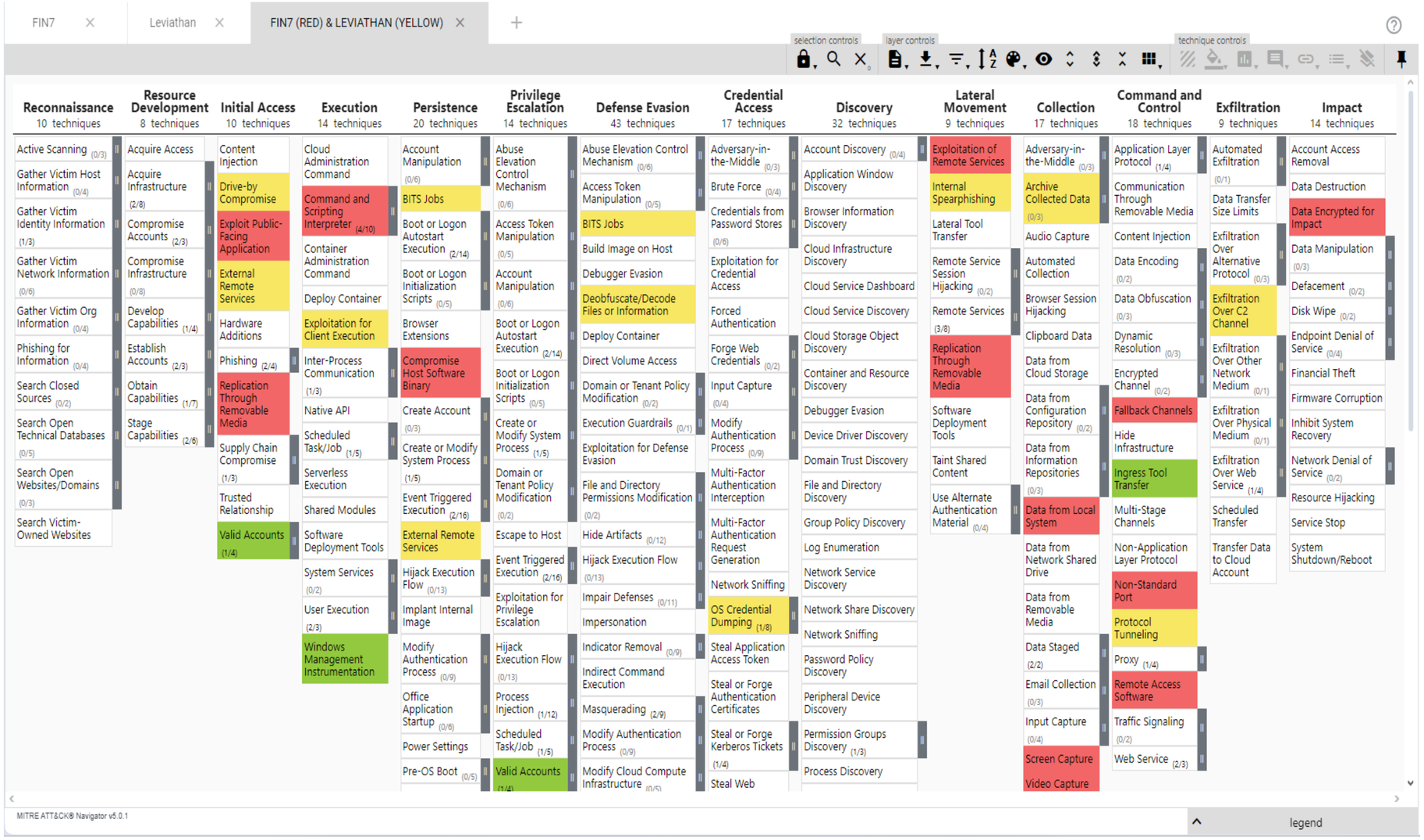
Tracked using various analytic methods



Mapped through public media reports

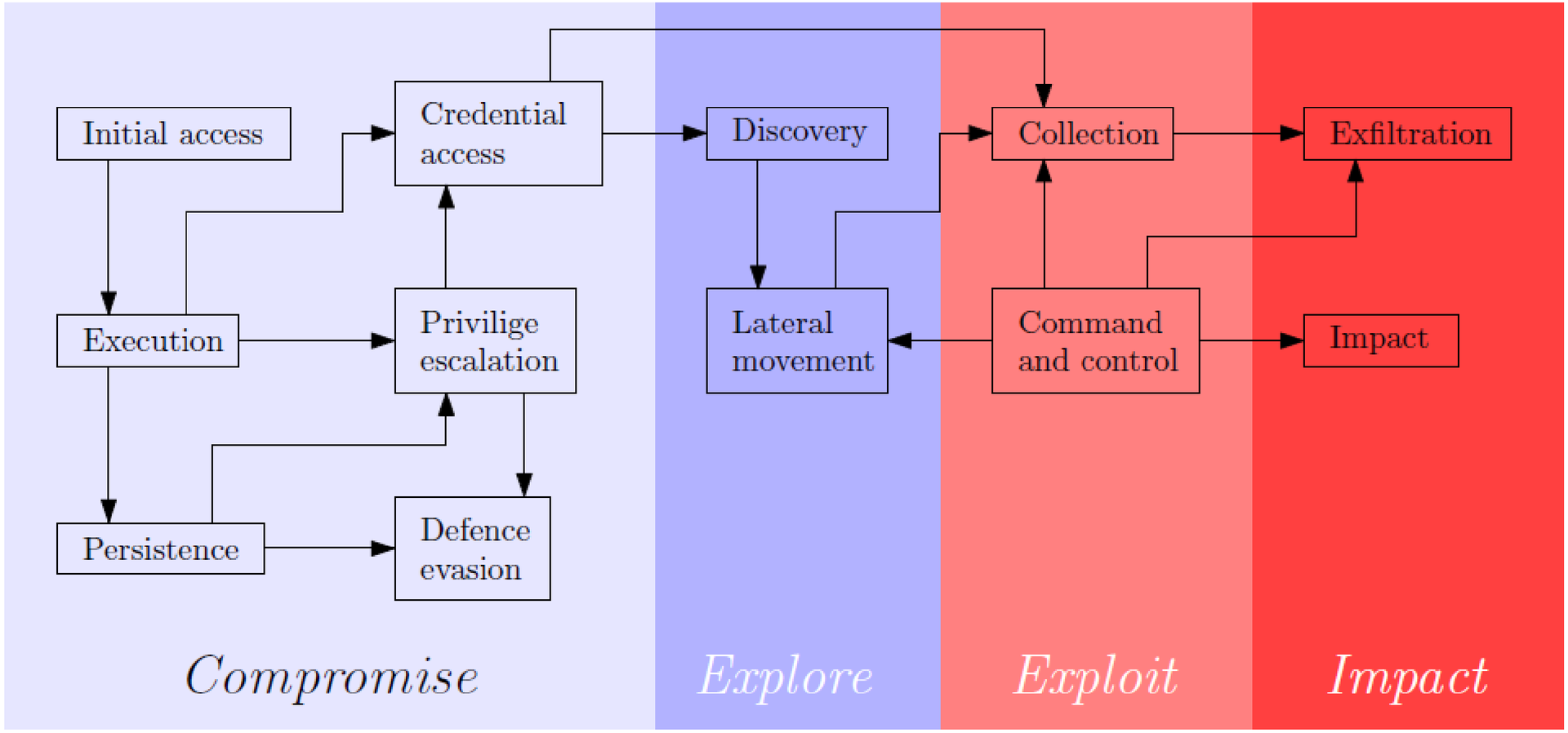
ATT&CK Navigator

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



Potential targets for railway industry:

- Signaling/switching
- Dispatch
- Locomotion
- Ticketing
- Data Collection
- PTC
- Utilities -


Initial access
Credential access
Discovery
Collection
Exfiltration
Execution
Privilige escalation
Lateral movement
Command and control
Impact
Persistence
Defence evasion
Compromise
Explore
Exploit
Impact

