INTERNATIONAL SECURITY ACTIVITIES

GÉANT SIG-ISM

Security management Inventory

WISE

Workshop in Abingdon, Feb. 26 – 28

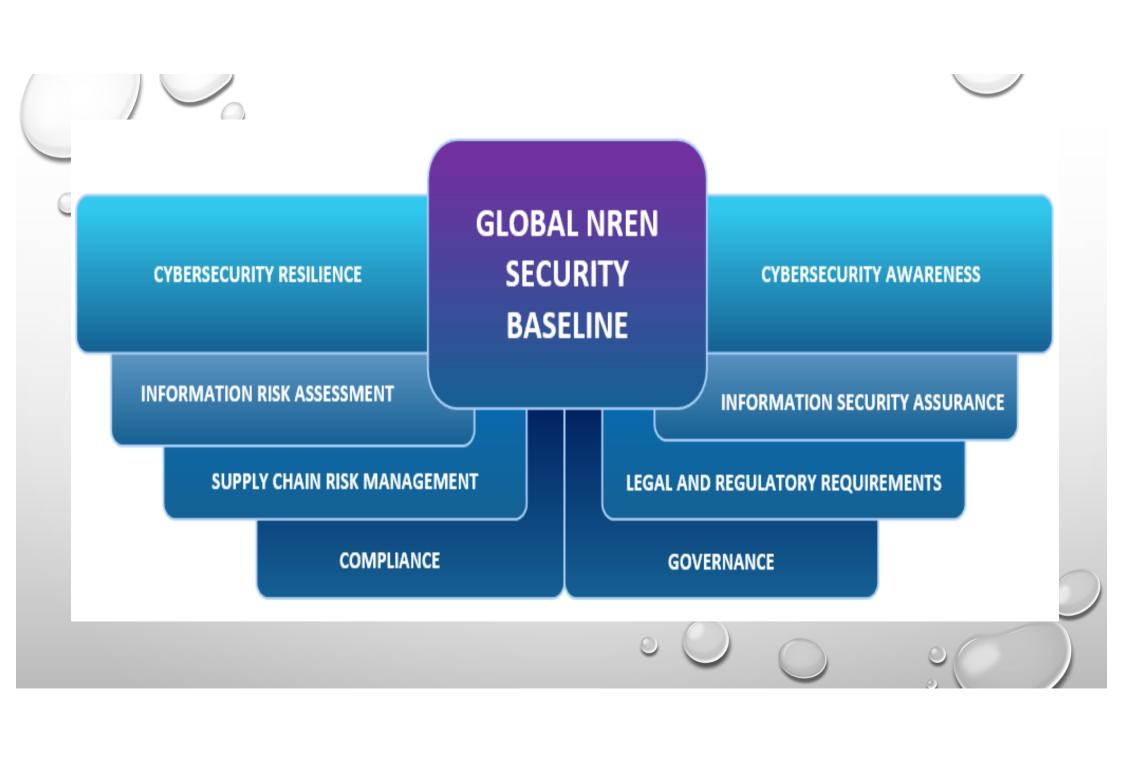
TF-CSIRT

CSIRT/FIRST meeting

Global NREN security group

Crisis exercise
Security baseline
DDOS mitigation

FIRST Academic Security SIG





2ND CRISIS EXERCISE GLOBAL NREN SECURITY GROUP

Participants:

RNP, Esnet, Internet2, Canary, Jisc, GÉANT, Nordunet, DFN, SURFnet, SANREN, AARNet, REANNZ

Purpose:

get a good representation in a VC within 1 hour to discuss and coordinate a global crisis

Method:

pre-announce for exercise 'window', announce by e-mail, telephone follow-up, VC

<u>Treath</u>: Strong suspicion on coming large scale, multi-vector DDOS attacks on scientific e-infrastructures by religious, right wing activists that think science is a treath for mankind

Timing:

