EaPConnect Cybersecurity Workshop 2022
GÉANT Security Roadmap

Alf Moens

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).

Who Am I?

Alf Moens, infected with collaboration virus

GÉANT
www.geant.org

Cybersecurity lead
Workpackage lead WP8 (GN4-3 & GN5-1)

SURF

TU Delft

GÉANT

2021-2026

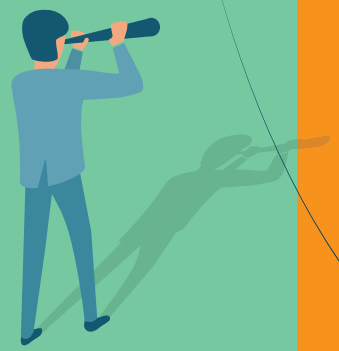
GÉANT Association Strategy

The GÉANT Association is the collaboration of European National Research and Education Networks (NRENs).

Together, we deliver an information ecosystem of infrastructures and services to advance research, education, and innovation on a global scale.

Vision

To collaborate to deliver the infrastructures and services that enable the R&E community to excel.



Mission

To empower R&E with an open, innovative, and trusted information ecosystem.

Ambition

To address and anticipate the needs of the R&E community by offering sustainable, open, innovative and trusted infrastructures and services.

To be a trusted and preferred-choice partner to the benefit of the European R&E community.

To collaborate and share knowledge to enable NRENs to improve their performance, both individually and collectively.

The GÉANT Association is driven by Eight Strategic Goals

Network
We are the trusted partner for pan-European and global advanced R&E networking.

Security
We provide a safe and secure information ecosystem for researchers, educators, and students.

Innovation
We continually evolve key infrastructures, innovate, and develop new services in order to fulfil the needs of the R&E community in a sustainable way.

Community
We are acknowledged worldwide as a leader for developing and supporting R&E networking communities, and global REN development.

European Union
We are seen by the EU as an indispensable partner for their vision.

Stakeholders
We forge relationships with other e-infrastructure providers, research infrastructures (RIs), and other stakeholders, to benefit the R&E community.

Governance
We have a governance structure that is agile and benefits from the diversity of our membership.

Funding
We will ensure financial sustainability to benefit our members.

