Cyber Security Exercises as an Effective Training Instrument in Hybrid Environment

Juliana Karakaneva

New Bulgarian University

Department of National and International Security

ykarakaneva@nbu.bg

Orlin Nikolov

Crisis Management and Disaster Response Centre of Excellence

Chief of Capabilities Branch

orlin.nikolov@cmdrcoe.org

BULGARIA

Cyber space and operations –
the digital basis of hybrid threats
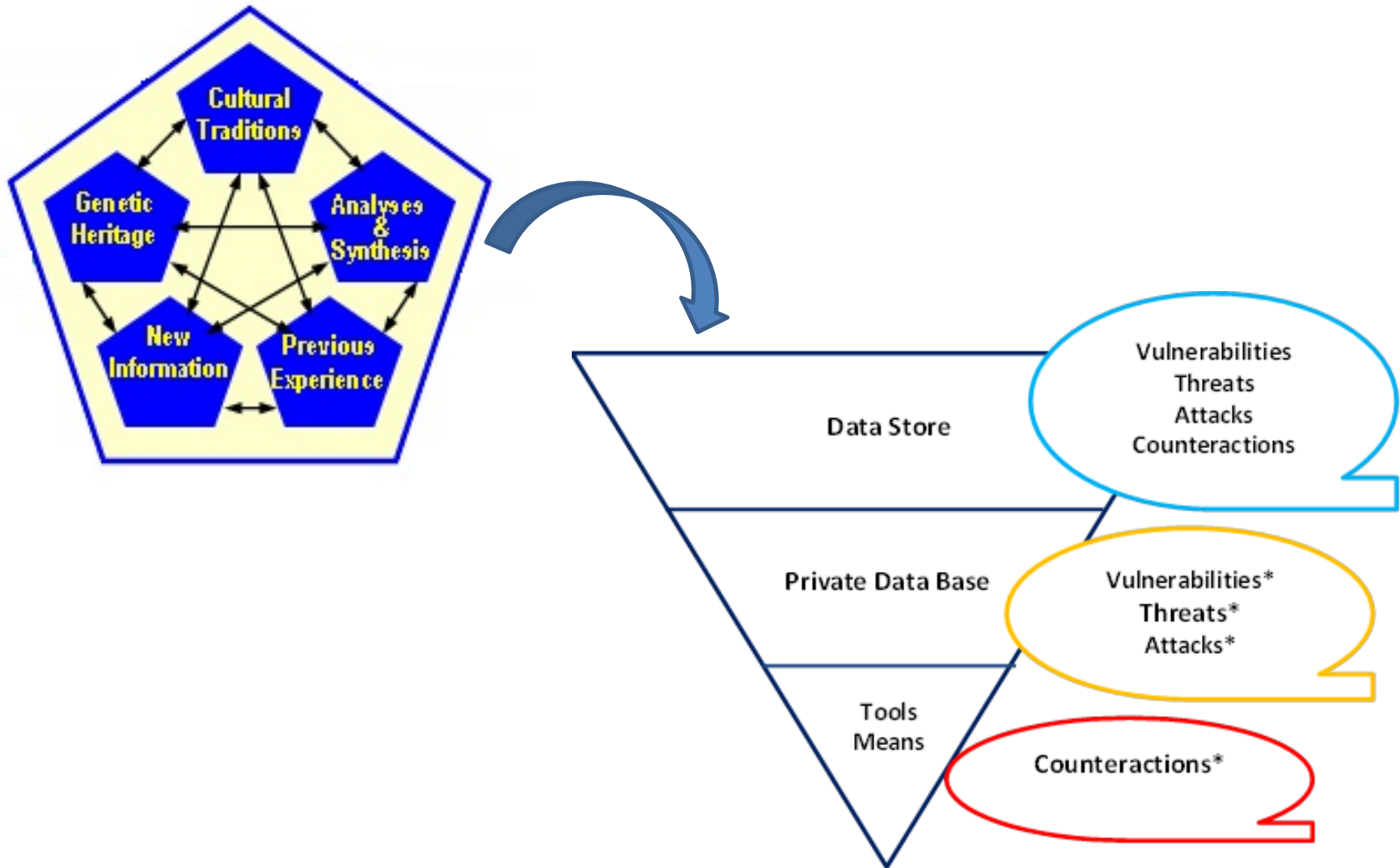
Conceptual approach to the cyber exercise

