A Review of Cyber-Ranges and Test-Beds: Current and Future Trends

Accepted Date: 2020.12.5

Authors: Elochukwu Ukwandu, Mohamed Amine Ben Farah, Hanan Hindy , David Brosset , Dimitris Kavallieros, Robert Atkinson, Christos Tachtatzis, Miroslav Bures, Ivan Andonovic and Xavier Bellekens

Sensors(SCI 3区)

Reporter: Yuqiao Gu

OUTLINE

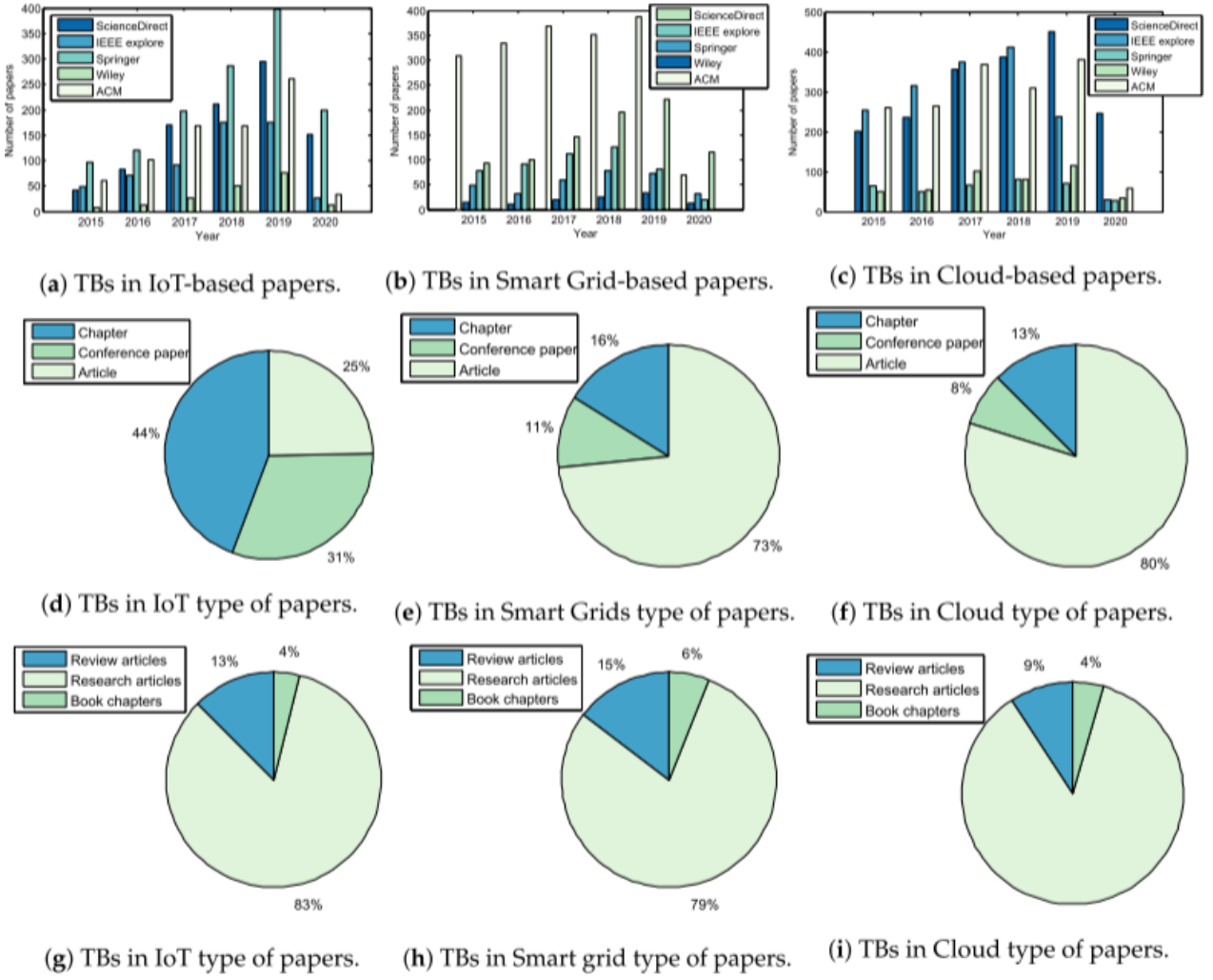
- **The purpose of this paper**
- **Research Criteria**
- **Systematic overview**
- **Technologies in cyber ranges and testbeds**
- **Applications and scenarios of cyber ranges and testbeds**
- **Taxonomies of cyber ranges and testbeds**
- **Discussion**

