GÉANT
Networks • Services • People

Security for Research and Education

Trends and current services

Alf Moens
Cybersecurity lead GÉANT
Workpackage lead GÉANT GN4-3 WP8 Security
Evangelos Spatharas
Head of Security GÉANT

19 January 2021

www.geant.org

1

Why Security? Just look at the Threats!

https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

2

Trends in Security 2021 – Top Threats for R&E

DDOS
Ransomware
Supply chain
Advanced Persistent Threats (APT)
Identity theft / Phishing / CEO fraude
Cryptomining

3

What can we do about that?

- Intelligence sharing
- Situational awareness
  - What and where is your infrastructure? Is it healthy?
  - What is happening in your environment?
- Training and awareness
- Tools

4

GÉANT Security products and services

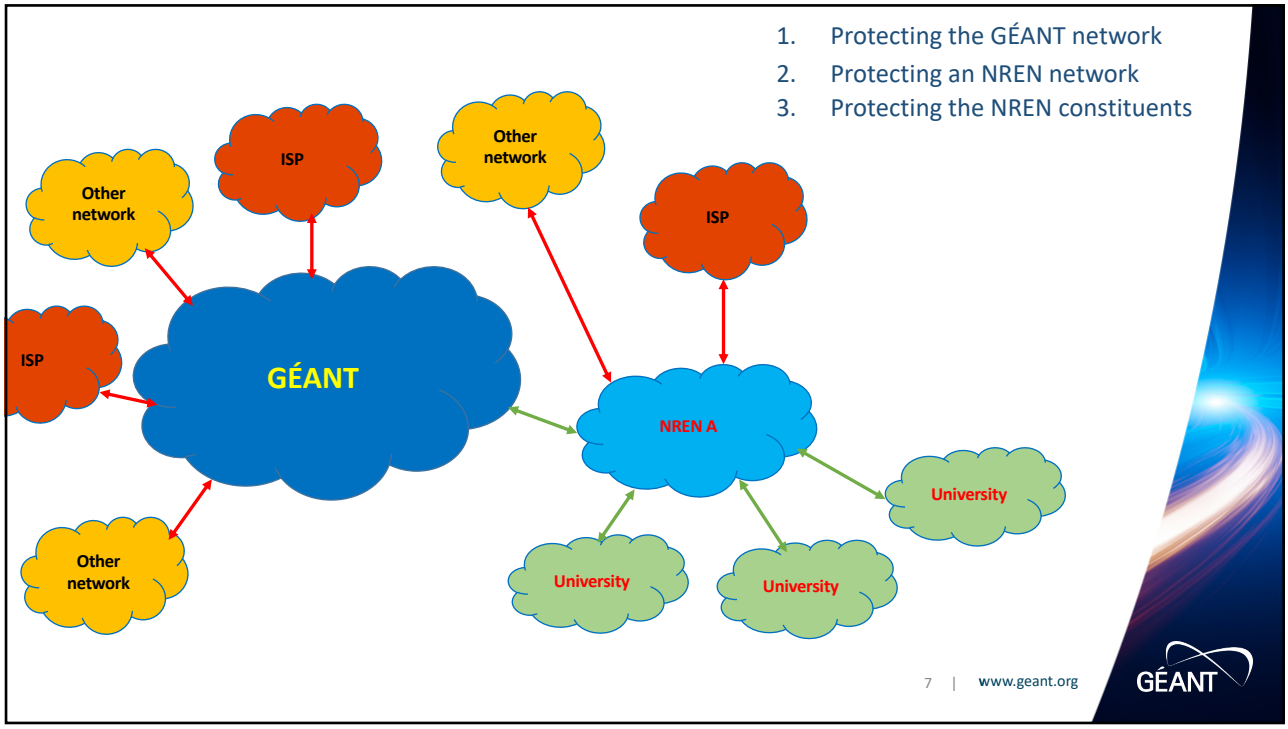
- Security Baseline (framework & assesments/benchmark)
- Training and awareness (Transits, TI, CLAW, CERT, netw security, cybersecmonth)
- Products and services
  - DDOS/SHARP
  - DDOS/NEMO
  - TCS
  - eduVPN (Official product in France)
  - SOC
  - VAAS (MoU Holm security)

