THE ROAD TO AUTONOMOUS CYBERSECURITY

Artificial Intelligence in Security and Defense – Possibilities, Risks and Threats

Martin Drasar, CSIRT-MU

drasar@ics.muni.cz

MUNI
CSIRT-MU

THE CASE FOR AUTONOMOUS CYBERSECURITY

- Cybersecurity is dynamic, evolving, and expanding domain
- Training of cybersecurity experts takes years up front and must be updated
- Experts are expensive and their supply is limited
- Technology (and potential attack vectors) are proliferating everywhere

- Wouldn't it be nice to have cybersecurity decisions and operation guaranteed 24/7, with rapid response and constant updating?

Cybersecurity and the Army

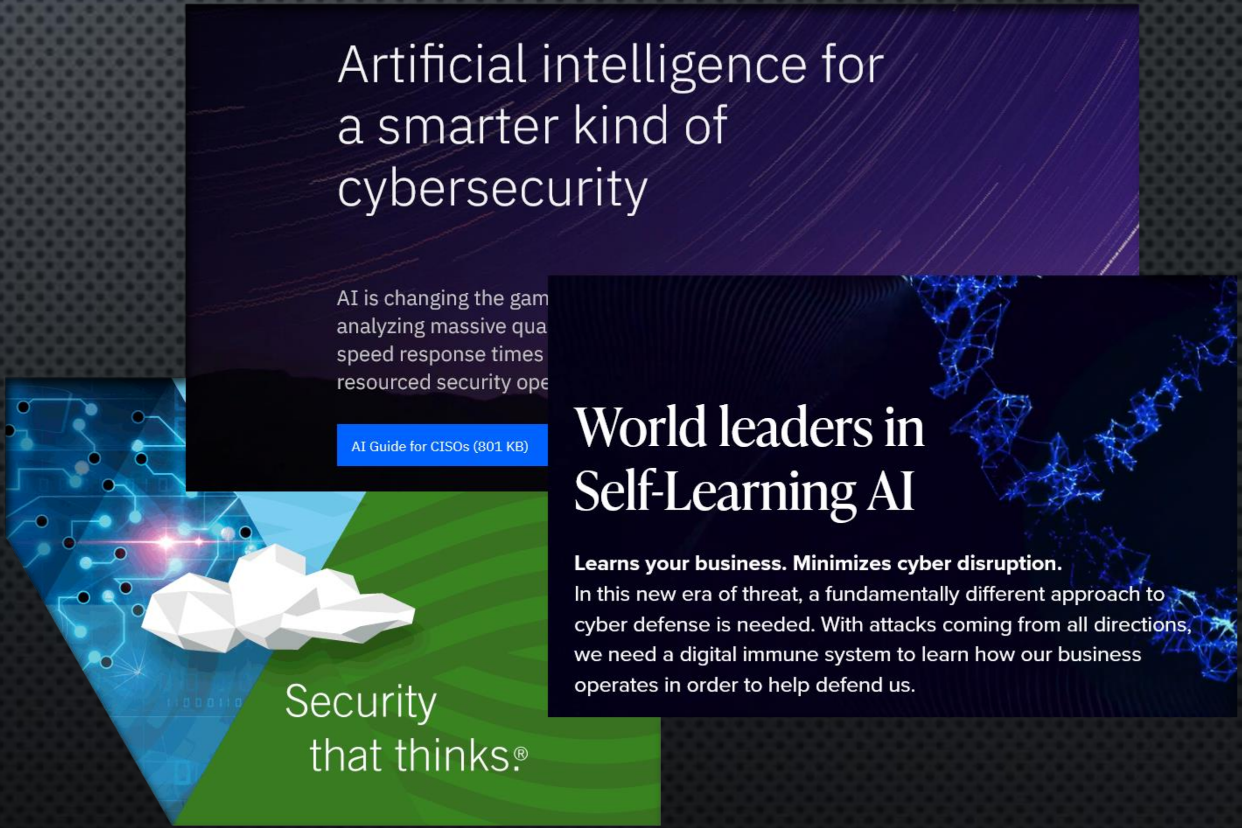
- Hybrid warfare is the norm
- Technology, communication, (semi) autonomous platforms provide enormous tactical advantage
- COTS SW and HW are being integrated
- Internet of Battle Things
- New attack vectors are emerging

