Cyber-crisis exercises

Charlie van Genuchten

Definition of cyber crisis

- *A cyber incident is an IT incident that disrupts the expected availability of services and/or provokes the unauthorised disclosure, acquisition and/or modification of information.*

- *A cyber crisis is "an abnormal and unstable situation in which strategic goals, reputation and reliability are threatened by a disturbance, intentional or unintentional, at the core of the targeted organisation."*

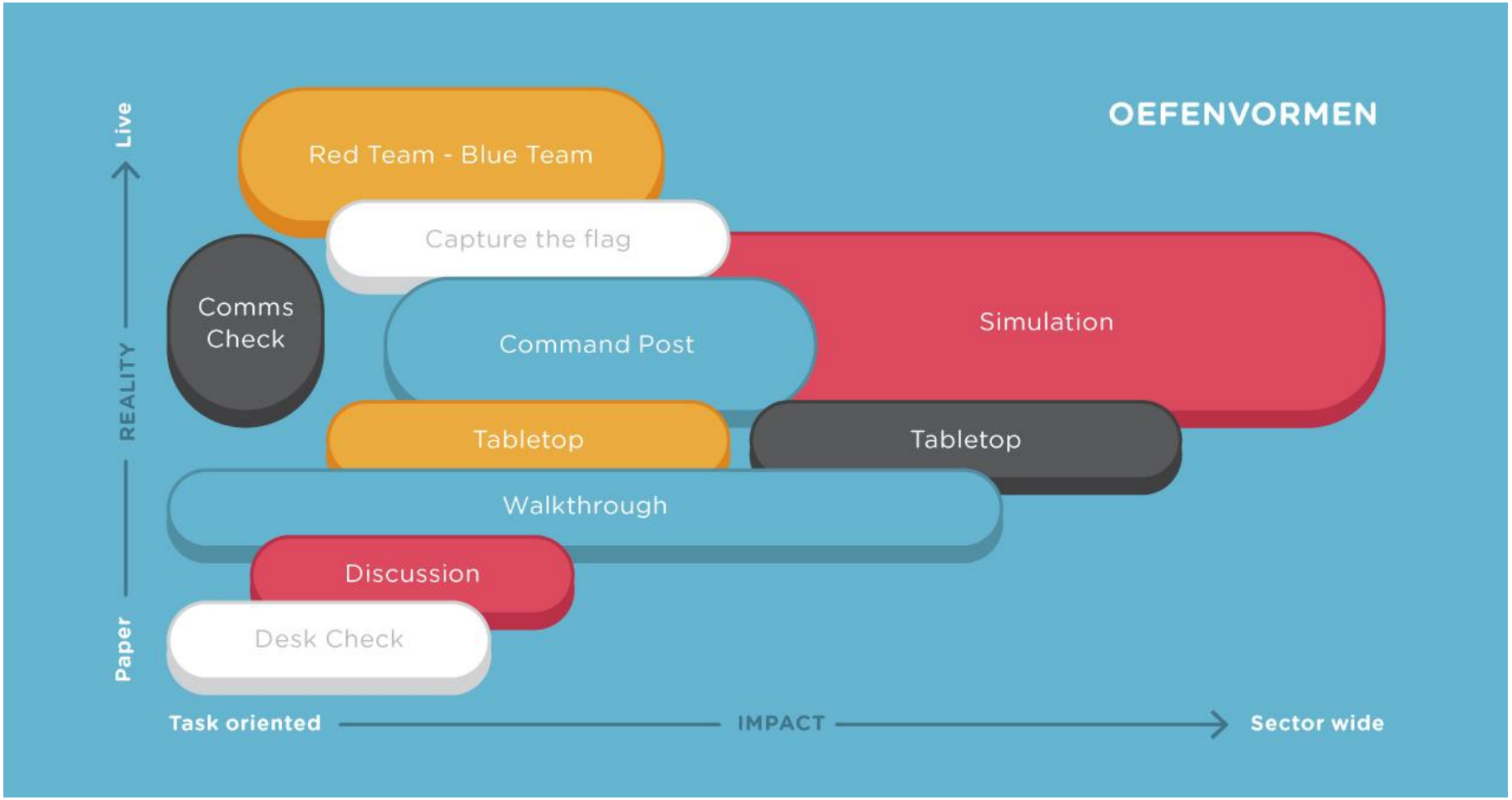
Exercises can be used to

- Validating policies, plans, procedures, training, equipment and/or inter-organizational agreements
- Testing ICT disaster recovery systems
- Clarifying and training personnel in roles and responsibilities
- Improving inter-organizational coordination and communications
- Identifying gaps in resources
- Improving individual preformance
- Identifying opportunities for improvement
- Providing a controlled opportunity to practice improvisation

Performance objectives can be

- *orientation/demonstration*: simulating experience of an expected situation to increase awareness of vulnerabilities and the importance of effective action in response to the simulated conditions;
- *learning*: enhancing knowledge, skills, or abilities by individuals or groups with the goal of mastering specific competencies;
- *cooperation*: providing an opportunity for people to work together to achieve a common end result;
- *experimenting*: trying new methods and/or procedures with the intent of refinement; and,
- *testing*: evaluating a method and/or procedure to assess which components are sufficiently developed.