The purpose of this paper

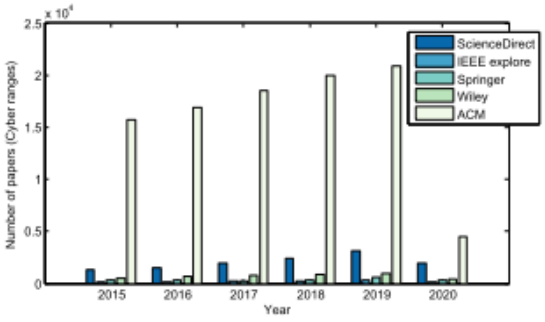
- **Survey recent CRs and TBs research**
- **Analyze and review state-of-the-art trends, scenarios and applications**
- **Establish a taxonomy for future CRs/TBs**
- **Equip cyber-security professionals with the relevant skills to combat cyber threats in next-generation highly inter-connected, multi-domain infrastructures**

Research criteria

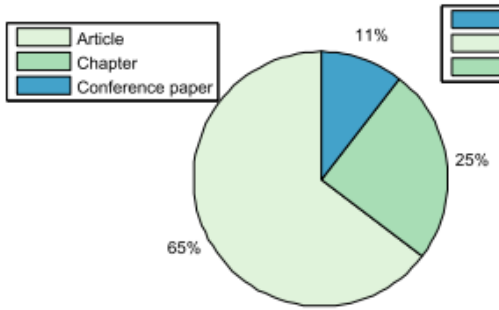
- “Cyber-Ranges” + (“Military” + “Defense” + “Intelligence”) or (“Industry” + “Commercial”) or (“Education” + “Research”)
- “Test-Beds” + (“IoT” or “Smart Grid” or “Cloud”) + cyber
- Published in 2015-2020
- In five databases: ScienceDirect, IEEE Explore, Springer, Wiley, and ACM



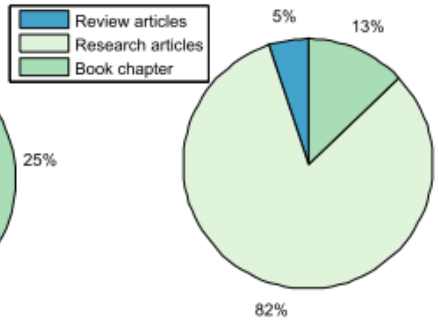
各数据库中TB在IOT、智能电网和云相关论文概况



(**a**) CRs in ScienceDirect, IEEE explore, Springer, Wiley and ACM.



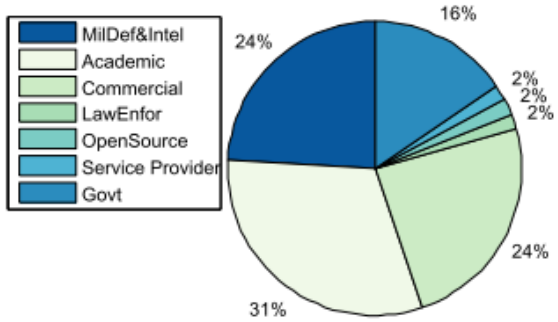
(**b**) CRs type of papers in Springer

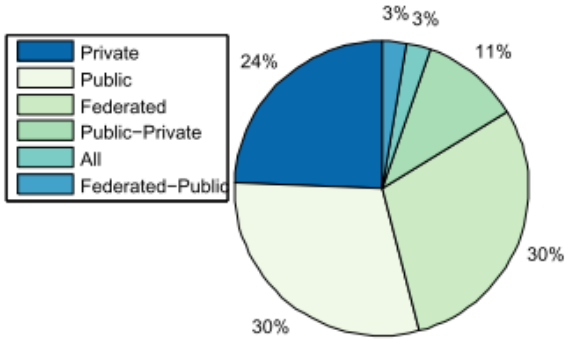


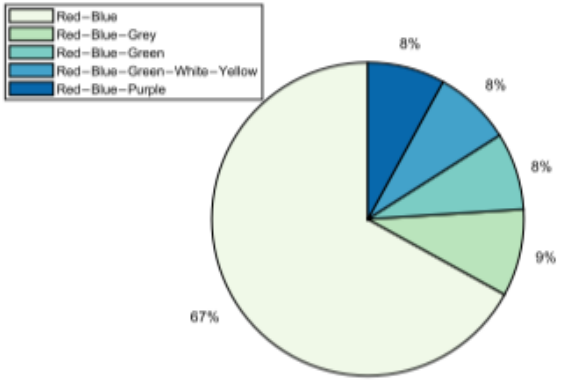
(**c**) CRs type of papers in Sciene Direct