THE CASE AGAINST AUTONOMOUS CYBERSECURITY (ESPECIALLY IN THE ARMY)

- Only a limited knowledge, why decisions were made
- No certification, no liability
- Battlefield conditions require creativity
- A lot of one-off learning situations

THE CURRENT STATE OF AI IN CYBERSECURITY

- Marketed as existing and working
- Focused on a specific niche
  - Anomaly detections
  - Big data processing
- Reflects AI development in other areas
- Limited focus on autonomy
  - Expert systems



Artificial intelligence for a smarter kind of cybersecurity

AI is changing the gam
analyzing massive qua
speed response times
resourced security ope

World leaders in Self-Learning AI

Learns your business. Minimizes cyber disruption.
In this new era of threat, a fundamentally different approach to cyber defense is needed. With attacks coming from all directions, we need a digital immune system to learn how our business operates in order to help defend us.

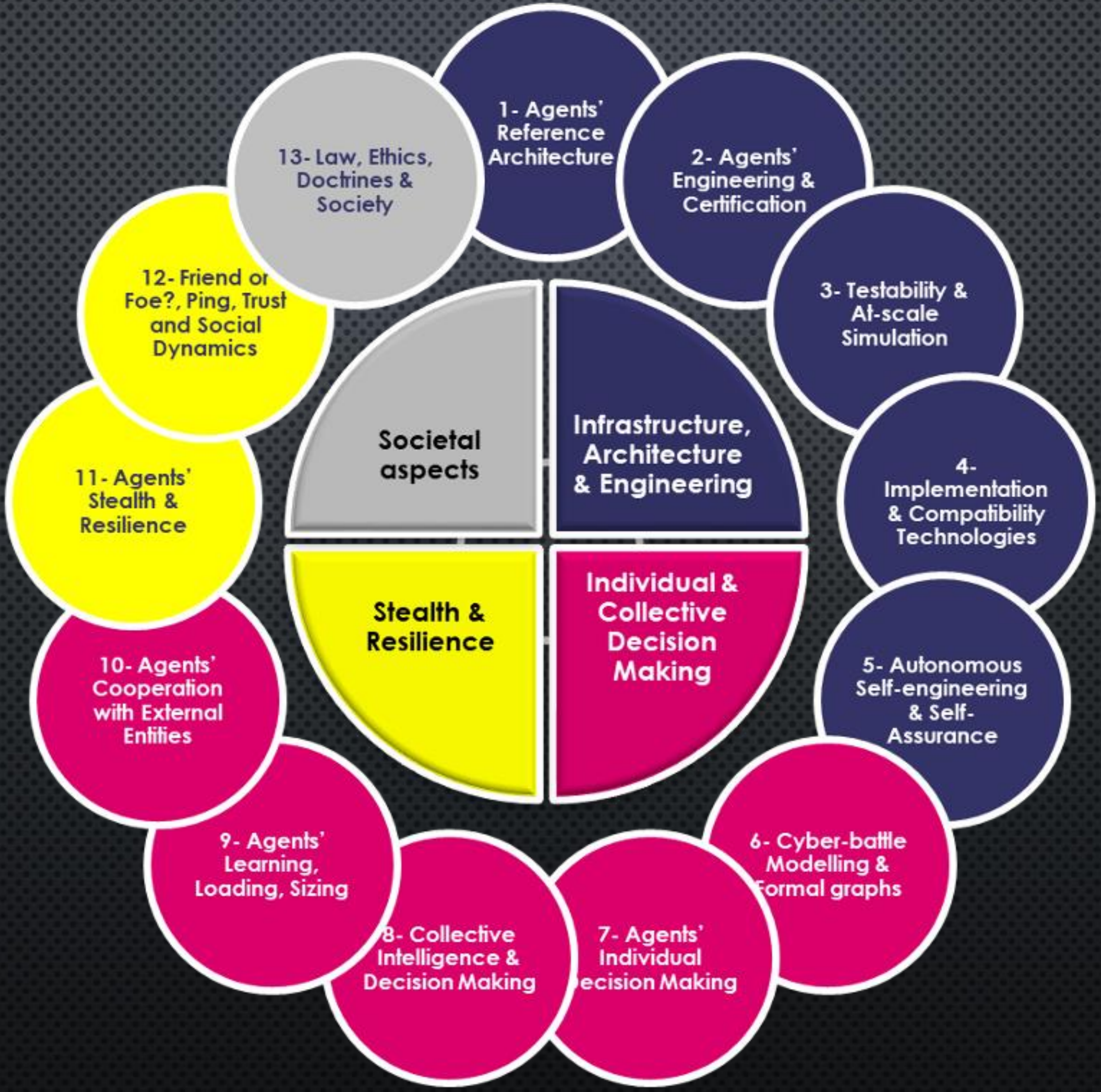
CYBERSECURITY AND AI IN THE ARMY RESEARCH

