

# Cybercrisisexercise OZON 2016

FROM IT TO BOARDROOM –  
A GAP BRIDGING EXERCISE



Remon Klein Tank  
(Wageningen University and Research / SURFcet)  
Sandy Janssen (SURFnet - Netherlands)

**SURF** NET

# Introduction

## • Remon Klein Tank (CEH, CISSP)

- Initiator and projectleader OZON
- Cybersecurity specialist at Wageningen University and Research
- Member of SURFcert (first Dutch Computer Emergency Response Team)
- SCIRT / SCIPR member (cybersecurity expert community)



## Sandy Janssen

Master of Law  
(University of Groningen)  
on safety regulations  
for High Voltage  
Power Lines.



Worked at the Centre of Information Technology at the University of Groningen.

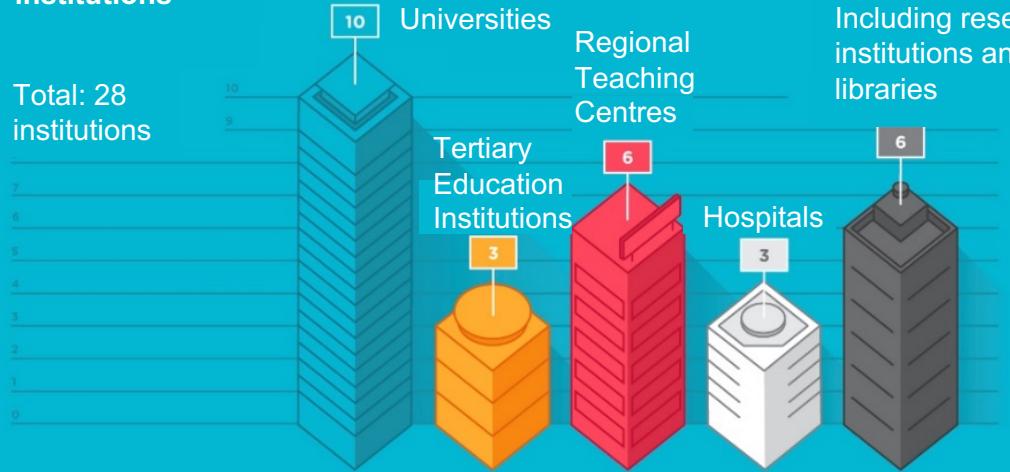
Since May 2016 part of Young Talent program of SURFnet and involved in setting up cyber crisisexercise OZON