Exercise types

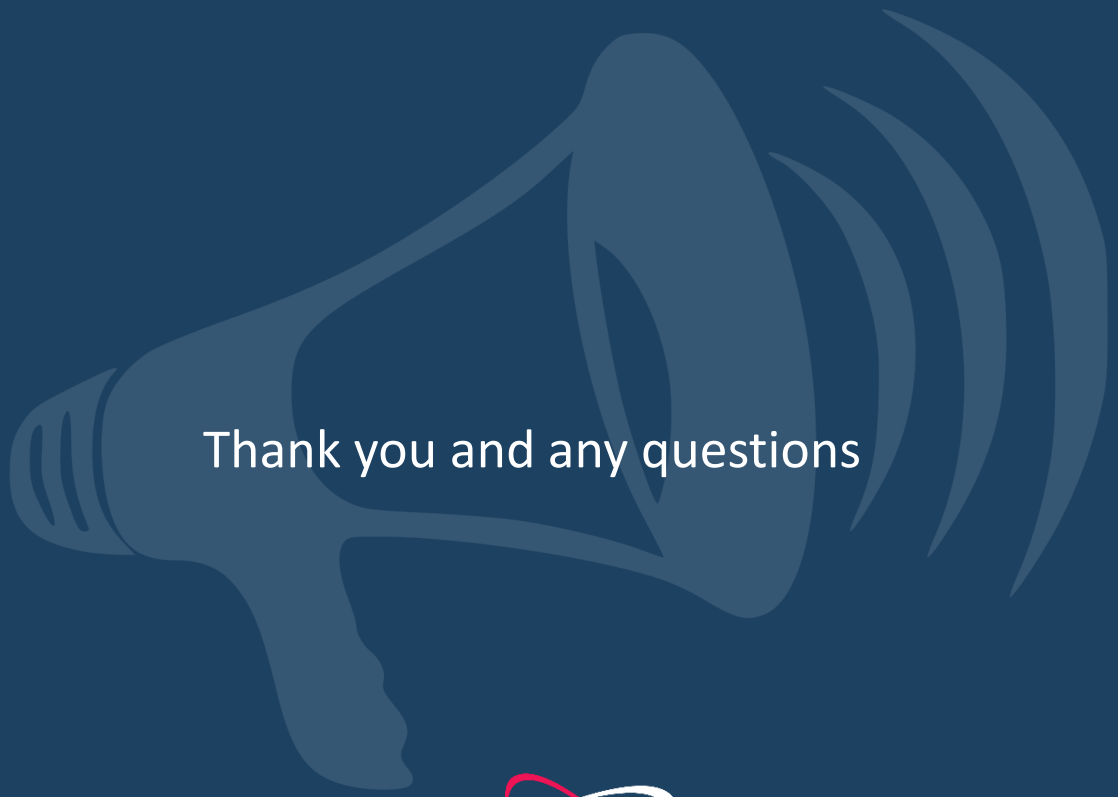


Exercise types

- **Desk Check** – A desk check is a method used to validate plans and procedures and any changes to them. This is usually conducted in conversation with the author of the plans and procedures.
- **Tabletop exercise** – a tabletop exercise covers all aspects of crisis management. All participants receive the same information in advance about the simulated crisis situation and their role.
- **Distributed tabletop exercise** – A distributed tabletop is a role-play exercise where participants play their usual role in the plans and procedures of a scenario. This exercise is similar in structure to a tabletop exercise, but there is no possibility for discussion.
- **Command Post Exercise (CPX)** 100 – In a CPX (sandbox exercise), a crisis is simulated without the use of emergency services, external environmental factors or players. The crisis teams deal with questions and orders in a realistic and evolving scenario.
- **Red Team/Blue Team -** In a Red Team/Blue Team exercise, the red team attacks the network or another important business service and the blue team tries to foil the attempt.

Community crisis management event

- November 2017
- In Malaga
- Scenario in the making



Thank you and any questions

GÉANT

Networks · Services · People

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).