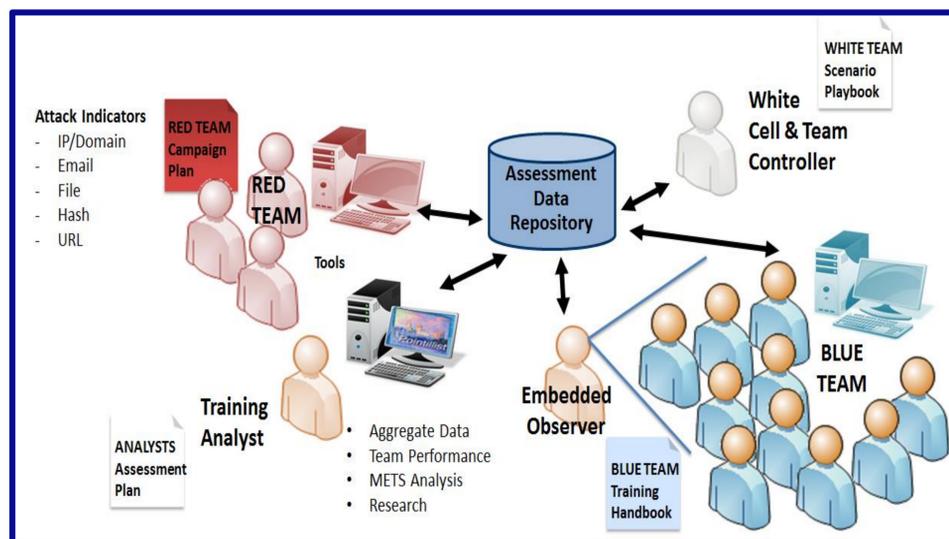


S&T Campaign: Human Sciences
Integration of Humans and Systems
Humans in Multi-Agent Systems

Norbou Buchler, (410) 278-9403 Blaine Hoffman (410) 278-5175
norbou.buchler.civ@mail.mil blaine.e.hoffman.ctr@mail.mil

Research Objective

- Define and standardize critical measures of military cyber-security team performance
- Evaluate the technical instruments available for recording these measures
- Define gaps in metric collection and evaluation; explore methods to address them



Performance and Assessment Elements of Cyber Defense Exercise

Challenges

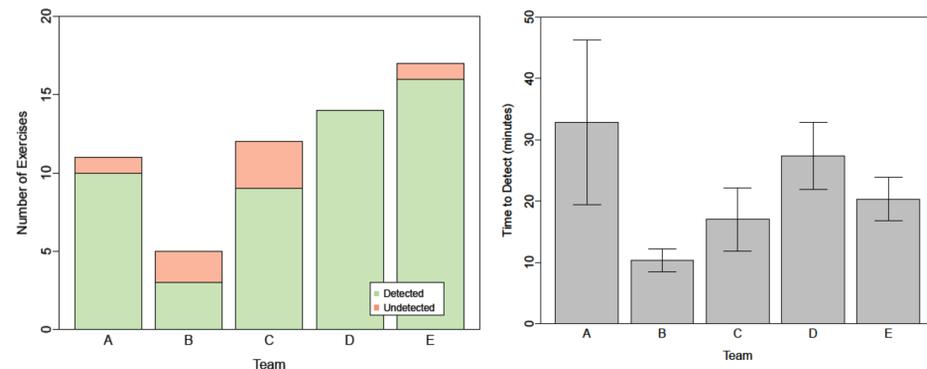
- Tool- and process-based gaps exist in data collection and scoring efforts.
- The complexity and adversarial nature of real-world cyber security does not easily lend itself to controlled laboratory studies.
- Collection and analysis of individual and team performance in cyber defense exercises is essential and valuable, but requires significant overhead in addition to exercise organization.

ARL Facilities and Capabilities Available to Support Collaborative Research

- Cognitive Assessment, Simulation, and Engineering Laboratory (CASEL) at APG, MD
- Prevalent use of open-source software solutions for cyber security enables running tools on ordinary PCs
- Laboratory facilities enable network simulation and testing for tool prototypes
- Intelligence analysts are available for insights into cyber protection team processes and tasks.
- Ongoing collaborations through the ARL Cyber Security Collaborative Research Agreement (CRA) – established relationship with the Army National Guard for CYBER SHIELD annual exercise

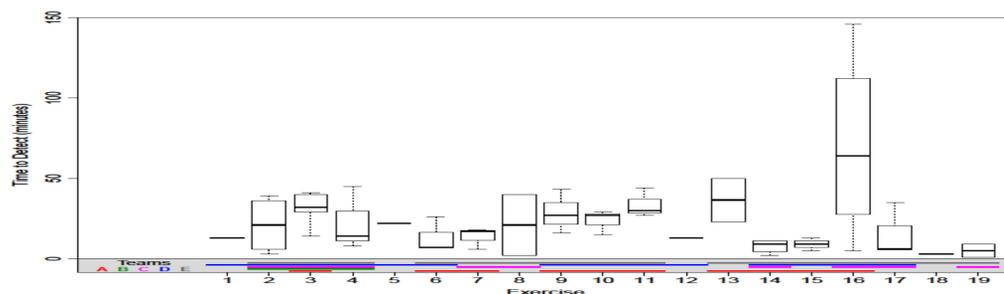
Results

- Cyber Protection Team (CPT) performance was highly variable (novice to expert teams) given by the number and probability of detecting ongoing cyber attacks.



Team Exercise Completion and Average Detection Times

- The teams exhibiting the fastest detection times were also the ones that detected the fewest events; thus, detection times need to be understood in terms of relative difficulty and context of the cyber attacks.



- Some events were challenging to detect. The outlier Event #16 is an ongoing ICS/SCADA attack. This highlights a critical cybersecurity challenge to a known vulnerability.

Complementary Expertise/ Facilities/ Capabilities Sought in Collaboration

- Tools to support automated collection – reduce resource / personnel needs
- Standards for data collection and automation processes across multiple training environments and/or events
- Cyber range facilities in which scenarios can be designed, built, and stored for teams to access for training
- Expertise and knowledge of Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) environments to integrate with cyber security knowledge and practice
- Greater access to CPT teams and cyber security exercises / events would provide more avenues to test and validate tools and metric collection