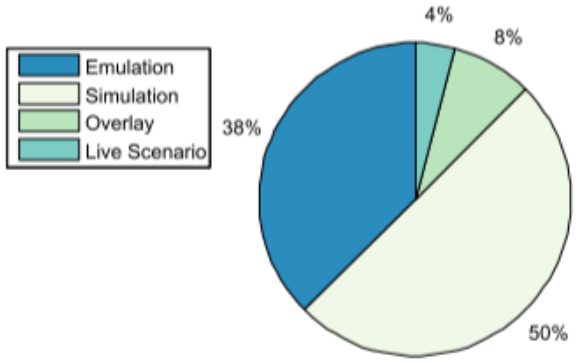
各数据库中CR发表论文概况

Systematic Overview





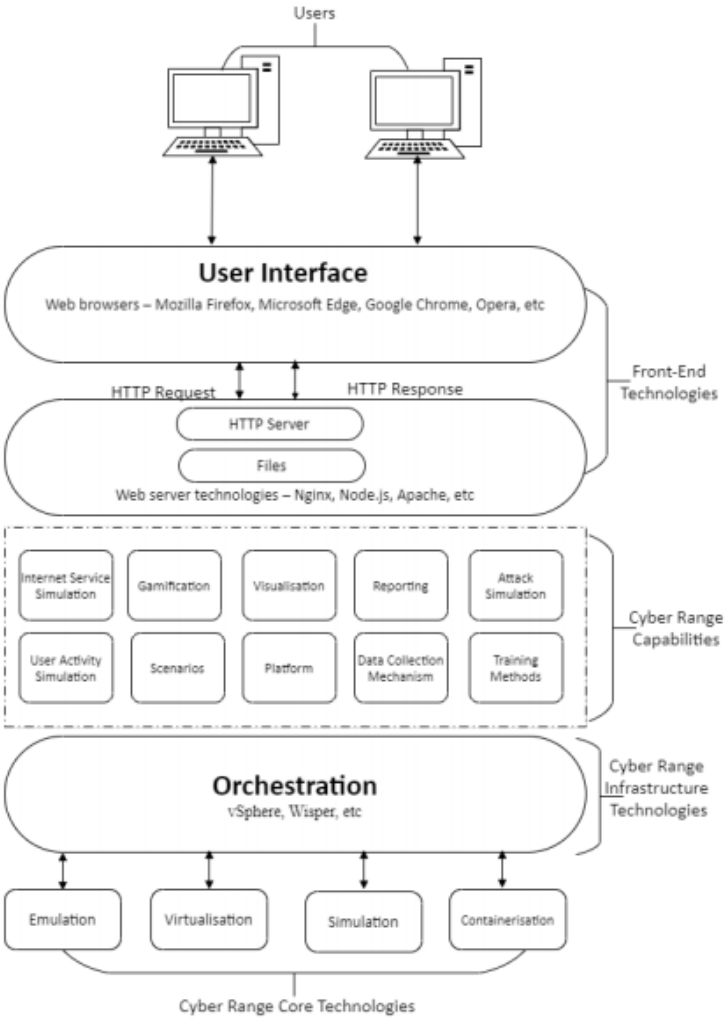


