Working Group Charter
v1.0.2 – 19 December 2024

Full Name of Group:

Global R&E Network Resilience & Vulnerability Risk Review WG

Short Name of Group:

GREN Resilience WG

Charter Authors:
David Wilde (AARNet), Harold Teunissen (SURF), Erik-Jan Bos (NORDUnet)

Background:
Since the first R&E Networks were created, the design principles behind our network architecture and services have evolved.

- Connectivity: Initially, the R&E Network fulfilled a role in a not yet existing market: simply delivering network connectivity to research and education for the first time.
- Performance: through the 1990s and into the early 2000s, as our members and customers became accustomed to their basic connectivity, the goal evolved to focus on performance – delivering the ultra-high-speed, low latency connectivity that enables the data-rich needs of research. In particular, the value proposition of R&E Network connectivity was that it is *better* than the commercial internet.
- Reliability: As we moved from the 2000s into the 2010s and network connectivity become increasingly vital to the operation of our connected institutions, the design goal of the network became focused on resilience; ensuring uptime through redundancy and other mechanisms. This was accentuated by the move to the cloud for many applications.
- Security: Finally, as we moved through the 2010s and into the 2020s, ensuring that our networks, platforms and services are secure from attack or compromise has become more critical than ever before. The boards and councils of our member institutions have become keenly aware of the risk and their responsibility to address this. This heightened awareness has been sharpened by the many public breaches and attacks, coming from both cyber-criminal activity and nation state actors.

Each design principle came with a set of assumptions and constraints – many of which have evolved over time. For instance, the bandwidth associated with 'performance' has moved progressively from 64 kbit/s (in the early 90s) to 400 Gbit/s and beyond today.

One of the assumptions in designing for reliability has generally been that outages are random and/or accidental. For instance, a ship dragging an anchor which breaks a subsea cable; a farmer with a backhoe digging up a buried fibre cable; a car accident bringing down an overhead cable; volcanic activity destroying a subsea cable; a disgruntled employee setting a university building with networking equipment on fire.

More recently, the goals of security and reliability have intersected, as we have begun to see examples of sabotage or other malicious attacks on physical infrastructure. These attacks may be with the intention of causing simple disruption of service, or potentially more complex motives such as disguising the insertion of network taps.

> *A good read on this topic is the British Government paper from 2017:*
> *https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/*
>
> *Examples of recent sabotages can be found here:*
> - *'Human activity' behind Svalbard cable disruption: https://thebarentsobserver.com/en/security/2022/02/unknown-human-activity-behind-svalbard-cable-disruption*
> - *Nord Stream gas 'sabotage': who's being blamed and why?: https://www.reuters.com/world/europe/qa-nord-stream-gas-sabotage-whos-being-blamed-why-2022-09-30/*
> - *Three Red Sea data cables cut as Houthis launch more attacks in the vital waterway: https://apnews.com/article/red-sea-undersea-cables-yemen-houthi-rebels-attacks-b53051f61a41bd6b357860bbf0b0860a*

These purposeful attacks bring into question whether the level of resilience designed into the GREN is sufficient to achieve the desired uptime. For instance, if three redundant links are required to meet an uptime target when protecting against accidental outages, then four links plus additional security & monitoring may be required to protect against the increased danger of malicious outages. But even less severe, recent submarine cable incidents around Africa have taught us that having your link redundantly implemented by using multiple cables can lead to unexpected loss of connectivity, as the dragging of a ship's anchor on the seafloor can damage multiple cables at once.

Several actions are required to understand these risks and identify potential actions. The first step is to understand the current state of the GREN: what resilience, redundancy, and security is in place? Where is the GREN potentially vulnerable?

From there, we can start to look forward: what design assumptions need to change? What goals do we need to work towards in terms of uptime, security, etc? Do we need to procure and deploy additional international links or move links to other submarine cables? If there is a serious outage, how do we act collectively to ensure maximum business continuity and minimal impact?

