The Global R&E Network (GREN) as Critical Infrastructure: A Strategic Framework

GREN Resilience WG – Final Report

Date: 18 May 2026
Authors: WG Members (see Appendix D)
Editors: Steve Maddocks (AARNet), Harold Teunissen (SURF), Erik-Jan Bos (NORDUnet)
Reviewer: Sabine Jaume (NORDUnet)
Version: Final

Executive Summary

Design principles for Research and Education (R&E) networks have evolved from connectivity (1990s) to performance (2000s), to reliability (2010s), and now to security (2020s). Reliability and security goals have converged, as physical sabotage and malicious attacks increasingly threaten global infrastructure.

Simply adding more (intercontinental) capacity and cable systems to the Global Research & Education Network[1] (GREN) certainly improves resilience but with diminishing returns in cost and time unless supported by additional measures. Resilience must be addressed through a balanced portfolio of actions:

- Define minimum service levels for long disruptions and pre-agree traffic prioritisation (a triage model).
- Prioritise critical workflows and users during crises, guided by a decision framework agreed in advance.
- Invest in the human network (relationships, contact paths, and joint exercises).
- Coordinate investment across systems, i.e. on a global scale, to maximise return.
- Expand the geographic footprint and diversity of Global R&E Exchange Points (GXPs), particularly in the Southern Hemisphere, and pursue longitudinal diversity (north–south as well as east–west).

GXPs are central to the GREN's resilience. Breaking very long transmission paths at intermediate GXPs creates additional switching points and ensures that an outage affects only a segment, not the entire (long) path. This is especially relevant in the Southern Hemisphere where GXPs are sparse today.

There are several initiatives for new submarine cables with deep involvement of R&E Networks. Appendices A and B describe two prominent examples. Appendix C holds a detailed level of potential additional resilience measures. Appendix D lists the name of the contributors to the GREN Resilience WG to date. Appendix E explains the abbreviations used in this document.

This report ends with the recommendation to the GNA-G Leadership Team to establish a standing group, reporting to the GNA-G Leadership Team, with a mandate to guard and increase GREN resilience and to publish an annual "GREN Resilience Report" covering: (1) the state of the GREN (with year-on-year changes) and (2) recommended actions.

[1] More information at e.g.:
https://www.canarie.ca/nren/gren/
https://nordu.net/gren/

1. Introduction

The Global Research and Education Network (GREN) is a loosely coupled, bottom-up federation of links, hardware, people, processes, and cultures; the people that run the GREN are as critical to resilience as the underlying links and equipment. The GREN Resilience WG's scope is limited to exactly this, as this was already sufficiently hard. At the same time, the Members of the WG acknowledge that there are many circumstances beyond the control of the people that run the GREN, including but not limited to middleware issues (such as DNS and NTP) and upper layer issues (such as recently witnessed with Cloudflare, CrowdStrike, Amazon, Microsoft, and others).

The Global R&E Network (GREN) is the collection of GREN Systems (for example, APOnet and AER) and certain inter- and intra-continental R&E links that together provide global transit for research and education. Each GREN System aggregates links procured and operated by individual R&E networks or their collaborations.

Most of the GREN rides on the world's ~450+ active submarine cable systems. Submarine cable cuts (roughly 150–200 per year) are common—mostly due to fishing and anchoring. Heightened geopolitical risks prompted the creation of the GREN Resilience Working Group (WG) under the Global R&E Network Advancement Group (GNA-G) Leadership Team. The WG charter (scope, goals, deliverables, timeline) is available at: https://www.gna-g.net/wp-content/uploads/2025/01/GREN-Resilience-WG-Charter-v1.0.2.pdf

This report focuses on the resilience of intercontinental R&E interconnections, with GXPs and the links between them explicitly in scope. Given the sensitivity of the topic, the work leading up to this report was handled under TLP:AMBER[2]. The Co-chairs thank all contributing R&E networks and participants (see Appendix D).

Figure 1 shows a (somewhat dated) artist's impression of the GREN and its Systems.

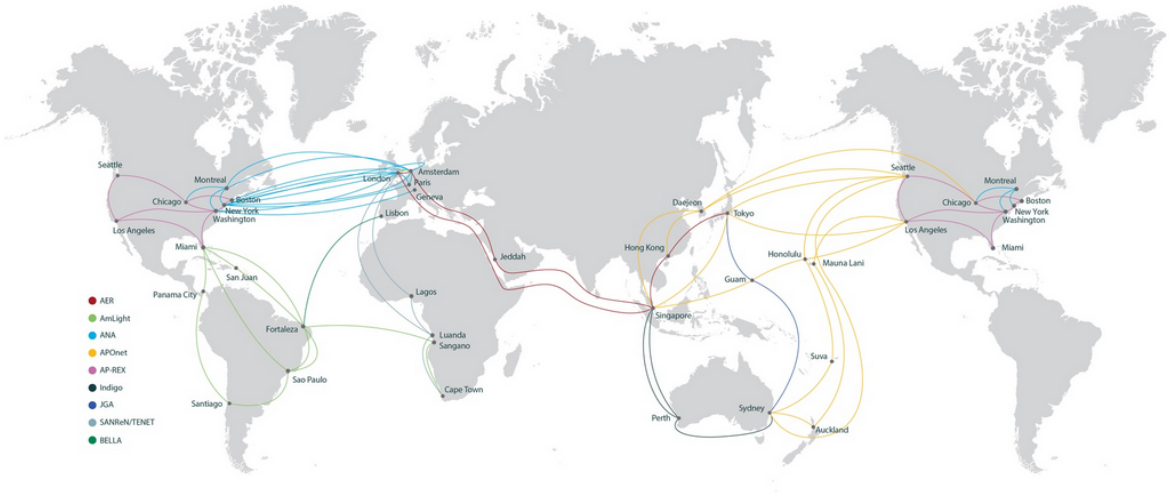

Figure 1. Artist's impression of then GREN and its Systems (source: GNA-G Website)