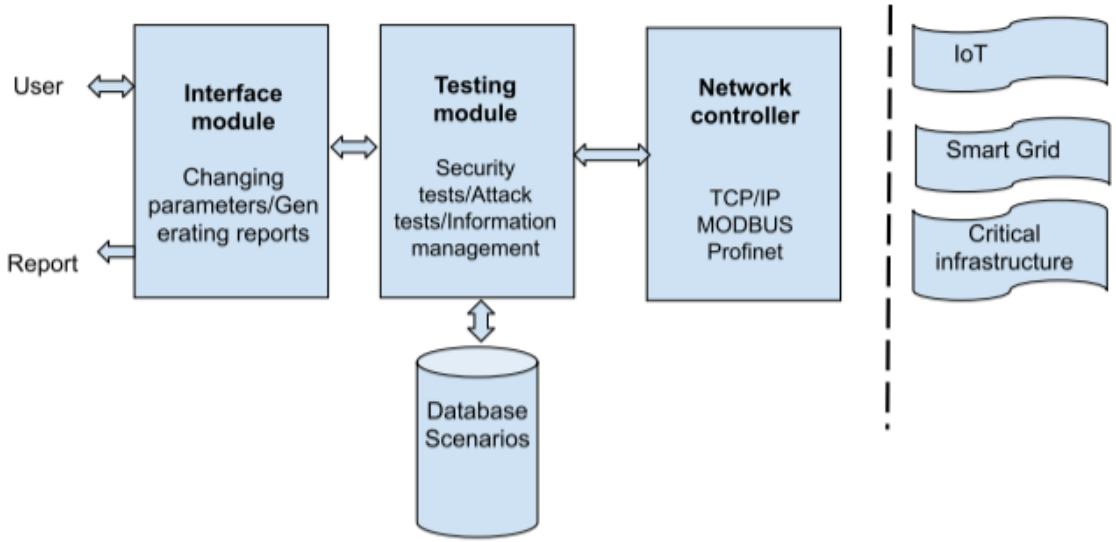


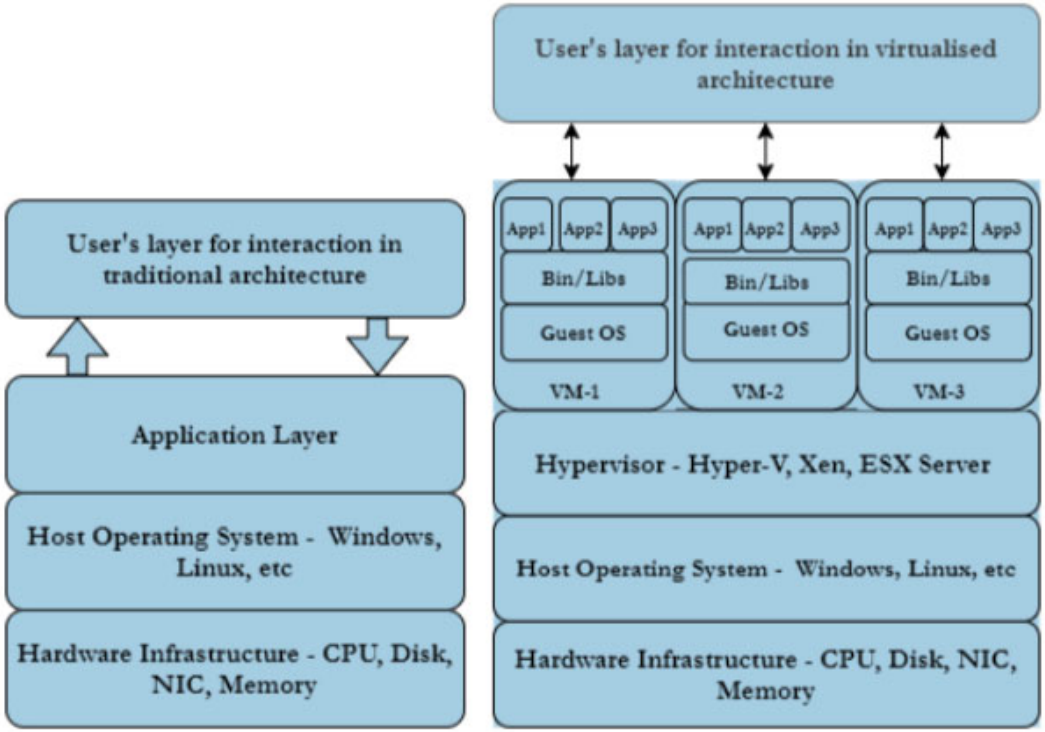
Technologies in cyber ranges and testbeds