5

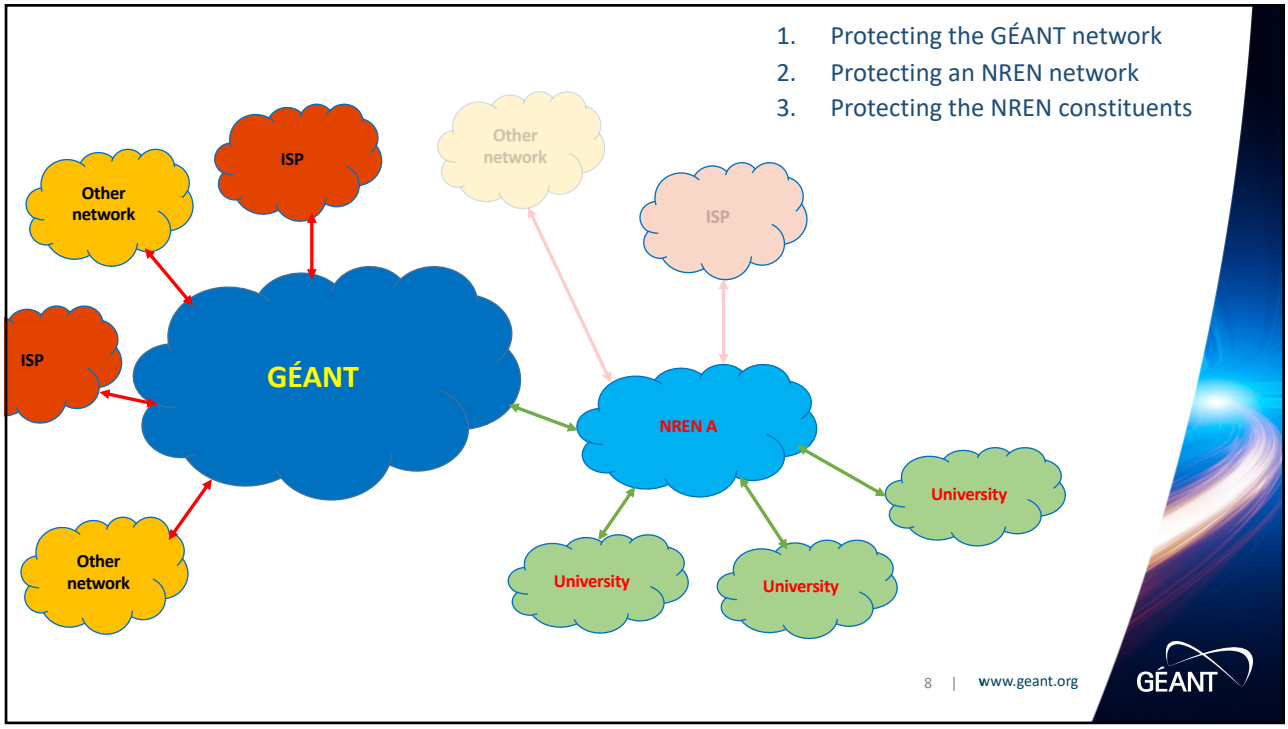
DDOS – Service Offering (simplified)