www.geant.org

GÉANT Thematic Roadmaps 2021 - 2026

Above the Net

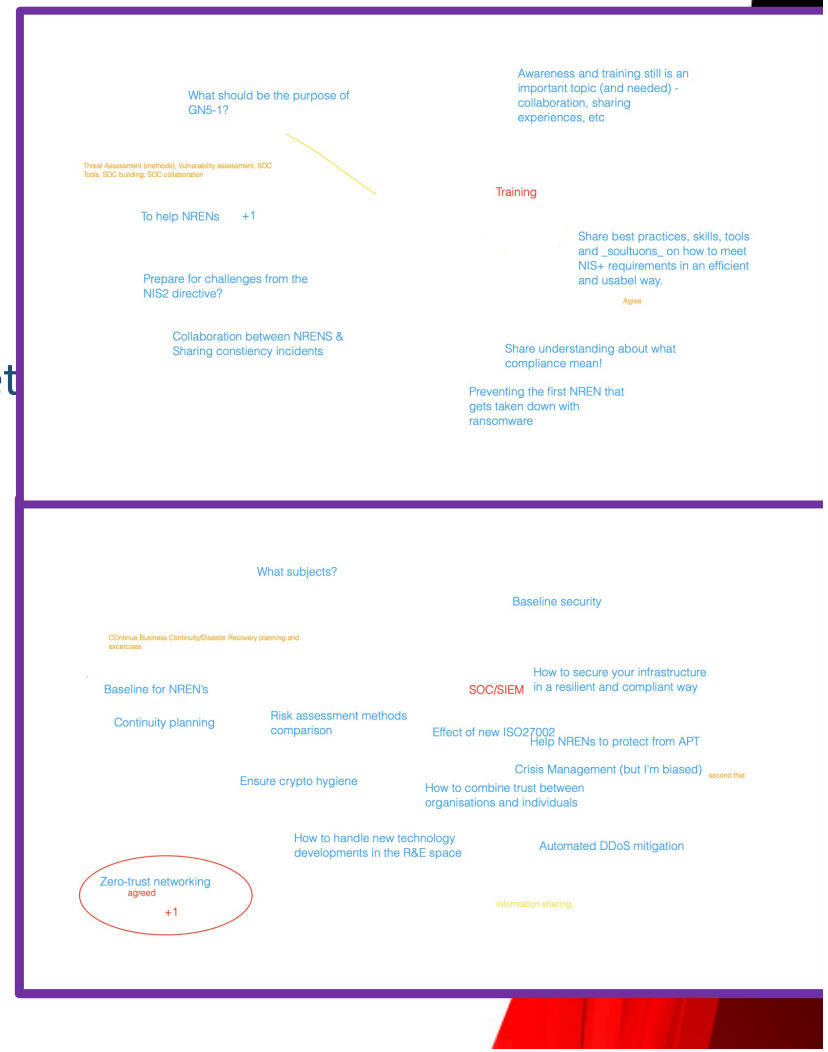
Security

Network and network services

Trust & Identity

Preparations for Security Roadmap

- Discussions in SIG-ISM and Security Day
- Discussions with Taskleaders WP8
- Security Insights Market research
  - Jisc, MARnet, IUCC, GARR, CARnet, RENATER, HEAnet, EEnet, RESTENA, URAN, RedIRIS and BELnet
- Interviews with experts
  - DEIC, Jisc, Internet2, DFN, Canary, SURF
- GA Security Spotlight
- GÉANT Compendium
- Insights from webinars, conferences, whitepapers



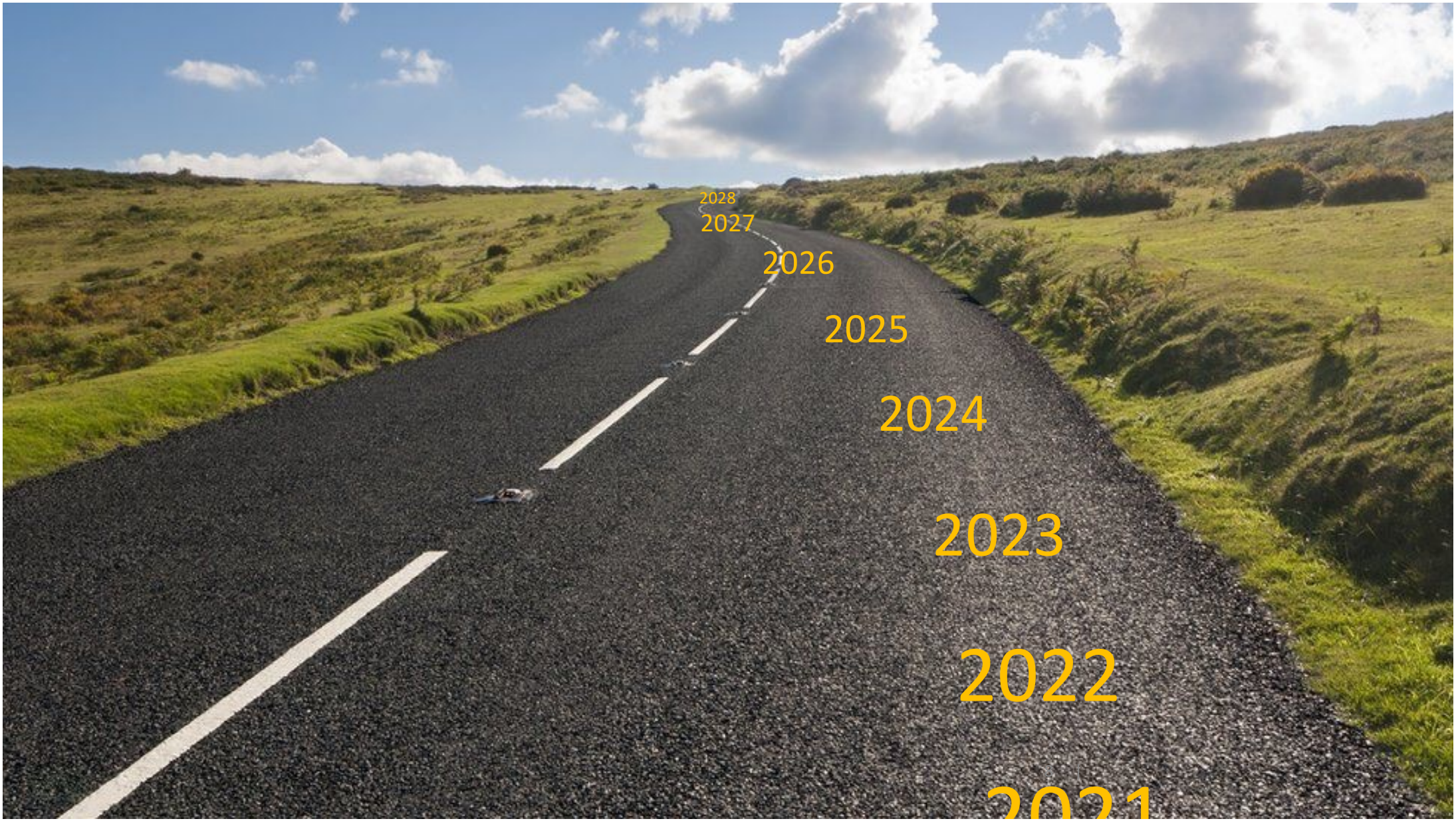
GÉANT Security Strategy – Main Objective