- Virtualisation
- simulation
- Containerisation
- physical hardware

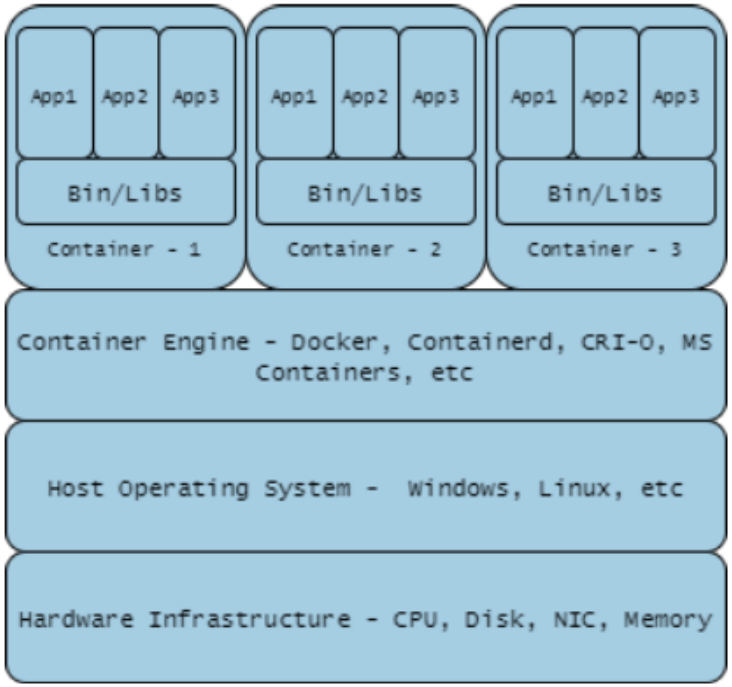
Architecture of cyber ranges and testbeds





