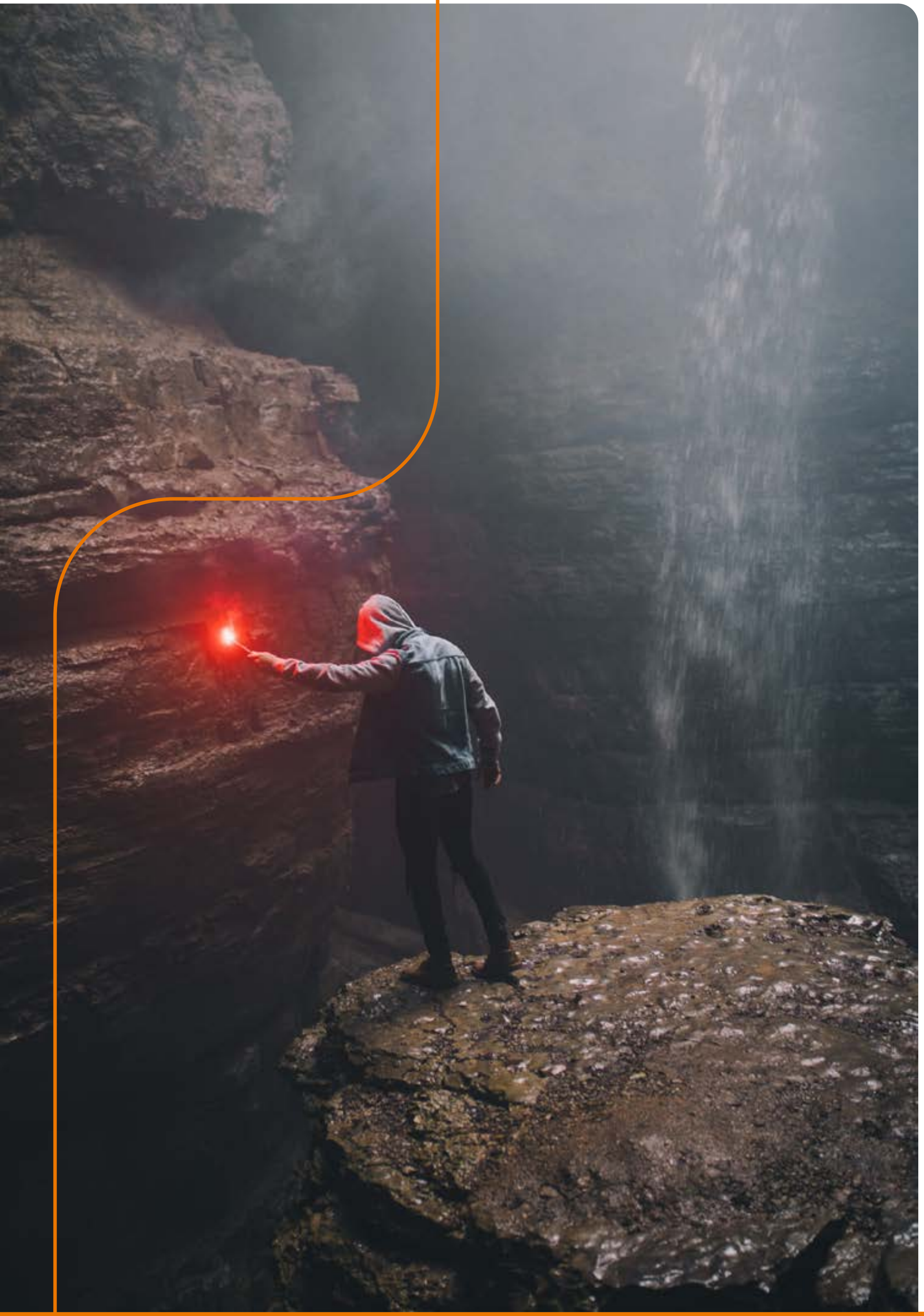
TRAINING FOR CRISIS: HOW PREPARE FOR THE WORST