The main objective of the GÉANT Security Roadmap is to continue the support of NRENs and GÉANT to provide for a safe and secure infrastructure and services for Research and Education on national, European and global level, reducing the likelihood of major disruptions to services or loss of data.

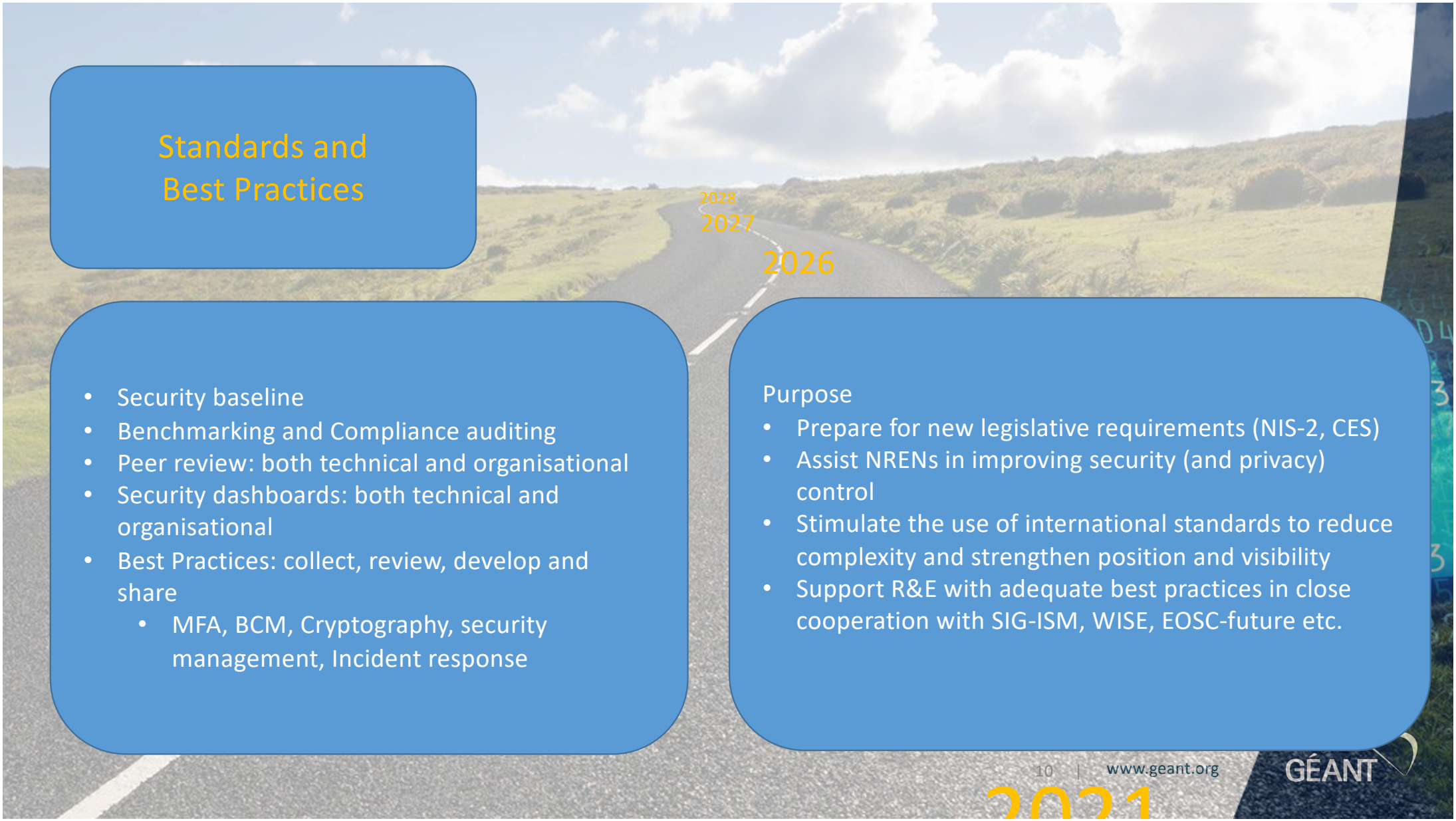
This will primarily be done by joint operation, development and sharing of products and services, active knowledge sharing, training and participation, in close collaboration with the staff of the NRENs, either in project style activities or in Task Forces and Special Interest Groups.