Wrote whitepaper and script for setting up cybercrisisexercises

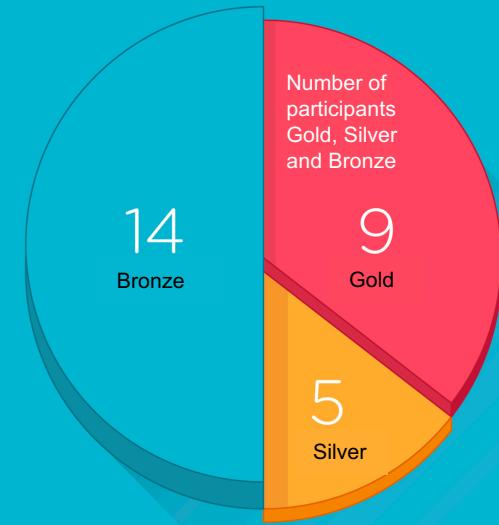
# Participants

## Participating institutions

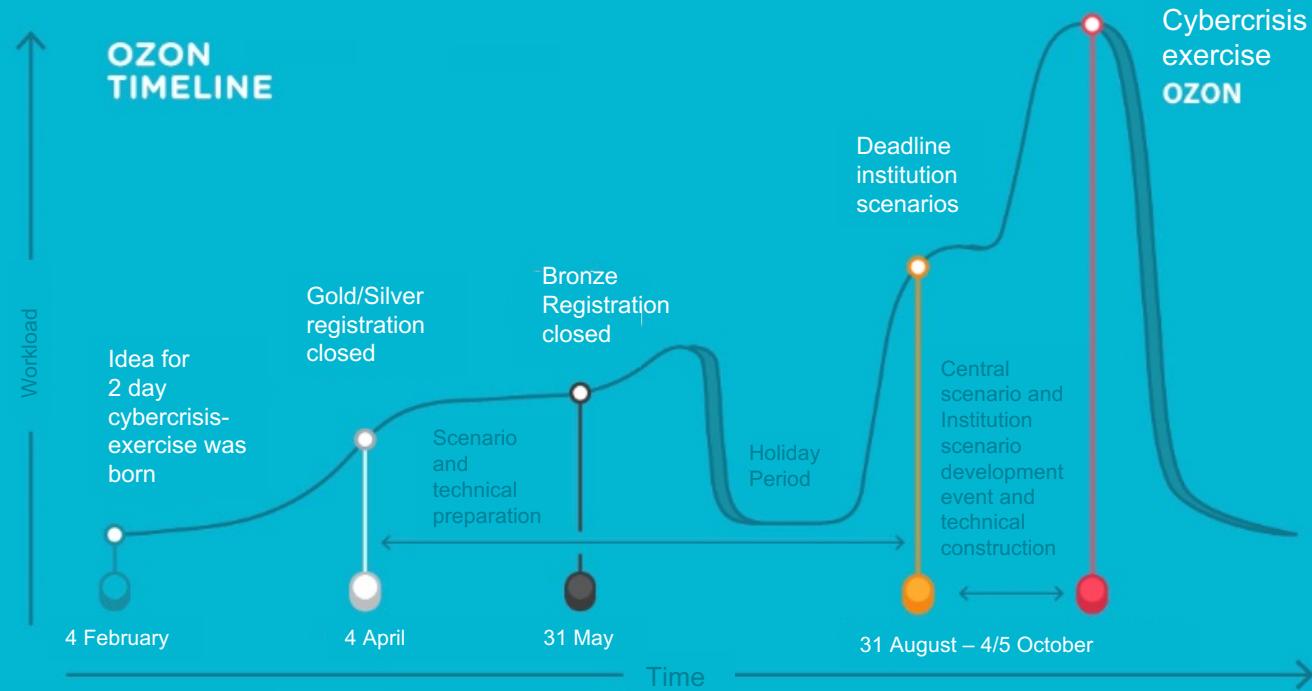
Total: 28 institutions



Other:  
Including research  
institutions and  
libraries

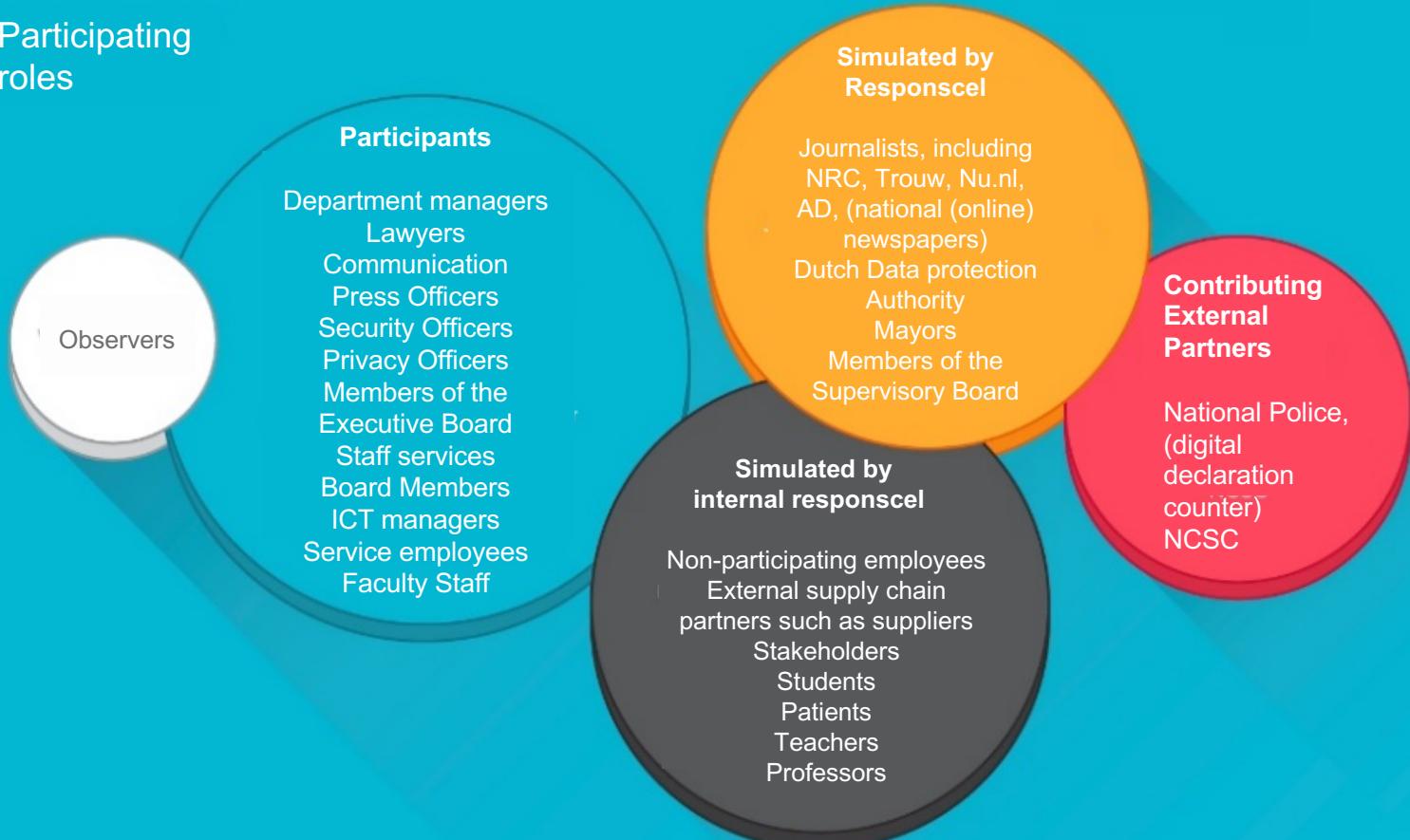


# Preparation



# Participating roles

## Participating roles



# Events

## Media and communication



**nrc.nl 'Hacktivisten' voor transparantie**

03/10/2015

De hackerscollectief 'Robbing Good' streeft naar het openbaren van misstanden in de organisatie-top. Wie niets verkeerd doet, heeft dus ook niks te verbergen' luidt het motto van de groepsleider die anonymiteit dient te blijven. In 2010 heeft het collectief een bijdrage geleverd aan Wikileaks en het hacken van Stratfor in 2012. In het teken van de internationale Cyber Security Awareness-week praat NRC met de groep over de positieve kanten van hacken.

**Je wilt graag anonym blijven. Zijn jullie een soort Anonymous?**

Alhoewel Anonymous een hoop geweldig hacktalent heeft willen wij Robbing Good daar niet mee vergelijken. Anonymous zijn tegenwoordig meer bekend om hun grote en vaak uitermate positieve acties. Een student aan de UvA schrijft "Supertargeted attacks en het plateaus van systemen van individuen zijn. Wij daar tegenover vinden het vooral belangrijk dat een bedrijf of publieke organisatie onheuse praktijken kan privacy en veiligheid."

Ozon.onion I - Een onvoldoende? 40 Euro lost het op