Bayesian Networks

Intersection between statistics, graph theory, and machine learning

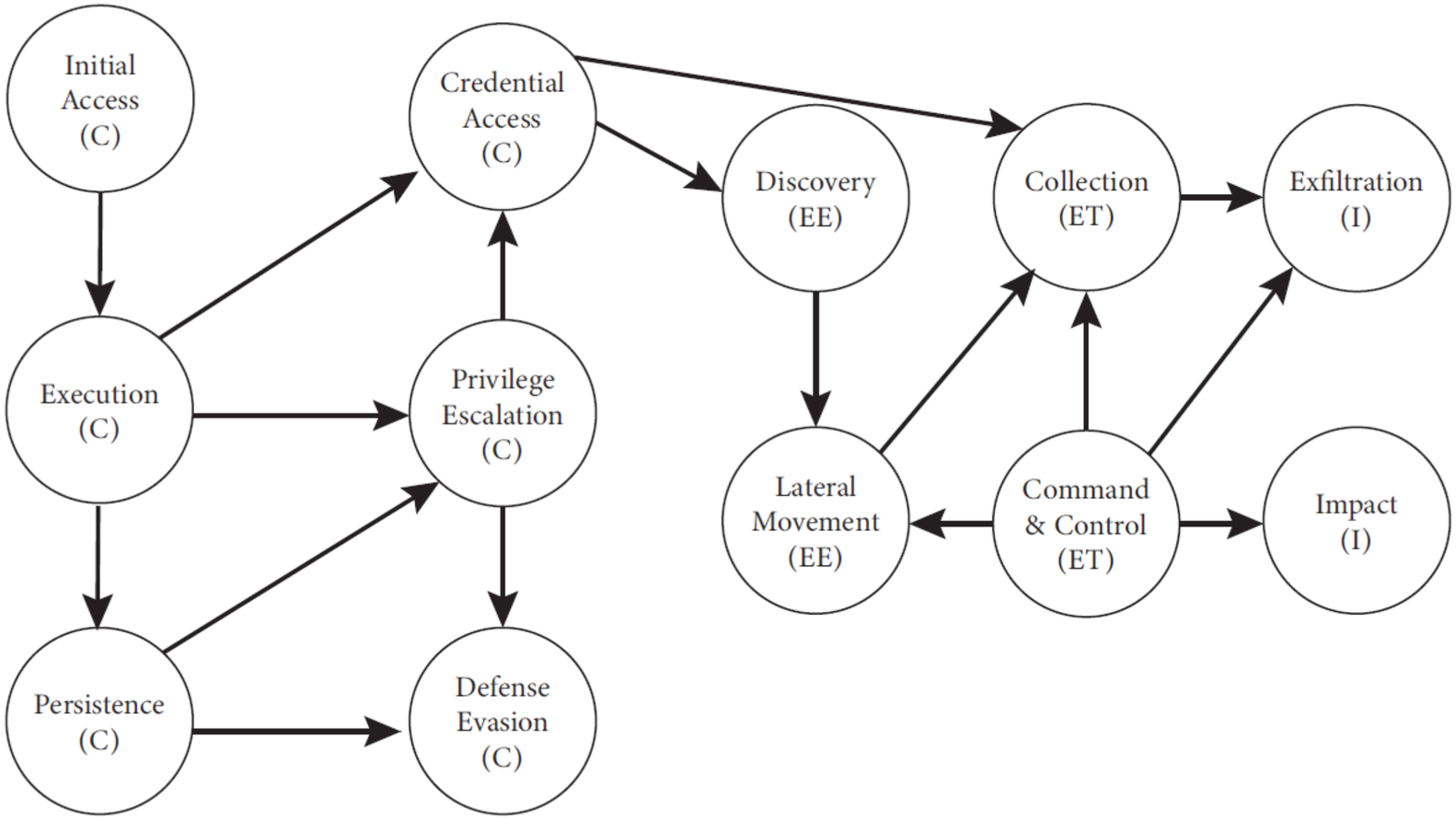
Consist of

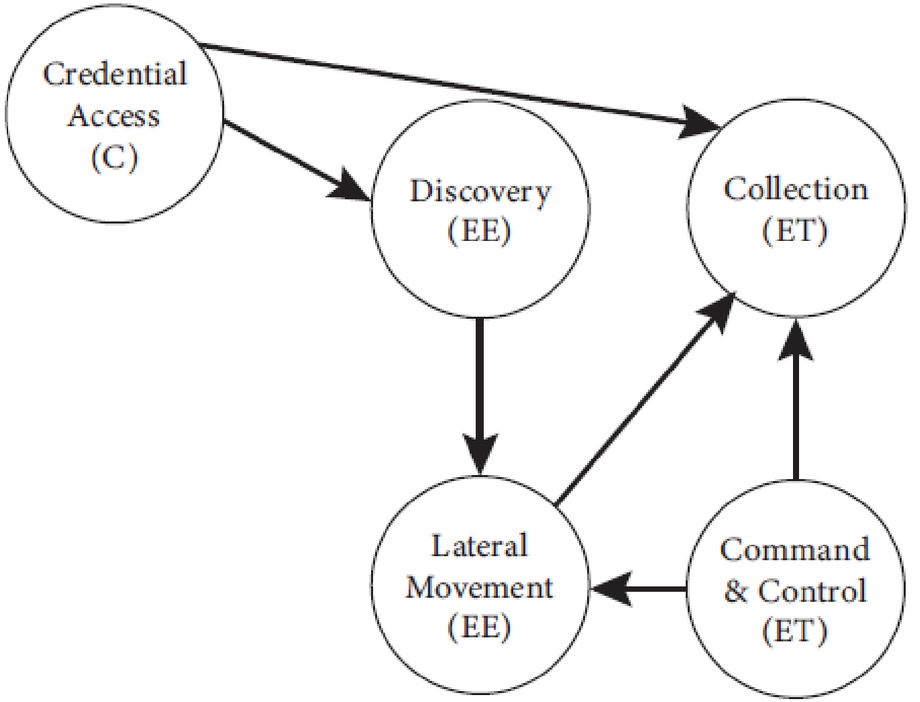
- a set of nodes, corresponding to variables
- a set of edges, indicating dependency
- a set of functions defined on the graph that specify a probability distribution