Major challenge: skill shortage

Identify and broker existing tools, encourage distributed services


2028
2027
2026
2025
2024
2023
2022
2021


Standards and Best Practices
Security Operations Support
Services and Tools
Incident Response and Crisis Management
Development of human capital, training and Awareness
Securing High Speed Networks
2023
2022
2021



Standards and Best Practices

- Security baseline
- Benchmarking and Compliance auditing
- Peer review: both technical and organisational
- Security dashboards: both technical and organisational
- Best Practices: collect, review, develop and share
  - MFA, BCM, Cryptography, security management, Incident response

Purpose

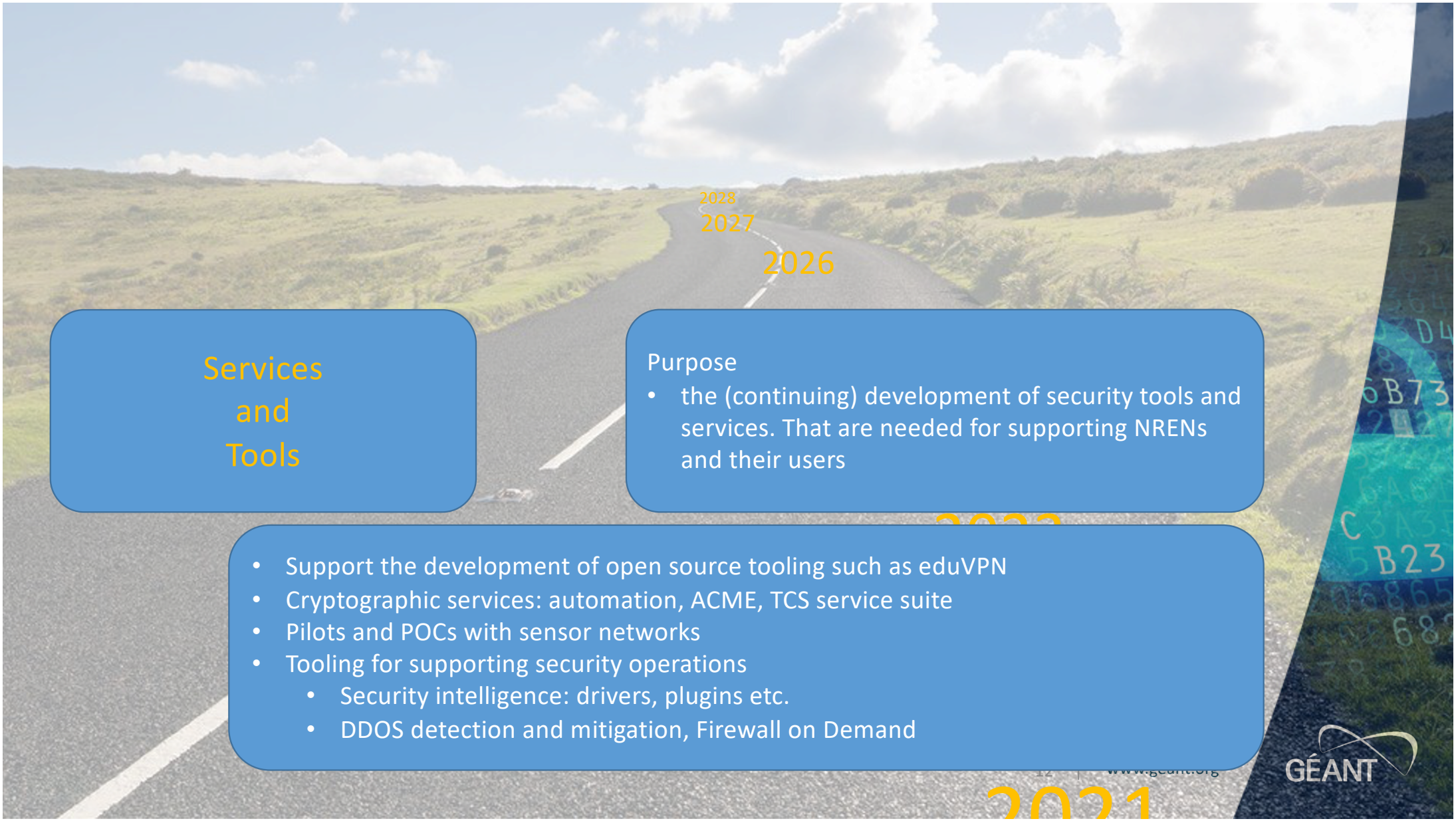
- Prepare for new legislative requirements (NIS-2, CES)
- Assist NRENs in improving security (and privacy) control
- Stimulate the use of international standards to reduce complexity and strengthen position and visibility
- Support R&E with adequate best practices in close cooperation with SIG-ISM, WISE, EOSC-future etc.