- IST-ET-109: Orchestration and Scalability of AI-driven Systems
- IST-ET-112: Machine Learning Ecosystem for the Rapid Research, Development, and Deployment of Artificial Intelligence and Machine Learning Capabilities
- IST-190: AI, ML and BD for Hybrid Military Operations
- IST-183: Deep Machine Learning For Cyber Defense
- IST-169: Robustness and Accountability in Machine Learning Systems
- IST-163: Deep Machine Learning for Cyber Defense
- IST-164: Securing Unmanned and Autonomous Vehicles for Mission Assurance
- IST-152: Intelligent, Autonomous and Trusted Agents for Cyber Defense and Resilience

IST-152: Intelligent, Autonomous and Trusted Agents for Cyber Defense and Resilience

- Members of 11 nations
- Research of the state of the art
- Assessment of potential methodological and technical approaches for cyber defense of C4ISR
- Development of reference architecture and a road map

- https://arxiv.org/ftp/arxiv/papers/1804/1804.07646.pdf
- https://arxiv.org/ftp/arxiv/papers/1803/1803.10664.pdf



Societal aspects

Infrastructure, Architecture & Engineering

Stealth & Resilience

Individual & Collective Decision Making

1- Agents' Reference Architecture

2- Agents' Engineering & Certification

3- Testability & At-scale Simulation

4- Implementation & Compatibility Technologies

5- Autonomous Self-engineering & Self-Assurance

6- Cyber-battle Modelling & Formal graphs

7- Agents' Individual Decision Making

8- Collective Intelligence & Decision Making

9- Agents' Learning, Loading, Sizing

10- Agents' Cooperation with External Entities

11- Agents' Stealth & Resilience

12- Friend or Foe?, Ping, Trust and Social Dynamics

13- Law, Ethics, Doctrines & Society

AICA-IWG

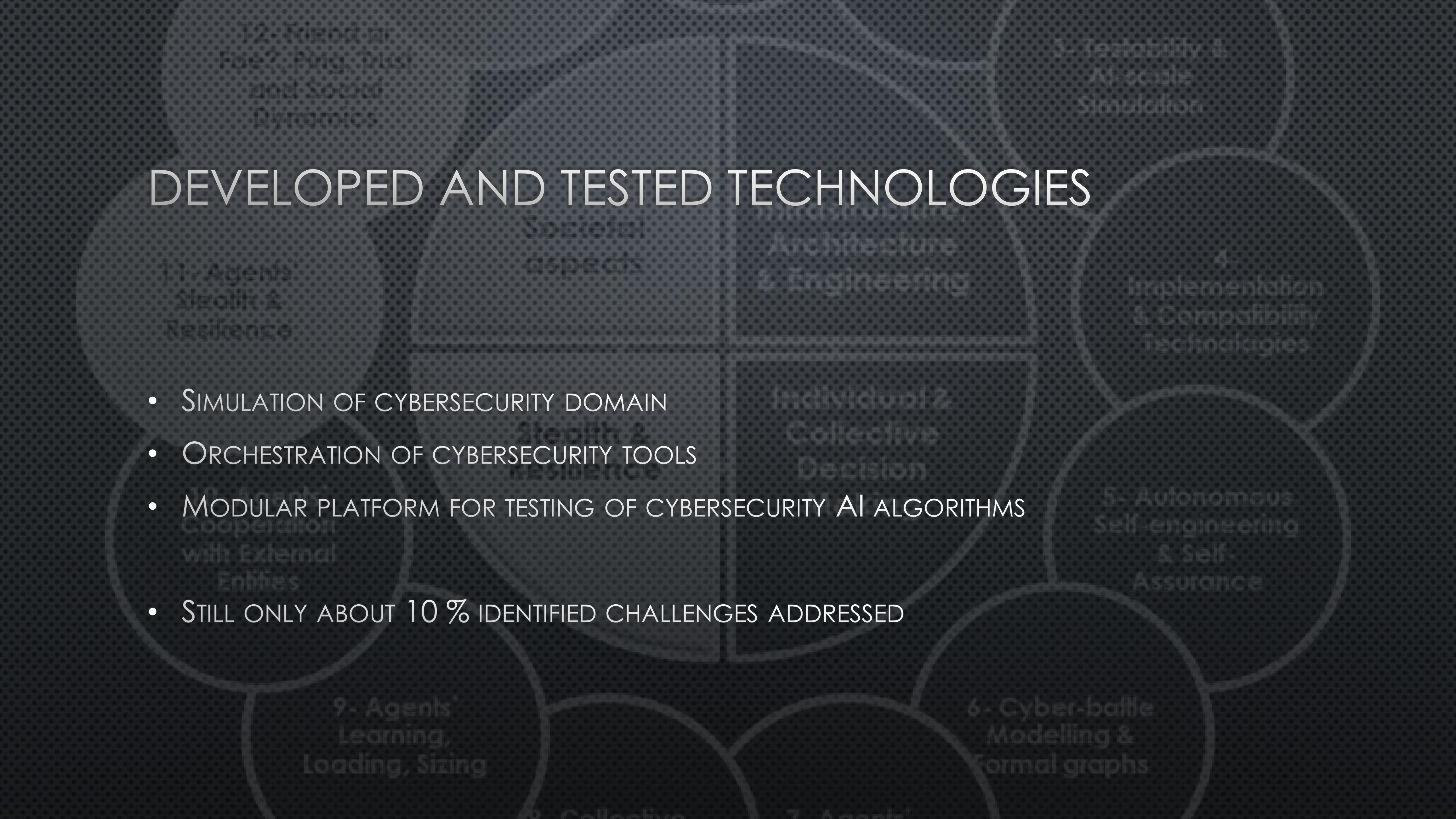
- Follow-up to IST-152
- Industry & Academia
- Addressing of research problems
- Development of supplemental technologies
- Development of autonomous cybersecurity prototypes

- https://www.aica-iwg.org/

PROTOTYPE DEVELOPMENT

- Ordered by NATO NCIA (https://www.ncia.nato.int/)
- Small-scale implementation of reference architecture
- Goal: implementation of an extensible platform for rapid prototyping of autonomous agents
- Use-case: securing of vehicular networks
- Identification of concrete engineering challenges
- Testing of existing tools