Charlie van Genuchten *SURF*

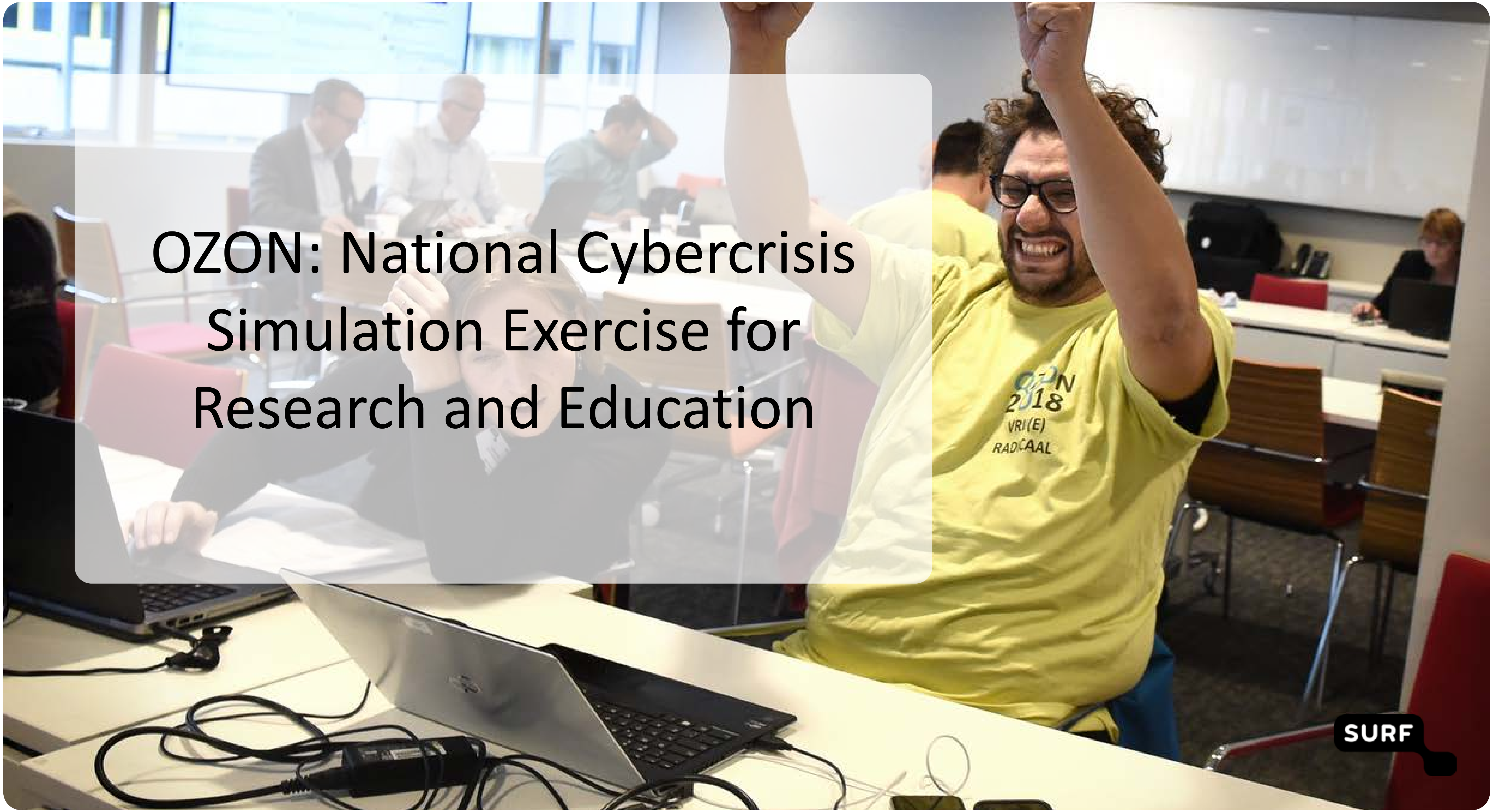
EUNIS/EUA Webinar May 6, 2021

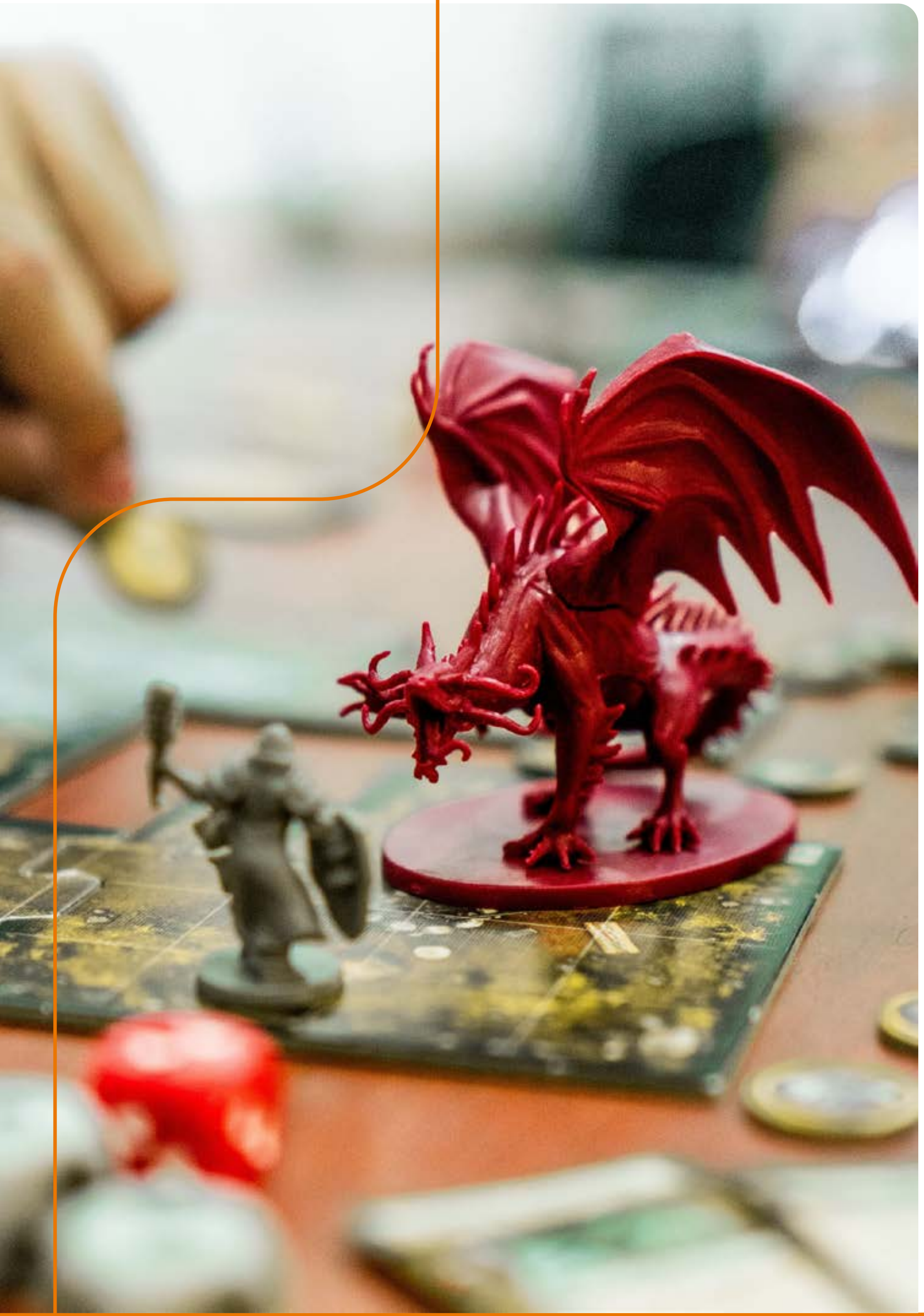


Why exercise?

- Validating policies, plans, procedures
- Testing ICT disaster recovery systems
- Training and validating roles and responsibilities
- Improving inter-organizational coordination and communications
- Identifying opportunities for improvement and gaps in resources
- Providing a controlled opportunity to practice improvisation

OZON: National Cybercrisis Simulation Exercise for Research and Education





Set up

- Exercising with 50 organisations

  → Two exercise leaders per organisation that help create the scenario for their organisation
- 1000+ people throughout the coutnry
- Everyone at their own work space
- 1 full day
- Ministry and other external stakeholders play along
- Journalists and media simulator
- Technical injects for the operational level

Scenarios

- 2016: Ethical hacking and data leaks
- 2018: Ransomware
- 2021: State actor attack

Most important lessons

- Make sure cyber-, network- and information crises are incorporated in your organisational crisis management procedure
- Regular (cyber)crisis exercises are a great way to improve your resilience as an organisation and raise awareness for security
- Biggest challenges named throughout the years:

  → Internal communication

  → Stakeholder management

  → Situation analysis

  → Endurance