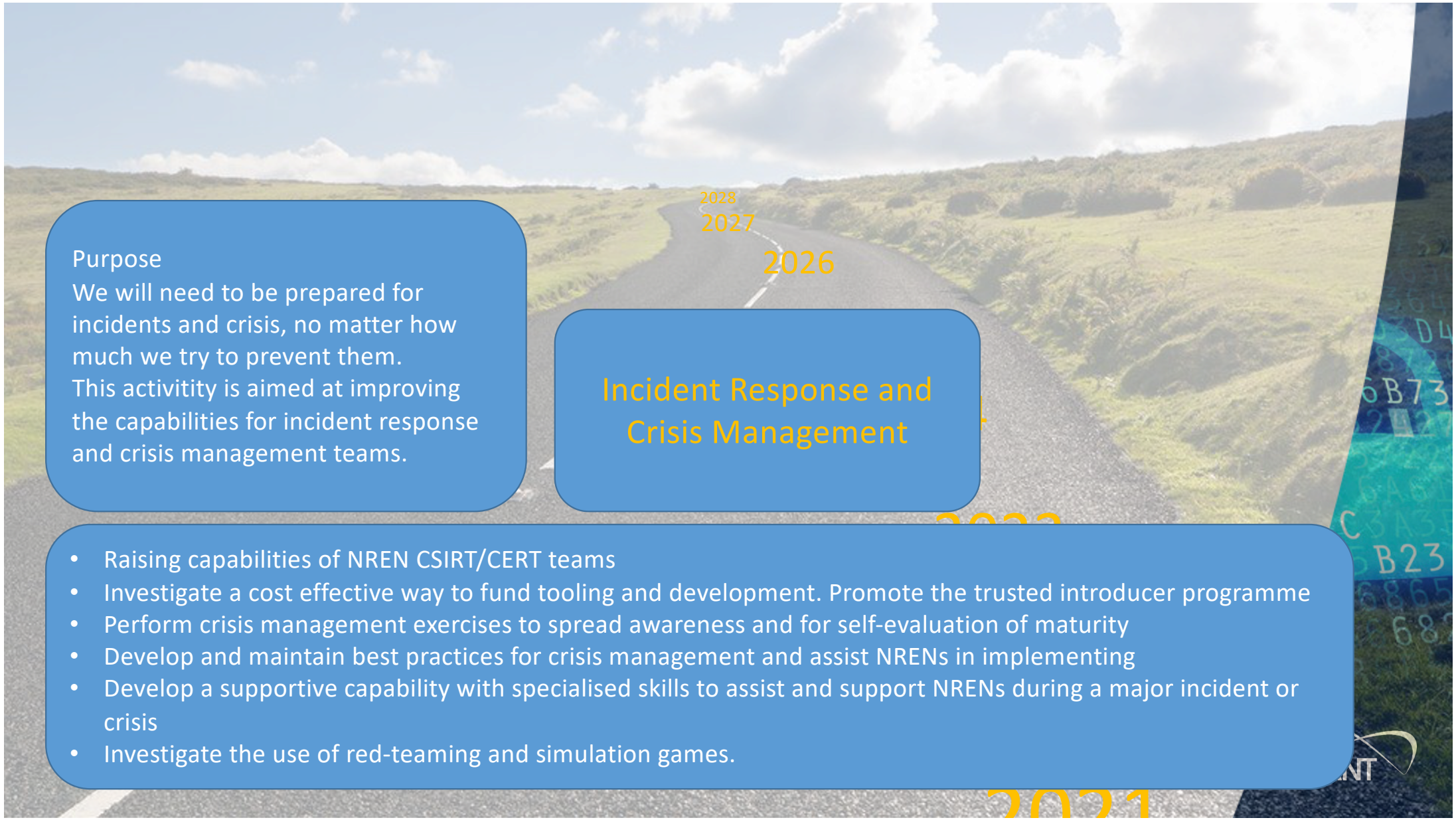
Security Operations Support

- Intelligence sharing and threat analysis
- DDOS protection
- eduVPN
- Vulnerability management services
- Cryptographic services: Certificates and document signing
- Community support

Purpose

Deliver dedicated and focused security services and support security operations centers (SOC), negotiate the use and re-use of security services. This subject area covers the operational side of security. Operational services that are needed to keep networks safe such DDOS detection, vulnerability scanning and certificate services.