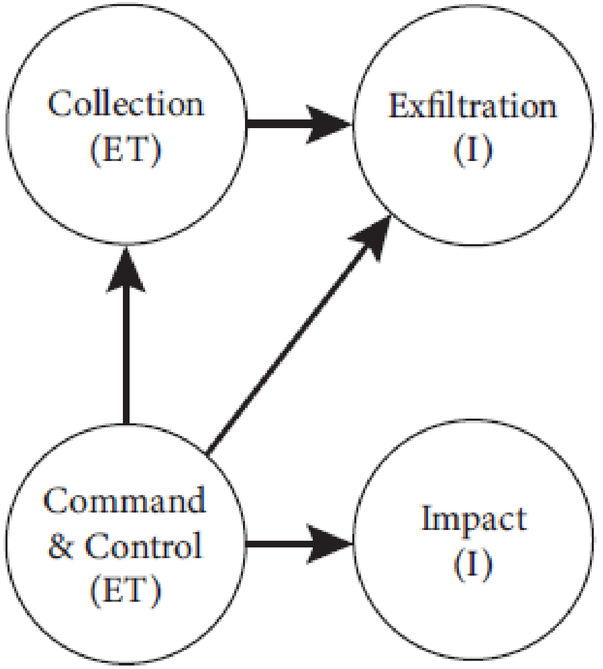
Bayesian Networks

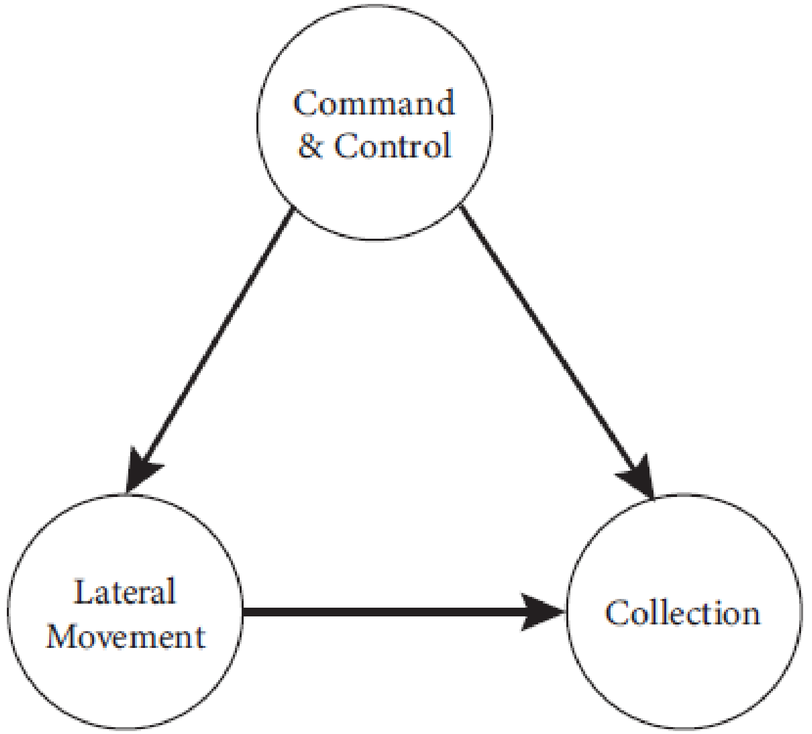
Intersection between statistics, graph theory, and machine learning

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


Initial Access (C)
Credential Access (C)
Discovery (EE)
Collection (ET)
Exfiltration (I)
Execution (C)
Privilege Escalation (C)
Lateral Movement (EE)
Command & Control (ET)
Impact (I)
Persistence (C)
Defense Evasion (C)


Credential Access (C)
Discovery (EE)
Collection (ET)
Lateral Movement (EE)
Command & Control (ET)


Collection
(ET)
Exfiltration
(I)
Command
& Control
(ET)
Impact
(I)


Command
& Control
Lateral
Movement
Collection

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