1. Protecting the GÉANT network
2. Protecting an NREN network
3. Protecting the NREN constituents

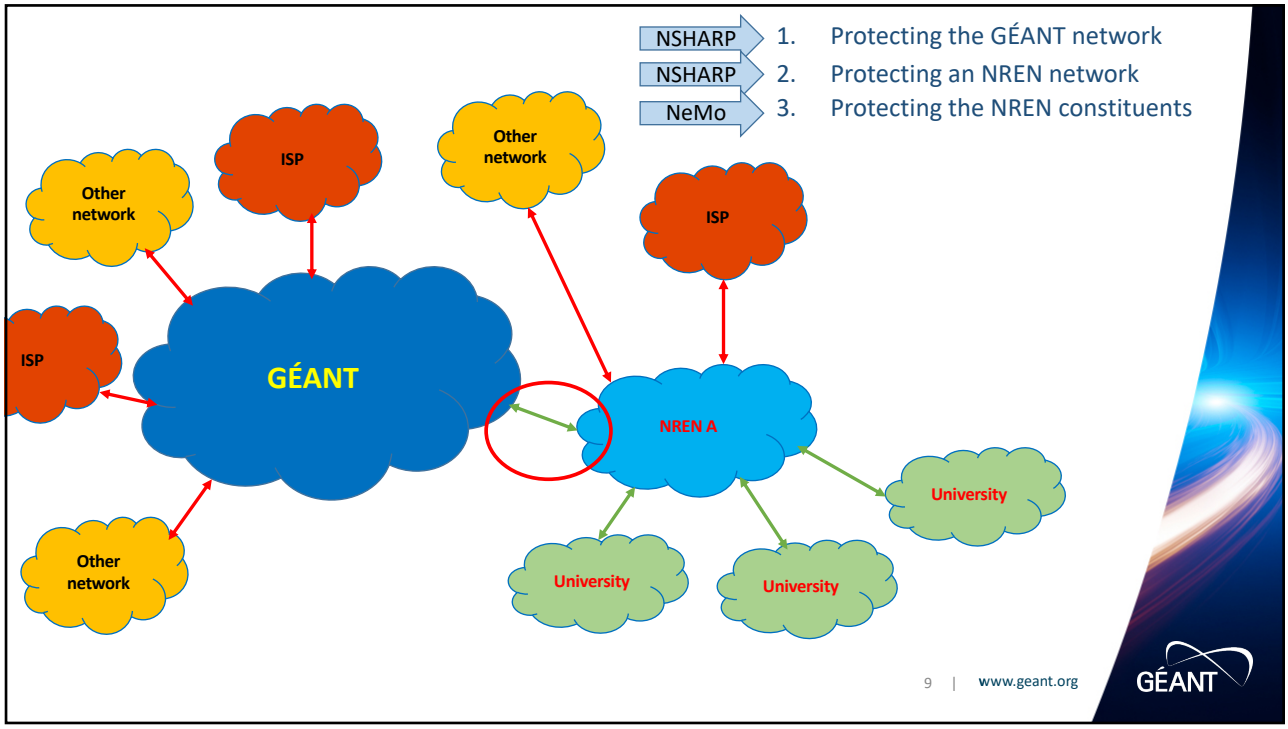
6


1. Protecting the GÉANT network
2. Protecting an NREN network
3. Protecting the NREN constituents
Other network
ISP
Other network
ISP
ISP
GÉANT
NREN A
University
Other network
University
University
7 | www.geant.org
GÉANT

7


1. Protecting the GÉANT network
2. Protecting an NREN network
3. Protecting the NREN constituents
Other network
ISP
Other network
ISP
ISP
GÉANT
NREN A
University
Other network
University
University
8 | www.geant.org
GÉANT

8



9

NSHaRP

NSHARP
NETWORK SECURITY HANDLING AND RESPONSE PROCESS

- An automated incident notification and handling system
- Extends detection and mitigation to the borders of GÉANT
- Supported by GÉANT OC and Security

DDoS C&A – Oct. 2019

FoD – Jan. 2016

FlowMon – Jun. 2015

RTBH – Oct. 2014

NSHaRP Bday - 2011

10 www.geant.org

10

DDoS C&A Future

- ✓ Tender for complete DDoS solution
- ✓ Deployment during 2021
- ✓ Most likely a paid service
- ✓ Overcome capacity limitations
- ✓ Live portal for customers
- ✓ Better detection/mitigation + custom mitigation profiles for NRENs need it
- ✓ Application layer mitigation support

11

DDOS – GÉANT future service offering

- Research into different deployment models
- Whitepaper describing best solutions
  - For different kind of attacks
  - For different situations, depending of your upstream and downstream architecture

12

DDOS - Nemo

- Detection and mitigation – toolset
- Based on DFN DDOS solution – packaged and documented
- Integration with Firewall-on-Demand
- Can be run
  - In the GÉANT network
  - In the NREN network

13

Security Operations Center

GN4-3 WP8 SOC
SOC tools architecture
Comprehensive set op SOC tools

NREN Security Operations Center

Several operating models:
- NREN centric
- NREN plus universities
- NREN plus outsourcing

Sharing Security Intelligence
- Indicators of compromise
- IP addresses, domains, e-mail addresses
- Background infiormation
- Field observations

Global Cooperation

AARnet - JISC - CANARIE

14

Security Baselining

Advanced
30% of NRENs
Solid security practices
Some NRENs are already compliant, most implement just individual requirements

Expert
10% of NRENs
Sophisticated security programme
Only a few NRENs are compliant
This is a long-term goal to achieve

Baseline
80% of NRENs
Entry-level security
The majority of NRENs are already compliant

15

Security Baselining

Policy
- *Management Commitment and Mandate*
- *Internal Security Policy*
- *Acceptable Use Policy*
- *Regulatory and Privacy*

People
- *Training and Awareness*
- *Personnel Management*
- *Supplier Management*

Threats
- *Risk Management*
- *Incident Management*
- *Business Continuity Management*

Operations
- *Tools*
- *Cryptography*
- *Access Management*
- *Patch Management*
- *Vulnerability Management*

16

Baseline, example, 2.3 supplier management & 3.3 Business Continuity

NO2.3	Requirements	1	2	3
NO2.3.1	A supplier security policy is in place and accessible for staff involved in contracting suppliers.	✅	✅	✅
NO2.3.2	All suppliers have contracts stating relevant security aspects.	✅	✅	✅
NO2.3.3	All suppliers are assessed according to their criticality and business impact and listed at a central location.	✅	✅	✅
NO2.3.4	SLAs, SLA reporting, meeting notes and other documents to assess the suppliers' performance on a regular basis are available.		✅	✅
NO2.3.5	Changes in the suppliers' services are monitored on a regular basis		✅	✅
NO2.3.6	Where appropriate, suppliers' services and products are audited or penetration-tested.			✅
NO2.3.7	Where appropriate, suppliers handling sensitive data have signed an NDA.			✅