2028
2027
2026
Services and Tools
Purpose
• the (continuing) development of security tools and services. That are needed for supporting NRENs and their users
• Support the development of open source tooling such as eduVPN
• Cryptographic services: automation, ACME, TCS service suite
• Pilots and POCs with sensor networks
• Tooling for supporting security operations
• Security intelligence: drivers, plugins etc.
• DDOS detection and mitigation, Firewall on Demand
2021
GÉANT



Purpose
We will need to be prepared for incidents and crisis, no matter how much we try to prevent them.
This activitity is aimed at improving the capabilities for incident response and crisis management teams.

Incident Response and Crisis Management

- Raising capabilities of NREN CSIRT/CERT teams
- Investigate a cost effective way to fund tooling and development. Promote the trusted introducer programme
- Perform crisis management exercises to spread awareness and for self-evaluation of maturity
- Develop and maintain best practices for crisis management and assist NRENs in implementing
- Develop a supportive capability with specialised skills to assist and support NRENs during a major incident or crisis
- Investigate the use of red-teaming and simulation games.

- Support training at both introductory and advanced levels suitable for a wide range of audiences
- Identify suitable training opportunities for security awareness, basic training, specialised training and related educational development needs for NREN staff and security teams, some will be “make”, others will be “buy”.
- Survey the training requirements of security teams and identify gaps/areas of improvement, develop trainings for or buy them
- Organise a annual security awareness cybersecurity month
- Investigate for a mentor/mentee programs to help develop and retain members of the local security teams. Support training-on-the-job and mutual traineeships or exchanges.
- Develop and maintain training material matched to the needs of the NREN security community.

Development of human capital, training and Awareness

Purpose

Training, awareness raising and exchange of expertise are amongst the key tools we can use to secure a security workforce for now and the near future.
Training and awareness are an essential part in the prevention of incidents.

- Analyse the needs for specialized tooling based on threats and risks
- Develop and maintain best practices for securing high speed networks
- Develop or acquire and optimize tooling for securing high speed networks

Purpose

High speed networks require high speed security. Some of the existing security tools are independent of transmission speed, but some other faces of high speed networking may require specific protection specially suited for high speed, high volume networks.

Securing
High Speed Networks

GN5-1 WP8: Security (proposed): Overview of activity – ongoing and new

A1: Best Practices, security baseline

A2: Incident Respons and crisis management

A3: Securing High Speed networks

A4: Security and privacy coordination across workpackages

B1: Delivery of Services and tools:

- DDOS detection & mitigation: NeMo + FoD
- Support for eduVPN
- Tools for security operations
- Cryptographic services
- Broker (NREN) security services
- Cyberthreat Analysis and Cyber Threat Intelligence

B2: Security Incubator

C: Security Training and Awareness

- Cybersecurity Month, Regular awareness updates
- Security training: Expert, basic and al-round
- Career development/ mentoring: identify talents, stimulate and support cross training