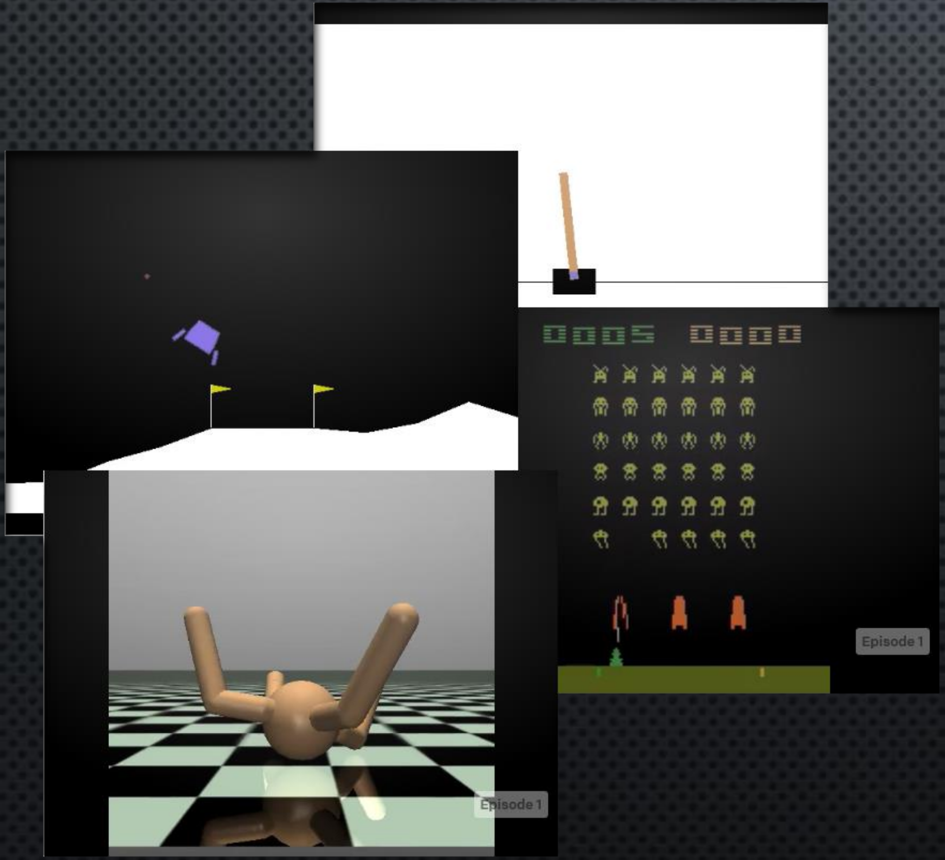
DEVELOPED AND TESTED TECHNOLOGIES

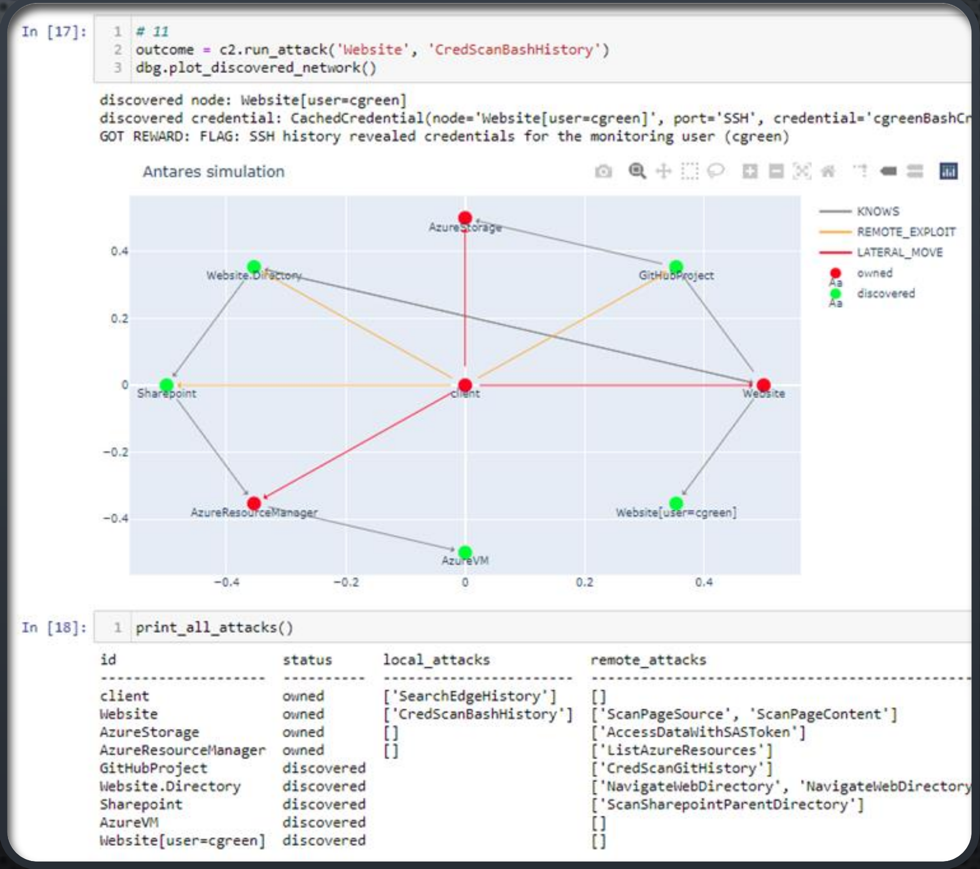

12- Friend or Foe?, Ping, Trust and Social Dynamics
3- Scalability & AI-scale Simulation
Societal aspects
Infrastructure, Architecture & Engineering
11- Agents' Stealth & Resilience
4- Implementation & Compatibility Technologies
Stealth & Resilience
Individual & Collective Decision
10- Agents' Cooperation with External Entities
5- Autonomous Self-engineering & Self-Assurance
9- Agents' Learning, Loading, Sizing
6- Cyber-battle Modelling & Formal graphs
8- Collective
7- Agents'

- Simulation of cybersecurity domain
- Orchestration of cybersecurity tools
- Modular platform for testing of cybersecurity AI algorithms

- Still only about 10 % identified challenges addressed

SIMULATION OF CYBERSECURITY DOMAIN





```
In [17]: # 11
         outcome = c2.run_attack('Website', 'CredScanBashHistory')
         dbg.plot_discovered_network()

discovered node: Website[user=cgreen]
discovered credential: CachedCredential(node='Website[user=cgreen]', port='SSH', credential='cgreenBashCr
GOT REWARD: FLAG: SSH history revealed credentials for the monitoring user (cgreen)
```

```
In [18]: print_all_attacks()

id                    status      local_attacks            remote_attacks
--------------------  ----------  -----------------------  ---------------------------------------------
client                owned       ['SearchEdgeHistory']    []
Website               owned       ['CredScanBashHistory']  ['ScanPageSource', 'ScanPageContent']
AzureStorage          owned       []                       ['AccessDataWithSASToken']
AzureResourceManager  owned       []                       ['ListAzureResources']
GitHubProject         discovered                           ['CredScanGitHistory']
Website.Directory     discovered                           ['NavigateWebDirectory', 'NavigateWebDirectory
Sharepoint            discovered                           ['ScanSharepointParentDirectory']
AzureVM               discovered                           []
Website[user=cgreen]  discovered                           []
```