Scope for the Group:
For the purposes of this activity, we're focusing primarily on the interconnections between R&E Networks, rather than intra-R&E Network connectivity out to their member institutions. Global R&E Exchange Points (GXPs) and the links between them are explicitly in-scope for this activity. Some intra-R&E Network paths may be considered, in the case where an R&E Network is providing transit across their network as part of the GREN.

Goal of the Group:
The aim of this GNA-G Working Group is to perform a high-level risk review of the GREN, to identify the resilience to accidental and malicious incidents, more specifically:

- This review should consider both links and exchange points (GXPs).

- It should document the failover/rerouting capabilities which are currently configured, indicating what links or services are protected and how. For instance, a point-to-point service carried by one link may failover to a backup path, but other point-to-point services may not.

- The consequences of failover/rerouting, such as lower available capacity or increased latency should be documented as much as possible.

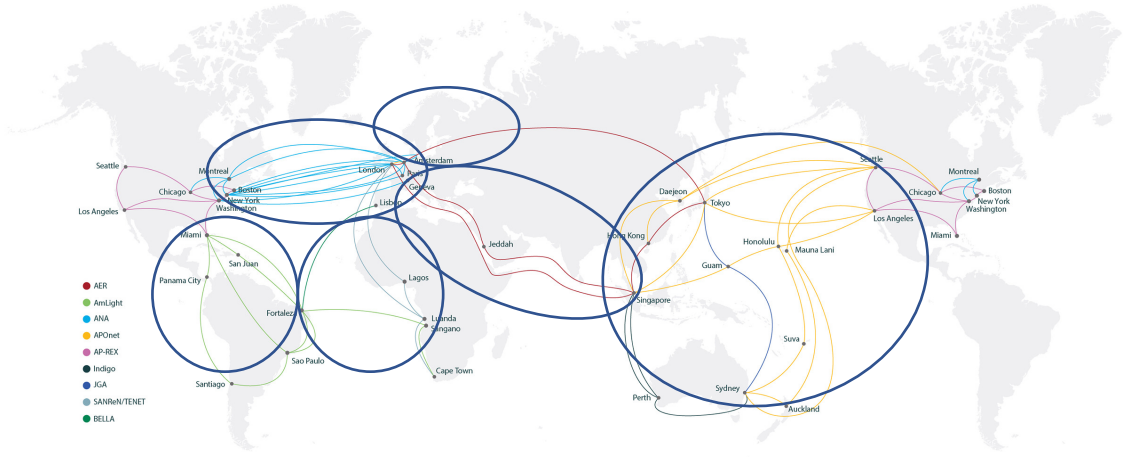
- Limitations due to an AUP or other constraints should be noted.

- If possible, if a link is carried on a fibre path which is collocated with a power/gas/pipelines/etc, this should be noted since it may increase its attractiveness as a target. Other sensitivities may be noted also, e.g. geopolitical issues related to the location or owner of a link.

The proposed approach is to examine the GREN by region first. In this part of the activity, we will rely as much as possible on the ongoing work and knowledge of the already existing groups, not duplicating efforts.

Proposed regions:
- North Atlantic – interconnecting Europe and North America
- South Atlantic – interconnecting South America, Western Africa, and Europe
- Pacific – interconnecting Asia Pacific & Oceania, Asia, and North America
- Europe/Africa – interconnecting Europe and Africa
- Indian – interconnecting Asia, Eastern Africa, Arab States, and Europe
- The Americas – interconnecting North and South America

Per region, we plan to use as much as possible of the knowledge and experience of the people involved in the GREN Systems, i.e. ANA, APOnet, AER, BELLA, AmLight, etc..



Planned links that are scheduled to be delivered any time soon and are deemed to play a role in the GREN will be considered in this activity.

These regions will then be brought together for a global view, which should also include any terrestrial cross-R&E Network transit (e.g. between non-neighbouring regions above) which may introduce or reduce vulnerability.