Aad Gille - 04/10/2016



COLUMN - Tijdens mijn onderzoek naar de onderwereld van het internet heb ik in het Dark Web, het deel van het internet dat het daglicht niet kan verdragen creditcardgegevens, drugs en wapens bestaan er ook webportals waar stud kunnen verbeteren. I legde een anonieme Bitcoin-betaling van €40 is het een onvoldoende om te laten toveren in een prachtig cijfer. Voor €80 kan rivalen naar een onvoldoende veranderen.

Om te testen of de service écht werkt heb ik €40 betaald om mijn ouderlijke mester aan de VU Amsterdam te veranderen. Om zo mijn benadeelen heb ik ervoor gekozen mijn enige 8 naar een 7 om te laat was mijn cijfer daadwerkelijk aangepast.

Aangezien de service goed werkt is het niet verrassend dat de uitermate positief zijn. Een student aan de UvA schrijft "Supertargeted attacks en het plateaus van systemen van individuen zijn. Wij daar tegenover vinden het vooral belangrijk dat een bedrijf of publieke organisatie onheuse praktijken kan privacy en veiligheid."

**nrc.nl**  
**Cyberveiligheid**  
**101**

05/10/2016

De acties van het hackerscollectief Robbing Good en het dark webportal Ozon.onion hebben het belang van cyberveiligheid weer op de kaart gezet. Om uzelf en uw organisatie zo goed mogelijk te beschermen tegen cybercriminelen, is bewustzijn van cyberrisico's en het nemen van beveiligingsmaatregelen van groot belang. Informatiebeveiligingsexpert Samme Drievellet spreekt in een interview met NRC over de need-to-knows in de cyberjungle.