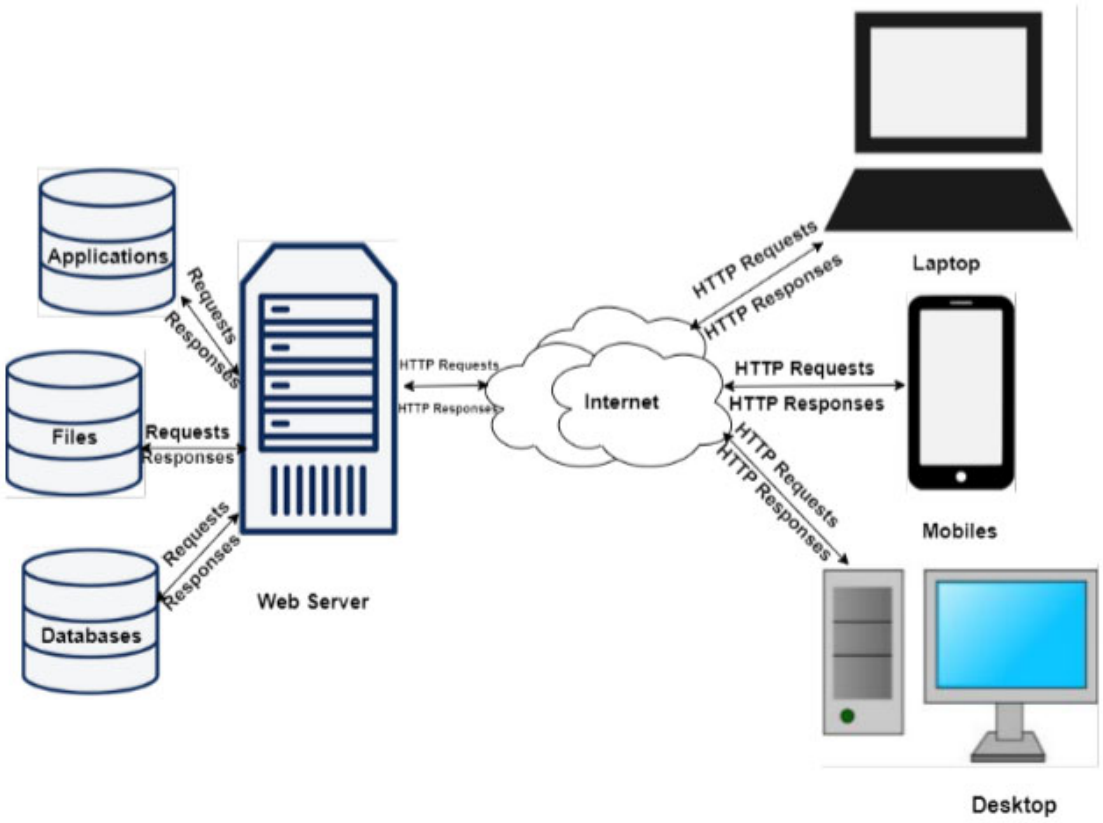


Hybrid Computing stack

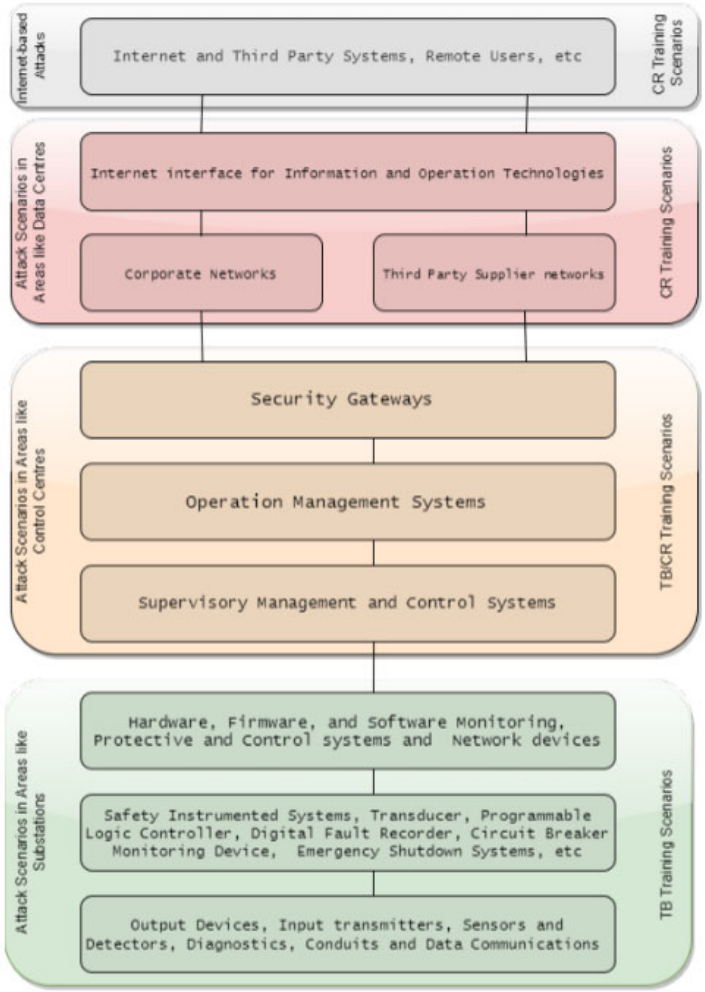


Containerisation Architecture

Front-End technologies



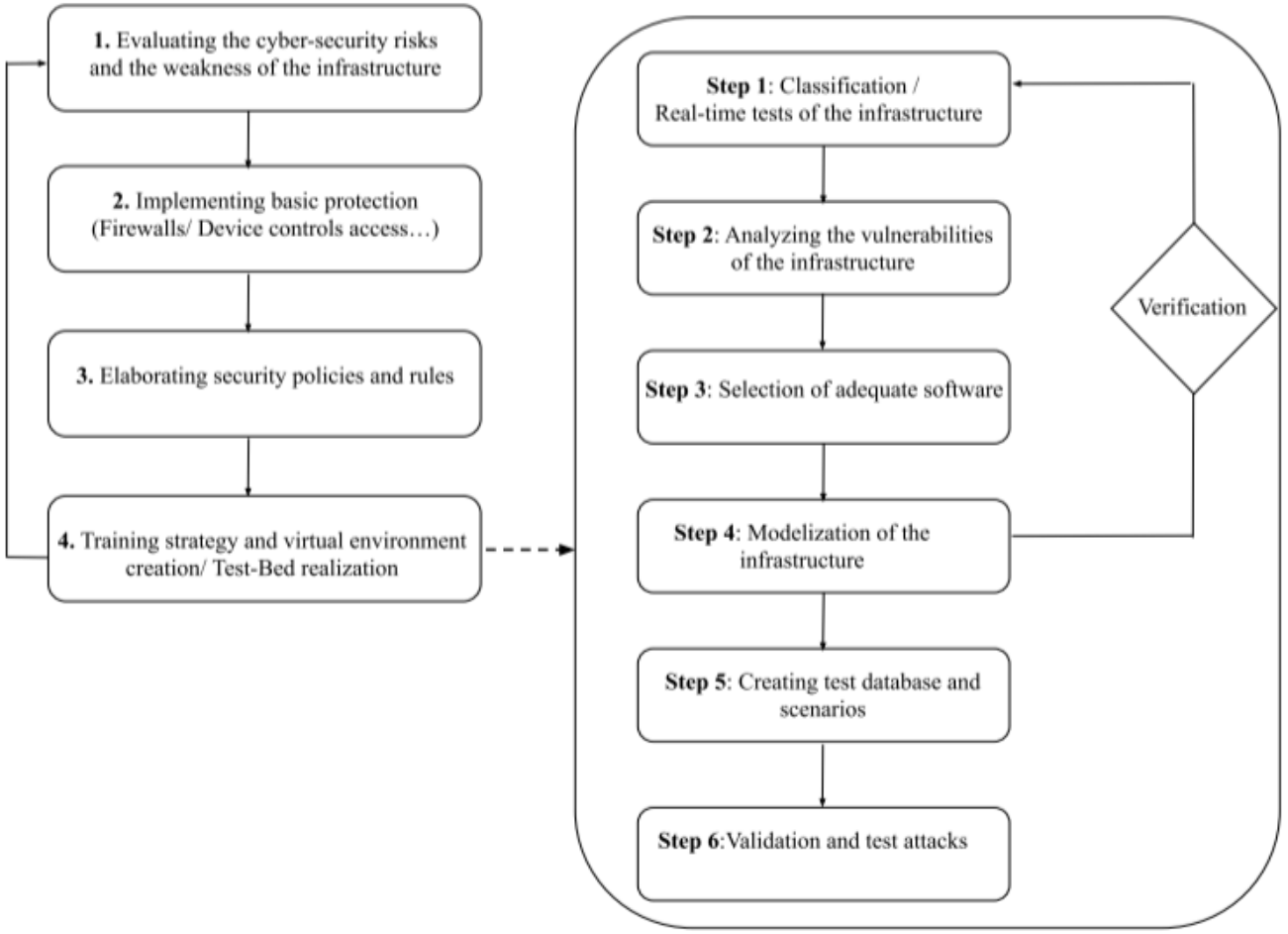
Scenarios of Cyber Ranges and Testbeds



Applications of Cyber Ranges and Testbeds

- Industrial and Commercial
- Education and Research
- Smart Grids
- Military, Defence and Intelligence
- IoT Devices