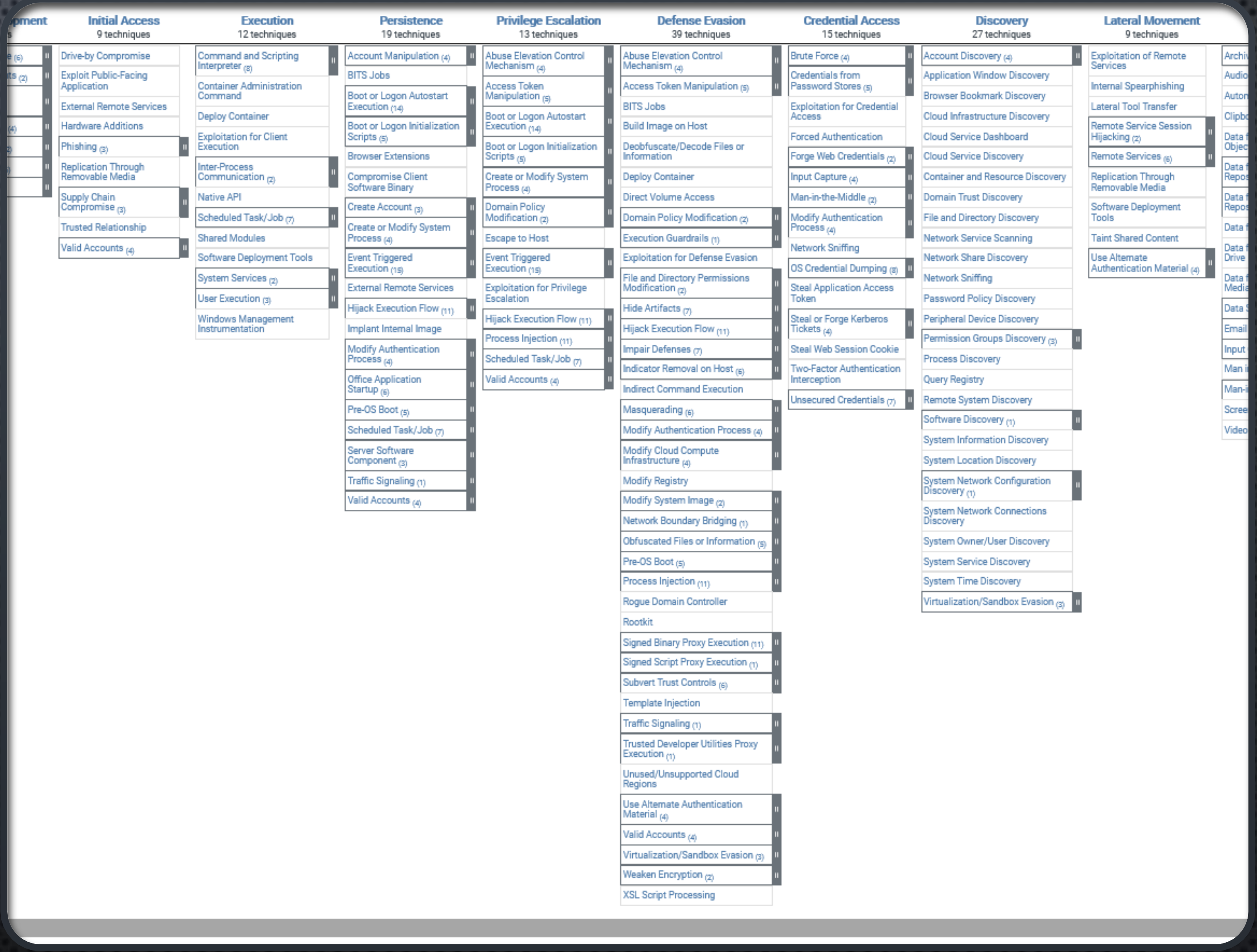
CYST: SIMULATION FOR AI DEVELOPMENT

- Environment tailored for development of autonomous cybersecurity solutions
- Multi-agent
- Integration of different attack, defense, and behavioral models
- Linking the simulation and emulation (e.g., human in the loop)
- Parametrized generation of cybersecurity scenarios
- Parallel training of attackers and defenders

- https://www.muni.cz/go/cyst-user

Orchestration of Cybersecurity Tools

- Reliance on off-the-shelf software
- Large variance in input/output between different tools
- Autonomous tools benefit from consistency



pment

s

- e (6)
- ts (2)
- (4)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
12 techniques

- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (2)
- Native API
- Scheduled Task/Job (7)
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (4)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- External Remote Services
- Hijack Execution Flow (11)
- Implant Internal Image
- Modify Authentication Process (4)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (7)
- Server Software Component (3)
- Traffic Signaling (1)
- Valid Accounts (4)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (11)
- Process Injection (11)
- Scheduled Task/Job (7)
- Valid Accounts (4)

Defense Evasion
39 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (7)
- Hijack Execution Flow (11)
- Impair Defenses (7)
- Indicator Removal on Host (6)
- Indirect Command Execution
- Masquerading (6)
- Modify Authentication Process (4)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (5)
- Pre-OS Boot (5)
- Process Injection (11)
- Rogue Domain Controller
- Rootkit
- Signed Binary Proxy Execution (11)
- Signed Script Proxy Execution (1)
- Subvert Trust Controls (6)
- Template Injection
- Traffic Signaling (1)
- Trusted Developer Utilities Proxy Execution (1)
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material (4)
- Valid Accounts (4)
- Virtualization/Sandbox Evasion (3)
- Weaken Encryption (2)
- XSL Script Processing

Credential Access
15 techniques

- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Man-in-the-Middle (2)
- Modify Authentication Process (4)
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (7)

Discovery
27 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Container and Resource Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery (1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3)