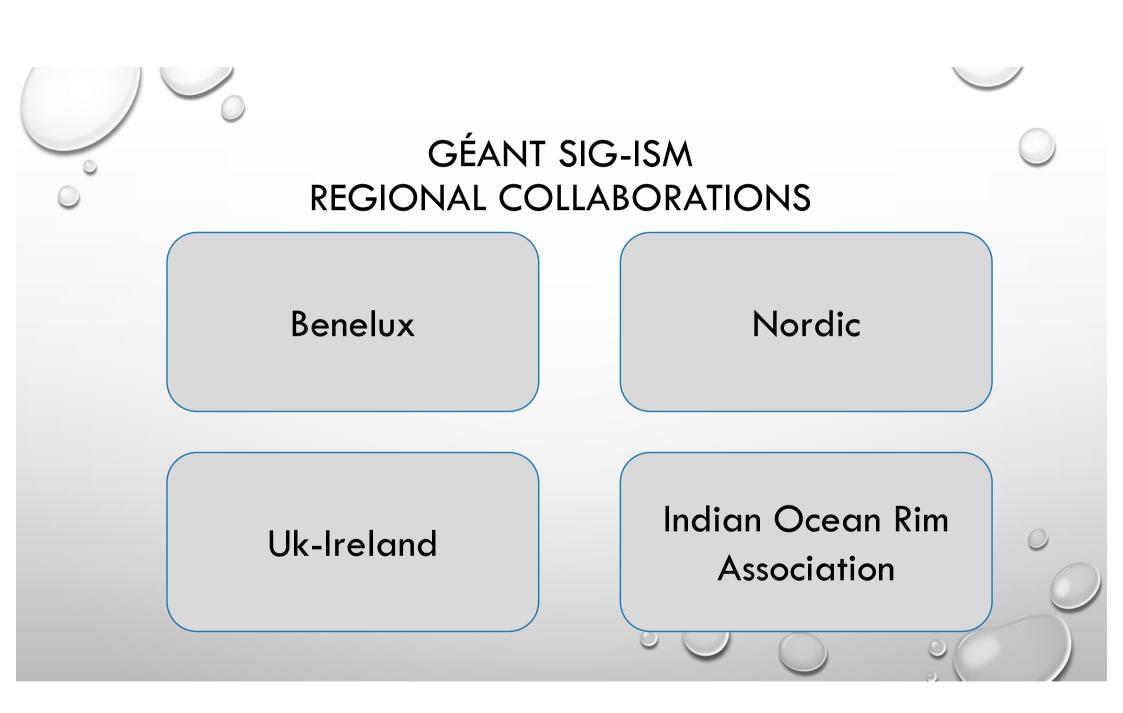
VC at 12.00 (noon) CET, announce e-mail 1 hour before

Results:

Telephone contact with all, within 15 minutes, 100% participation in VC

Conclusion:

++ VC is good for a 'war'-room
-- Strong dependency on
internet





GÉANT SECURITY WHITEPAPER

- Scope:
 - GÉANT and NRENs
 - Internal organisation of security, products and services, security for the constituents
- Reach: 2018 2022, input for GN4-3 program 2019 2022
- Status:
 - Whitepaper input collected from communities and individuals
 - Draft whitepaper reviewed by participants of communities and external NREN experts
 - Draft whitepaper reviewed by GÉANT GPPC
 - Whitepaper distributed to NRENs for 'scoring'



GÉANT WHITEPAPER: 6 SUBJECTS AREAS

Security Baselining For Products, Services And Organisations

Managed Security Products and Services

Legal and Privacy Compliance

Management of Risks

Training and Awareness

Incident Response, Business Continuity and Crisis Management

GÉANT Community Program

GÉANT Whitepaper: 12 Subject Proposals

Annex 1: Baselining for Products and Services and Organisations

Annex 2: Firewall on Demand

Annex 3: Centralised DDoS mitigation

Annex 4: SOC operations and tools

Annex 5: Vulnerability Assessment "as-a-service"

Annex 6: EduVPN

Annex 7: Other security products and services

Annex 8: Legal and Privacy Compliance

Annex 9: Management of Risks

Annex 10: Training

Annex 11: Awareness

Annex 12: Incident Response, Business Continuity and Crisis Management