GN5-1 TIMELINE

September – November determine GN5-1 WP and Task structure

November structure is available for the GA

November GA approval of the structure

January 2022 Strawman DoW available to NRENs

January – February 2022 Consensus building

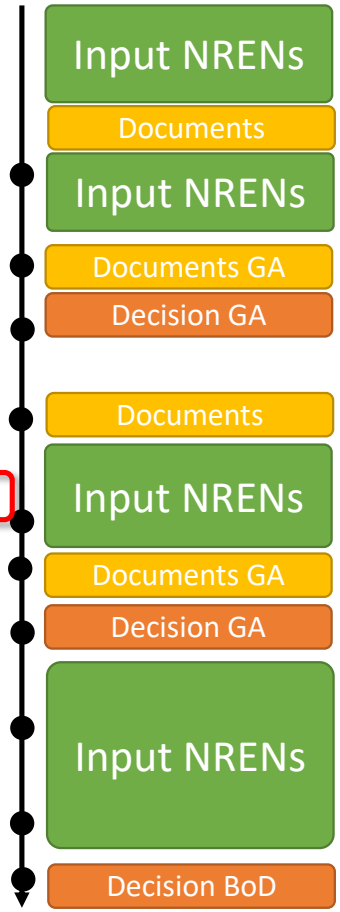
March 2022 Tinman available to the GA

March GA 2022 Approve Tinman and budget allocations per WPs

March – April 2022 Adaptation of proposal to the call, recruitment of roles

April 2022 Allocation of budget to partners

May – June 2022 Approval by the board



April – July Information gathering

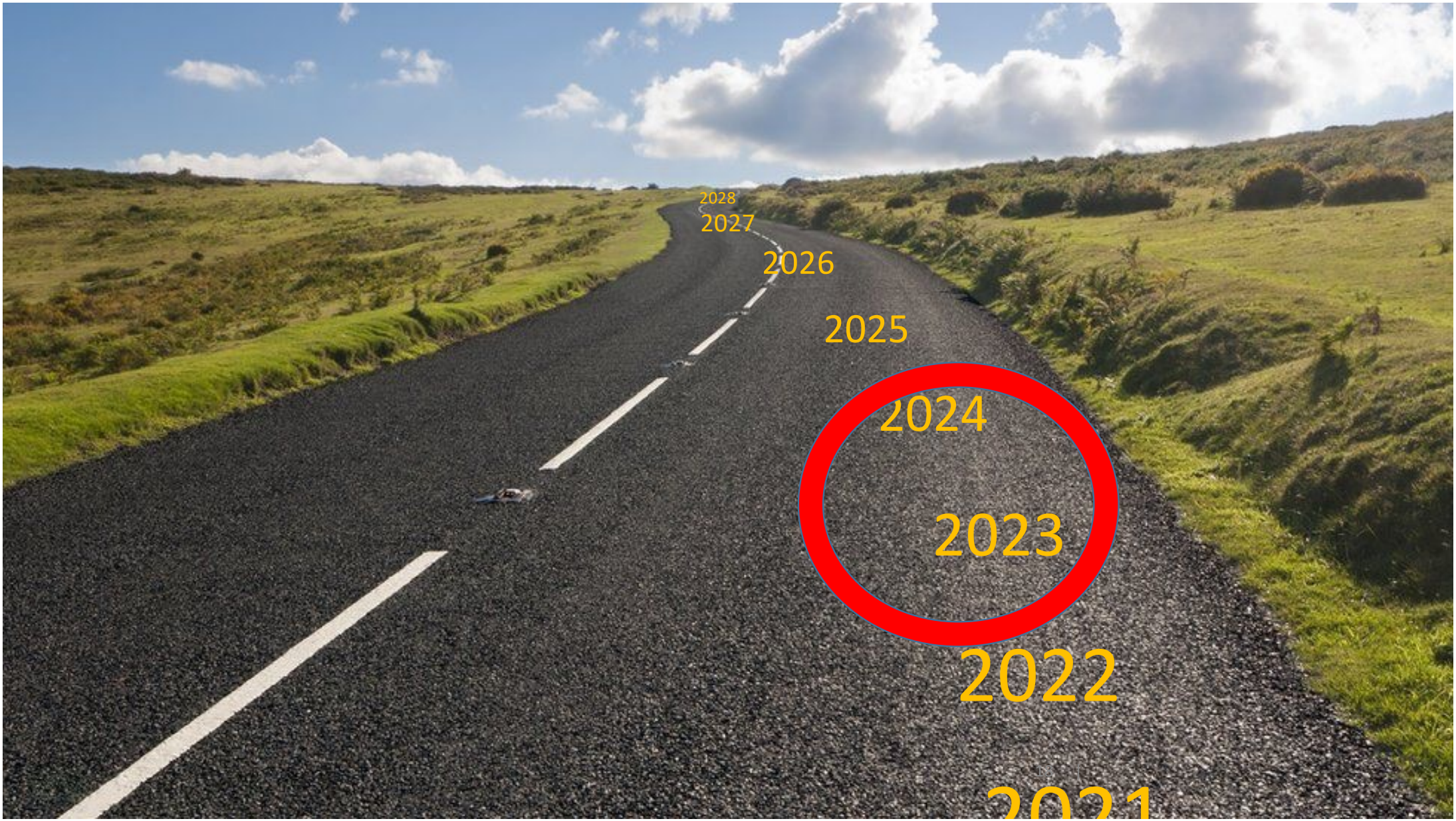
August 1st versions of thematic roadmaps available to the community