Realization of Cyber Ranges and Testbeds



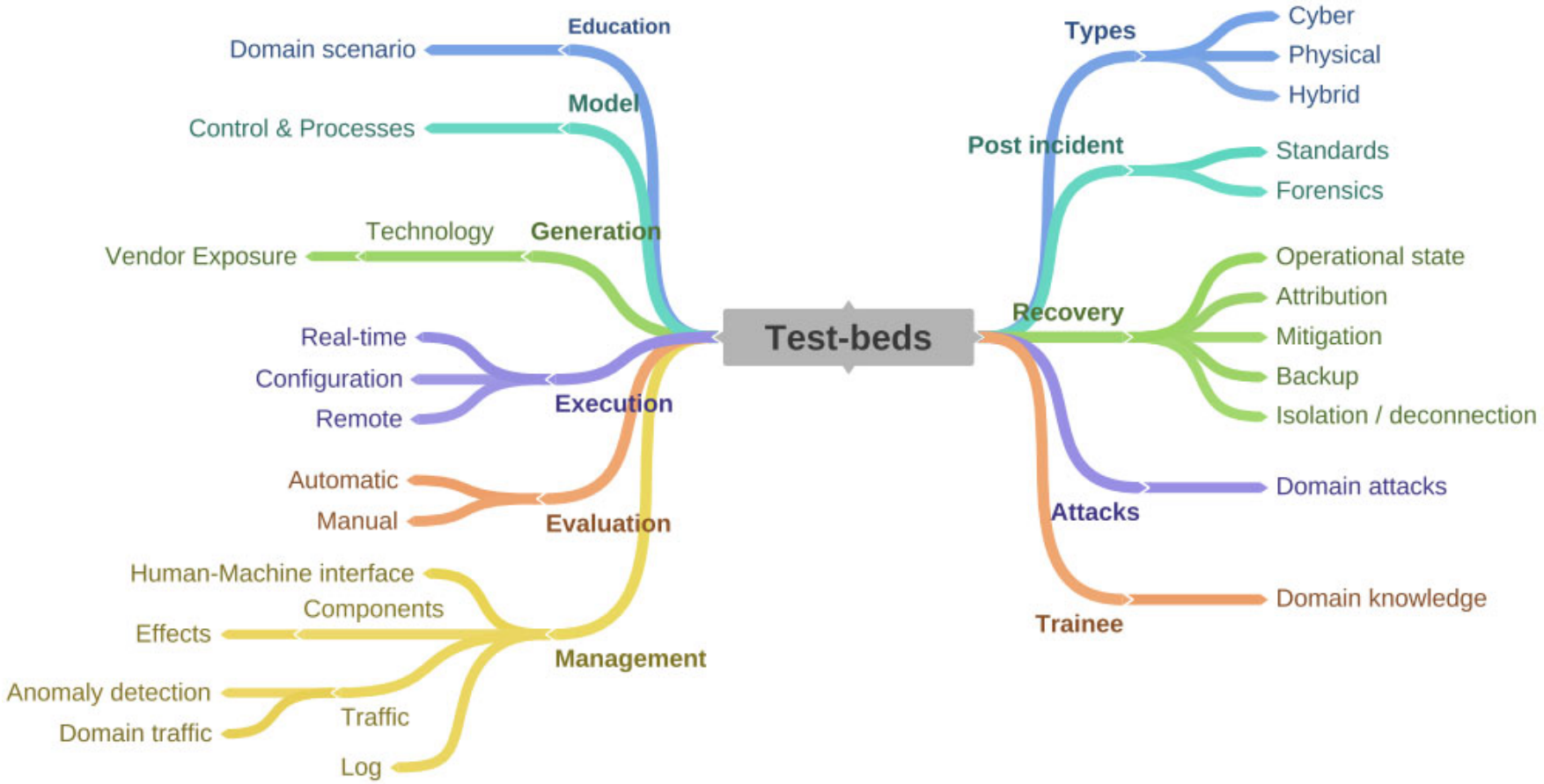
Taxonomies of cyber ranges

- Management
- Monitoring
- Econometrics
- Types
- Teaming
- Recovery
- Attack Types
- Scenarios

Taxonomies of testbeds

- Education
- Model
- Generation
- Execution
- Evaluation
- Management
- Types
- Post-Incident
- Attacks
- Trainee


Cyber-Ranges
Teaming
Red
Blue
White
Yellow
Green
Purple
AI based agent
Types
Hardware
Simulation
Federation
Hybrid
Emulation
Econometrics
Threat Forecasting
Choices implications
Mitigation impact
Assessment models
Monitoring
Users
Actions
Inputs
Path
Teams
Platform
Health
Connections
VPN
P2P
TCP/IP
Status
Virtualisation
Performance
Progress
Management
Data management
Storage
Analysis
Dashboard
Attack type
Scenario
Add
Modify
Update
Delete
Launch
Types
Users
Roles
Reporting
Test-beds
Recovery
Pre
Policies
Patch
Assets
During
Operational state
Attribution
Mitigation
Backup
Isolation / deconnection
Post
Standards
Forensics
Attack type
Security Configutration
Vulnerability
OSI layer
Integrity
Availability
Social engineering
Scenarios
Narrative
Dilemma
Desire
Goal
Conflict
Consequences
Domain
Defence
Naval
Communication
4G
5G
Maritime
Vessel
Port
Industrial
Supply chain
Industry 4.0
ICT
Space
Aviation
Power
Vehicular
Cloud
IoT
Education
Tutoring
Scoring
Demonstration
Analysis & Review
Simulation
Role-based
Case studies
Gamification
Achievements
Leaderboard
Progressbar
Bonus
Discovery
Quests
Progression
Real time feedback
Activity feed
Combos
Countdown
Levels
Point based
Gifting
Rewards
Trophies
Status
Avatar
Type
Static
Dynamic


Test-beds
Education
Domain scenario
Model
Control & Processes
Generation
Technology
Vendor Exposure
Execution
Real-time
Configuration
Remote
Evaluation
Automatic
Manual
Management
Human-Machine interface
Components
Effects
Traffic
Anomaly detection
Domain traffic
Log
Types
Cyber
Physical
Hybrid
Post incident
Standards
Forensics
Recovery
Operational state
Attribution
Mitigation
Backup
Isolation / deconnection
Attacks
Domain attacks
Trainee
Domain knowledge

Discussion

- Real-Time Auto-configurable Systems

THANK YOU!