Aspects:

- Organizational

- Cognitive

- Training

Cyber Exercise Organizational Aspect
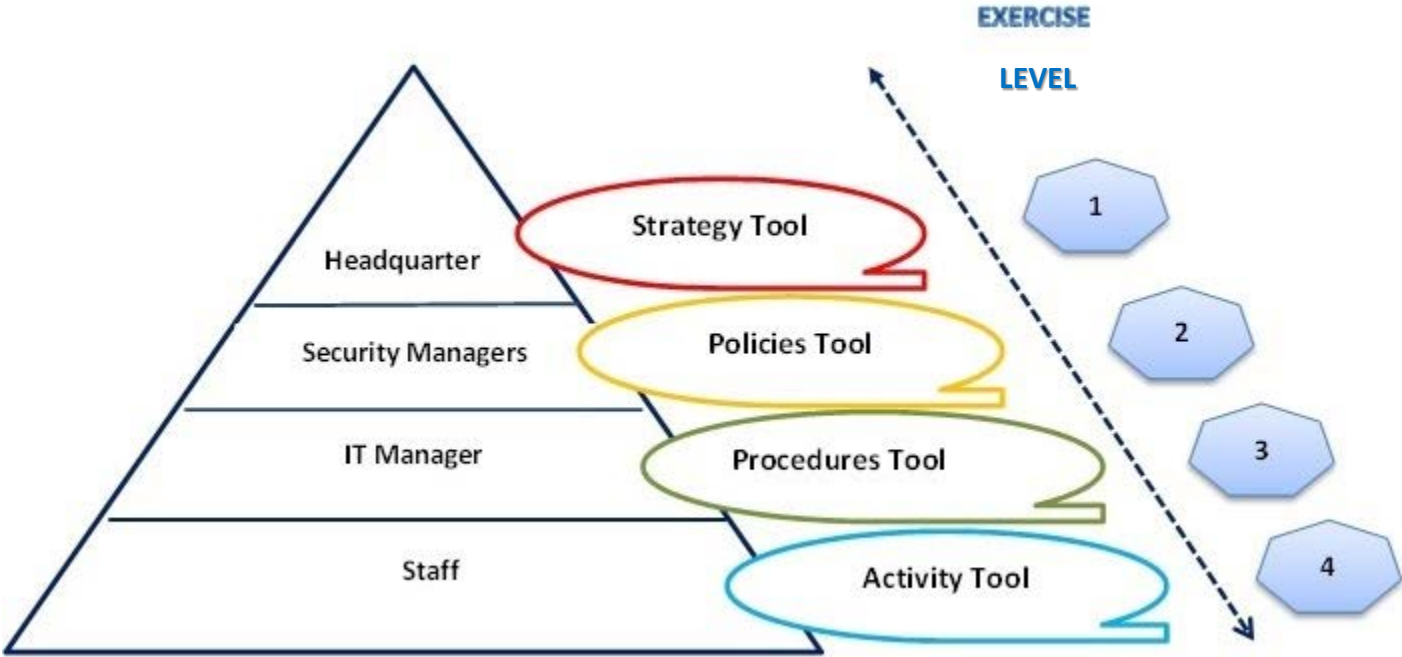
Cyber Exercise Cognitive Aspect

Adopted Classification of threats

- Destruction of information
- Corruption of information
- Disclosure of information
- Theft, loss of information
- Elevation of privilege
- Illegal usage
- Denial of use

Cyber Exercise Training Model

Concept of Tool

- DB of security events
- DB of response alternatives
- Searching instrument
- Test module
- Evaluation module
- Statistics module

Metrics for Assessment

Training Level of participants

- Input test

- Output test

Success of the Exercise

- Final evaluation

The tasks have been solved

- training of personnel for dealing with cyber attacks;
- development of the necessary system infrastructure - introducing systems for monitoring, prevention and detection of intrusions;
- improvement the security system;
- accumulation of information and knowledge generation;
- improvement of the process of planning and preparation of the next exercise

Discussion