**Wie zit er achter cyberaanvallen en datalekken?**

In tegenstelling tot wat er vaak op tv te zien is zijn hackers doorgaans geen pokdalige pubers die voor de lol organesaties aanvallen. Het zijn professional, georganiseerde hackers die doelgericht door; door;

- Cybercriminelen: zij zijn achter geld aan en plegen hierdoor fraude of verkopen informatie;
- Bedrijfsconcurrenten en buitenlandse inlichtingendiensten: zij stelen informatie om economische- of politieke voordelen te behalen;
- Hackers: het infiltreren van goed beveiligde systemen is een leuke uitdaging;
- Hacktivisten zoals Robbing Good: plegen cyberaanvallen uit politieke of ideologische doeleinden;



# Technical elements

## Robbing Good

knowledge is Power, Power to the People!



Disclosing critical research and business information on a prepared website

This is an OZON exercise website. All content on this website is for exercise purposes only.

Welkom op deze veilige Operation Ozon website

**Door het enorme volume aanvragen is er enige vertraging in de verwerking.**

Wij bieden verschillende diensten aan:

Create Your own Grades (Even niet beschikbaar op de WUR want die ligt plat 😊)

Download een patiëntendossier

Crowdfund het hacken van een cijferadministratie

En nu ook beschikbaar:

Sensitive docx: spannende interne documentatie van diverse publieke instellingen

Binnenkort:

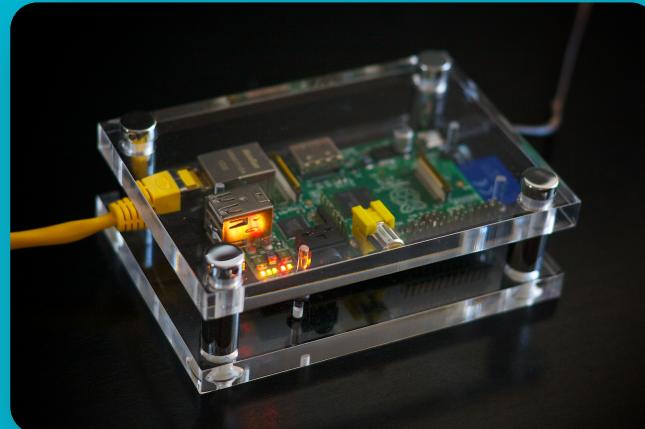
**tilburg de gekste** [@yousnowig\\_3d](#) [Follow](#)

BAM! Gewoon een 9 voor Internationaal Strafrecht. #<http://createyourowngrades.nl/>

[Reply](#) [Retweet](#) [Favorite](#) [More](#)