Lateral Movement
9 techniques

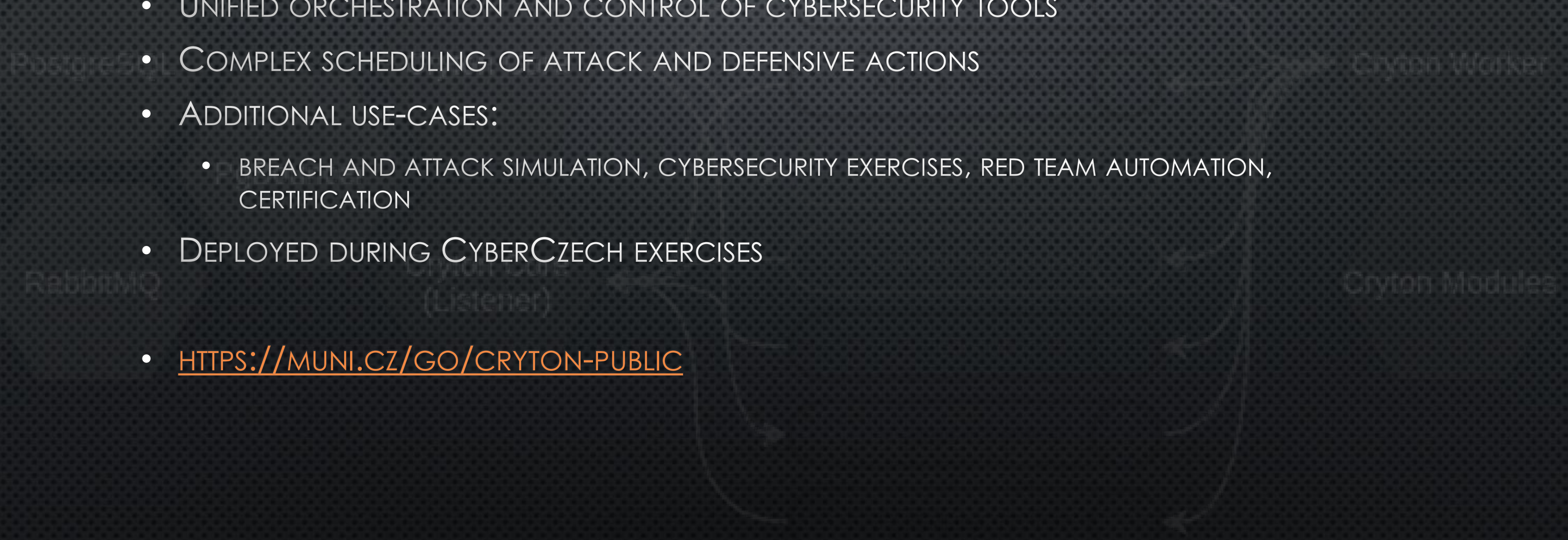
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

- Archi
- Audio
- Auton
- Clipbo
- Data f Objec
- Data f Repos
- Data f Repos
- Data f
- Data f Drive
- Data f Media
- Data S
- Email
- Input
- Man i
- Man-i
- Scree
- Video

CRYTON: ORCHESTRATION AND AUTOMATION

- UNIFIED ORCHESTRATION AND CONTROL OF CYBERSECURITY TOOLS
- COMPLEX SCHEDULING OF ATTACK AND DEFENSIVE ACTIONS
- ADDITIONAL USE-CASES:
  - BREACH AND ATTACK SIMULATION, CYBERSECURITY EXERCISES, RED TEAM AUTOMATION, CERTIFICATION
- DEPLOYED DURING CYBERCZECH EXERCISES

- HTTPS://MUNI.CZ/GO/CRYTON-PUBLIC



AICA PLATFORM

- Developed by Argonne national laboratory
- Extensible, multi-platform, python & docker-based implementation
- Virtual network testbed in construction for upcoming NATO Cyber Coalition 22

- HTTPS://GITHUB.COM/AICA-IWG/AICA-AGENT

CONCLUSION

- Autonomous cybersecurity is nowhere near ready for operation deployment
- Multitude of issues remain unsolved: research, technical, legal, and ethical
- There is no concentrated effort to get the technology ready, issues are being solved in isolation

Invitation

- AICA conference 2022
- October 25 – 26
- Highlights:
  - Alexander Kott, Chief Scientist at the US Army Research Lab
  - Hands-on workshops for aforementioned technologies
  - Presentations/discussions regarding the research and development of autonomous cybersecurity agents

- https://www.aicaconference.org/