NO3.3	Requirements	1	2	3
NO3.3.1	A BCM process is defined, documented and implemented.	✅	✅	✅
NO3.3.2	A Business Continuity Manager responsible for the BCM process is assigned.	✅	✅	✅
NO3.3.3	A BCP exists, which covers at least disasters produced by power failure, fire and water.	✅	✅	✅
NO3.3.4	A list of managers responsible for handling disasters at any point in time is defined.		✅	✅
NO3.3.5	The BCP covers all NREN-specific disasters from the GÉANT Disaster List.		✅	✅
NO3.3.6	The organisation participates yearly in a crisis simulation, such as the GÉANT CLAW workshops.			✅
NO3.3.7	A manager on duty is assigned to be available on call 24/7/365.			✅

17

Task 2: Security Baselining (example)

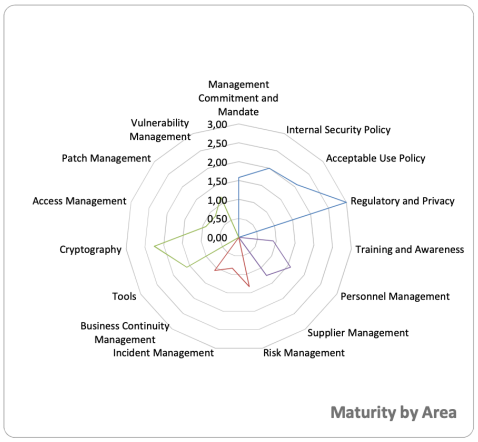
Security maturity

Current Maturity Score

Functions	Security Practices	Current	Maturity 1	2	3
Policy and Leadership	Management Commitment and Mandate	1,58	0,33	0,25	1,00
Policy and Leadership	Internal Security Policy	2,00	1,00	1,00	0,00
Policy and Leadership	Acceptable Use Policy	2,08	0,83	0,75	0,50
Policy and Leadership	Regulatory and Privacy	3,00	1,00	1,00	1,00
People	Training and Awareness	0,92	0,67	0,25	0,00
People	Personnel Management	1,58	0,83	0,50	0,25
People	Supplier Management	1,25	0,50	0,50	0,25
Threats	Risk Management	1,33	0,83	0,25	0,25
Threats	Incident Management	0,83	0,33	0,50	0,00
Threats	Business Continuity Management	1,08	0,83	0,25	0,00
Operations	Tools	1,58	0,83	0,25	0,50
Operations	Cryptography	2,25	1,00	0,75	0,50
Operations	Access Management	0,92	0,67	0,25	0,00
Operations	Patch Management	0,83	0,33	0,00	0,50
Operations	Vulnerability Management	1,17	0,67	0,25	0,25

Functions	Current
Policy and Leadership	2,17
People	1,25
Threats	1,08
Operations	1,35

Current Maturity Score

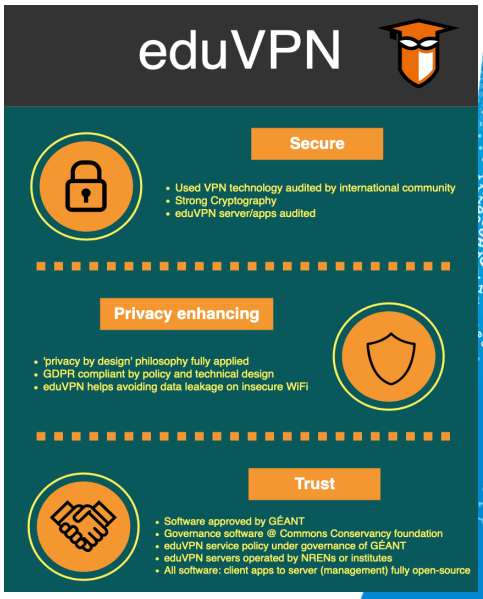


18

Status August 2020:
9 countries added in apps: Norway, Uganda, Pakistan, Finland, France, Sri Lanka, Morocco, Estonia, Albania

28 institutes added in apps: Unit, EUR, PolSl, STC, Trimbos, HEAnet, Tuni, Differ, Perdana, Pionier, GÉANT, Cnous, CSC, Uminho, HS-OS, Hiof, UniOsnabrück, VAMK, DIAK, IPB, University of Nimes, ENSMA, RENU, VU, HSTrier, KENET, Saxion, TUDelft

Estimated between 35,000 and 60,000 unique App downloads
Example: Radboud University (NL) reported over June 2020: 3300 unique users, max 900 simultaneous users



19

alf.moens @ geant.org
www.geant.org

As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3)

20