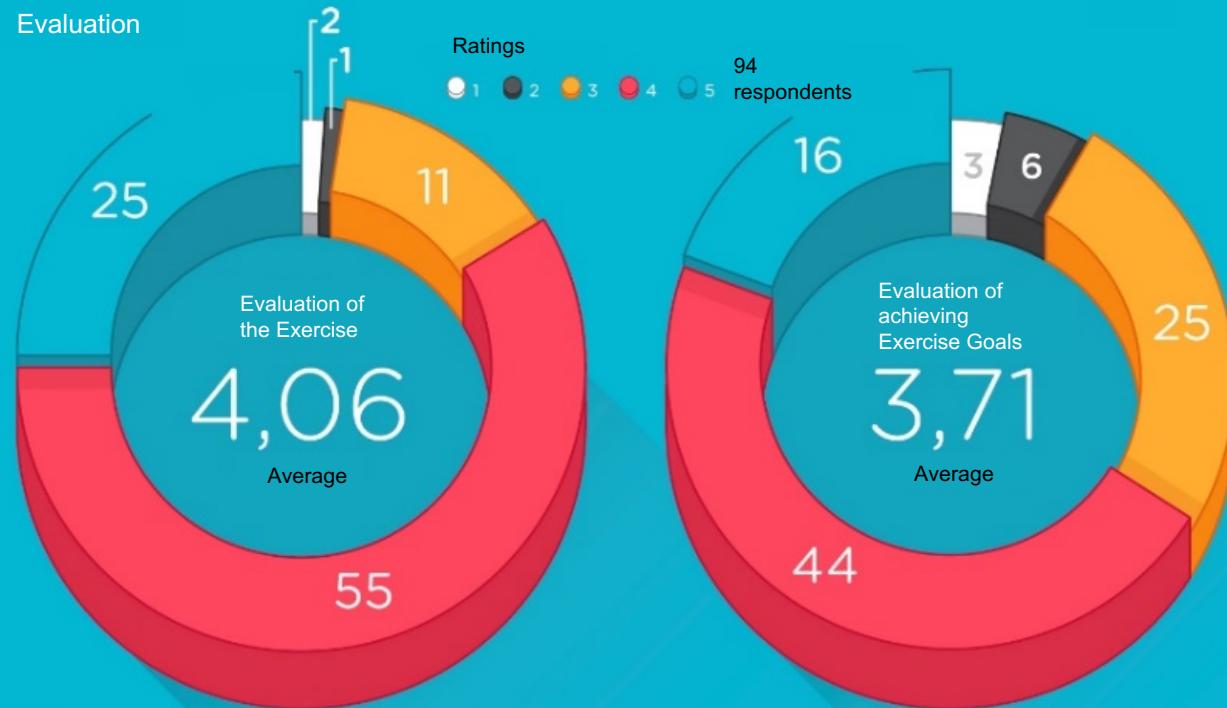
7:50 AM - 4 Oct 16 · Embed this Tweet

Offering "create your own grades" through websites



Raspberry pi's to be found in the network with mirrors of the websitess

# Ratings



# Cybercrisisexercise OZON

## Background and purpose

- Crisis exercises within institutions are mostly physically oriented (i.e, fire, evacuation, drills)
- The need to practice with cyber crisis / IT security
- Inspiration by participating in other big cyber exercise

## Purpose:

- Increase awareness and resilience
- To test the internal and external information chain
- To test internal communication, processes, and testing protocols
- To increase knowledge and understanding of the development a cyber crisis

## Conduct and performance

- The content was prepared by OZON team and the institutions, for completeness and robustness we had assistance of external agency.
- Two days of exercise directed from the central location at SURFnet, the players practiced on location and in their own role.

## Outcomes

- Experienced as succesful, informative and highly realistic
- Voluntary participation and practiced with great enthousiasm
- The involved where very positive and the atmosphere was good.
- Gaps where bridged between operational/tactical and strategic level
- Gaps where bridged between different disciplines like communication and technique
- Cooperation between institutions strengthened

## Scenario and exercise

- Multilayer attack, with ethical and criminal component;
- Strategic and technical dilemmas to encourage cooperation between strategic, operational and tactical levels
- Both technical and strategic challenges; leakage of researchdocuments, business data, manipulating data, mirror sites, simulation of productionenvironments
- Big challenge to find compelling case for bridging the gaps between technical and strategic level

## Results, recommendations and what's next

- Make cybersecurity integral part of crisis management
- Sharing information earlier in crisisprocess between organisations
- Research into form of national coordination in a sector-wide cyber threat. To define autonomy and mandate of the institutions
- To practice more large- and small exercises, sectoral- and/or topic specific. Preparation and execution of exercise together to achieve economies of scale
- To share the outcomes, conclusions and recommendations of exercises to create more awareness and to create support of cyber threats and exercises.
- Outcomes, lessons learned and recommendations stipulated in whitepaper, script for cybercrises exercise and video impression

# To know more? / Questions?

- What's next: OZON 2018, NOZON small exercise with institutes, International cybercrisisexercise Géant (European collaboration on e-infrastructure for research and education) internal cybercrisisexercise within SURFnet
- White paper available in Dutch and English
- <https://www.surf.nl/kennisbank/2016/whitepaper-cybercrisisoefening-ozon.html> /
- Article in Informatiebeveiliging Magazine Moens, A, Janssen, S.B "Ozon: Bruggen bouwen; een cybercrisisoefening" PvIB 01-2017, p. 10-15
- Script of OZON in Dutch
- <https://www.surf.nl/kennisbank/2017/handleiding-en-draaiboek-opzetten-cybercrisisoefeningen.html>  
Soon also in English available
- Video impression with English subtitles
- <https://www.youtube.com/watch?v=DqS0g9kuDmc>