The review should include some initial recommendations:

- Updates to architectural design principles in terms of possible uptime service level targets, and the recommended resilience to achieve this in terms of number of paths and exchange points.
- Identify any new links or exchange points which may be needed to achieve this, or regions requiring particular attention.
- Suggested mechanisms which would improve resilience (partnerships or MOUs; failover or other high availability configurations; monitoring of outages; encryption or other mechanisms to secure the network; scheduled failover testing; etc).

For the moment, this exercise is focused on reviewing the network architecture itself. The exercise of identifying governmental or legislative initiatives aimed at protecting network cables is considered out of scope, and should be investigated separately:

E.g. US discussions: https://www.lawfareblog.com/protecting-undersea-cable-system
Or the International Cable Protection Committee https://www.iscpc.org/

Deliverables:

The initial intended outcomes are:

1) An initial high-level kick-off document defining the problem space, outlining the identified key areas of focus, and the proposed process to complete the review.
2) A report delivered in four parts, with each part released as soon as it has been completed:
    a. A snapshot of the current GREN, identifying vulnerable points in areas such as but not limited to:

   i. submarine cables,
   ii. cable landing stations,
   iii. GXP (Global R&E Exchange Points), and
   iv. Commodity Internet connectivity.
b. Recommended updates to architectural design principles in terms of possible uptime service level targets, and the recommended redundancy required to achieve this in terms of number of paths and exchange points.
c. Specific network-focused recommendations (e.g. new links or exchange points) to address vulnerable points in the GREN
d. Any other recommendations to address vulnerabilities – e.g. partnerships or MOUs; failover or other high availability configurations; monitoring of outages; encryption or other mechanisms to secure the network; scheduled failover testing; etc

This four-part format is intended to enable initial results to be shared more rapidly to the GNA-G community and the Global R&E Network CEO Forum for discussion and comment. Furthermore, we expect that residual risks will be identified towards the end of this work as we cannot fix all issues, e.g. as there is missing infrastructure due to lack of investment opportunities or funds. That said, it is paramount to be aware of these residual risks and these can form an excellent opportunity for mitigation during future investments.

Additional possible future deliverable – to be decided on later:

- *Turn this one-off survey into a regular survey/audit process, to be updated as new links and exchange points are brought online, and with changes to the geopolitical environment as required.*

Confidentiality:

During the work of the GREN Resilience Working Group, we will be assessing our networks, vulnerabilities, and resilience. This is information we should and will not share openly. Therefore, the work of this WG will be under TLP:AMBER: "Limited disclosure, restricted to participants' organization and its clients"[1].

Timeline:

- October 2024 – Present at the GNA-G Community VCs
- November 2024 – Form Working Group; appoint co-chairs; begin work
- January 2025 – complete deliverable 1a (initial scoping document and project plan); present to CEO Forum VC (to be planned)
- January 2025 – complete deliverable 2a (snapshot of current risks)
- April 2025 – complete deliverable 2b (recommended updates to architectural principles) and 2c (specific network recommendations)
- May 2025 – complete deliverable 2d (any other recommendations)

[1] For more information, please refer to:

- https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage
- https://www.first.org/tlp/

- June 2025 – Present finished deliverables at CEO Forum F2F meeting in Beijing, China, for comments and guidance

Collaboration & communication methods:
The WG will convene regularly as it sees fit by Zoom.

Shared document folder on Box.com:
'GREN Resilience WG' (all WG Members are Editor)

Mailing list:
<gren-resilience-wg@lists.gna-g.net>

GNA-G Leadership Team Liaison(s):
- David Wilde (AARNet)

Co-Chairs (alphabetically by R&E Network):
- Steve Maddocks (AARNet)
- Harold Teunissen (SURF)
- Erik-Jan Bos (NORDUnet)

Initial members (alphabetically by R&E Network):
- Michal Krsek (CESNET)
- Alex Moura (KAUST)
- Kirotaka Sato (KDDI)
- Ivana Golub (PSNC/GÉANT)