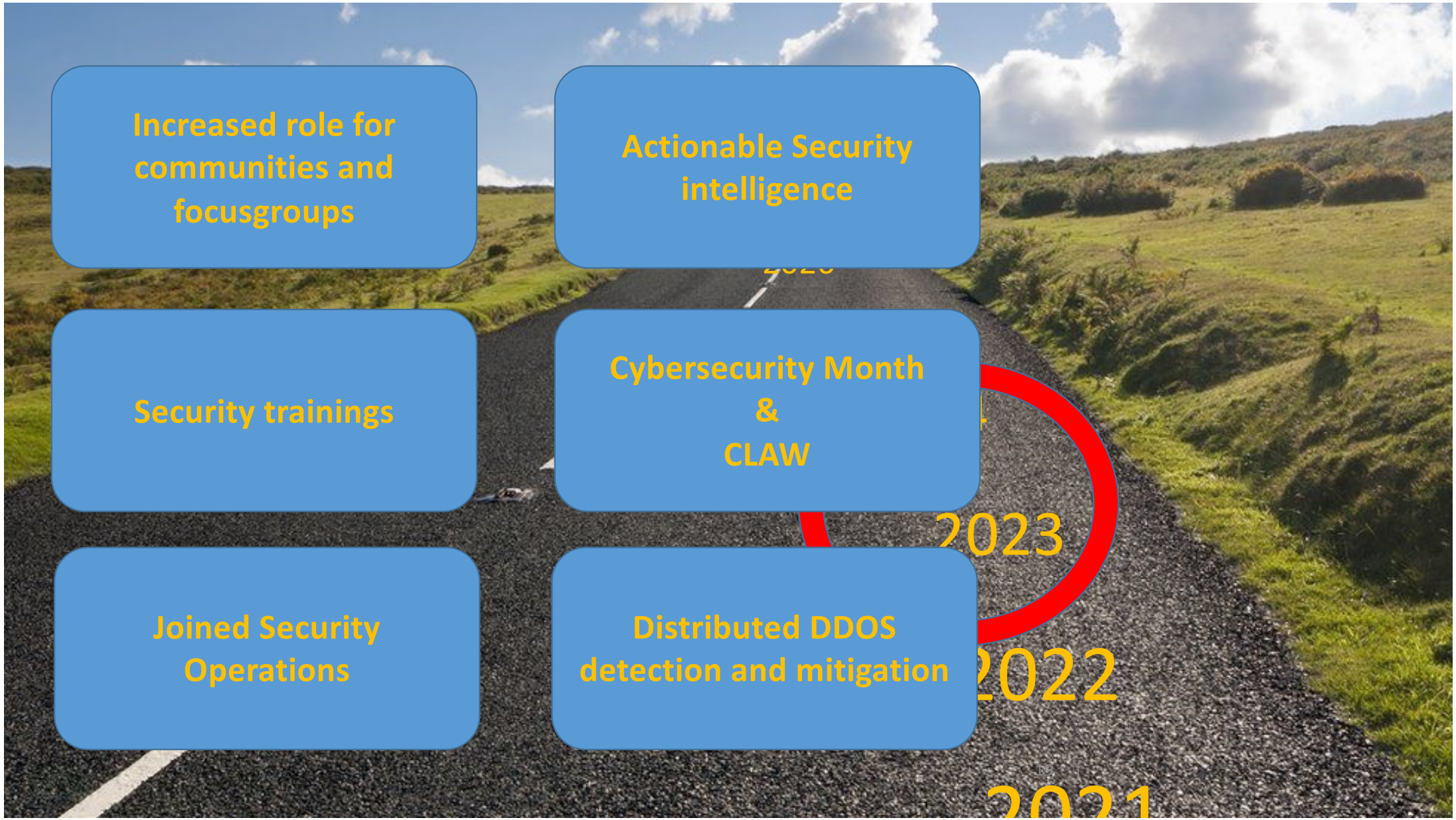
August – October Consensus building

November –thematic roadmaps available to the GA

November GA – presentation and comments from NRENs

April 2022 – review of thematic roadmaps


2028
2027
2026
2025
2024
2023
2022
2021


Increased role for communities and focusgroups
Actionable Security intelligence
Security trainings
Cybersecurity Month & CLAW
Joined Security Operations
Distributed DDOS detection and mitigation
2023
2022
2021

GÉANT
Networks • Services • People

Thank you for your attention

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)