Resilience depends on people. Lower barriers between teams and the running of regional crisis exercises to build cohesion and shared practice across GREN participants is an important activity that is often overlooked. Especially, in a worsening geopolitical climate, global collaborations can still and have to still succeed, but they need to be more intentional, resilient, and values-aware than before. In times of increasing geopolitical challenges, it is even more important to maintain person-to-person trust, even when state relations deteriorate. At the same time, of course, there is a need to remain compliant with laws, sanctions, and export controls. Furthermore, we need to be transparent with each other, as transparency

[2] More information on TLP:AMBER can be found at: https://www.first.org/tlp/

reduces suspicion, which is often the first casualty of geopolitics. Also, there is the need to be open about constraints, i.e. legal, political, and financial, and the need to share information about risks early instead of quietly working around them. Governance and decision-making must be made visible, of course taking the necessary security constraints into account. Finally, investing in trust continuously (not just at looming or actual crises) is of utmost importance. Trust comes both from regular communications and informal interactions at community events, while showing stability and reliability over time and respecting local contexts and constraints.

2. Approach

The WG met several times during 2025 by video conference to gather information on: (1) cable systems in use for the GREN, (2) services that constitute the GREN, and (3) the GXPs where regional and national R&E networks interconnect. Because the initial material was incomplete, a deep dive was conducted on the AER system to understand practical resilience; the findings are summarised in this report.

To broaden the perspective, the Co-chairs consulted R&E networks outside AER[3], APOnet[4], and ANA[5]. For example, the South African NREN system (SANReN and TENET) operates capacity on multiple systems (including WACS, SEACOM, Equiano) towards Europe and, jointly with FIU, on SACS (Brazil–Angola) for Africa–Americas connectivity. TENET is liaising with AER operations to exchange practices and insights.

The current geopolitical situation limits fully open global discussions of the resilience of the GREN; the WG sought to maintain an open and balanced approach throughout.

We distinguish three disruption types by scope:

Type	Disruption
1	A single cable or landing station is disrupted
2	A regional disruption to GREN infrastructure
3	A widespread, system-level disruption with global impact

Table 1. Types of disruption

Mitigations vary by type. For Type 1, existing redundancy often suffices. For Type 2, chokepoints such as the Red Sea area or some of the large GXPs do require special attention. Type 3 extends beyond the R&E domain and demands cross-sector coordination.

To note:

- A type 3 disruption could be the result of one major issue in a region or, more likely, an accumulation of multiple type 1 and type 2 disruptions, spread over time. As an example, a (hypothetical) GREN System consisting of three links may have one link down for planned maintenance work for three weeks, while a cable break on the second link occurs in the first half of this planned maintenance period and a power issue in one of the Cable Landing Stations of the third link happens in the second half. This would cause a type 3 event, at least for the GREN, that can last for days or a week in a row.
- A single disruption may be the result of planned maintenance work, have a natural course (an earthquake, a power issue, or a software or hardware fault), or be of malicious nature, e.g. by a state actor. In the current climate, coordinated state-level attacks are considered more plausible and potentially more severe than ever before since World War II.

[3] Asiapacific Europe Ring: https://aer-network.net/

[4] Asia Pacific Oceania Network: https://www.aponet.global/

[5] Advanced North Atlantic collaboration: https://www.anaeng.global/

Two framing questions guided the analysis:

1) What minimum service level must the R&E community maintain during major crises ("science as critical infrastructure")? Needs range from basic communications (e-mail) to movement of large datasets to available compute.
2) Given target service levels, how can the GREN deliver these with constrained resources? This includes ensuring that GREN operations staff can still communicate (e.g., satellite-phone backups if terrestrial and mobile networks are impaired).

3. Findings

3.1 Risks

GREN Systems are generally inherently resilient, but stylish topology maps often hide important commonalities and single points of failure. Common risks include:

- Different links sharing the same submarine cable system or waterway.
- Multiple systems terminating at the same cable landing station (CLS) or sharing the same backhaul trench to a GXP.
- Nearby CLSs aggregating in a single data-centre location.
- Multiple links converging on one GXP location.
- Operational knowledge concentrated among a small number of people.
- Lack of pre-agreed prioritisation of services for crisis operation.

As an example, on 27 June 2024, AER (Figure 2) experienced its 'worst day': Several links in the Red Sea were cut and some remaining AER links were unavailable due to faults or maintenance, highlighting chokepoint exposure and the value of diversity. This is shown in Figure 3.

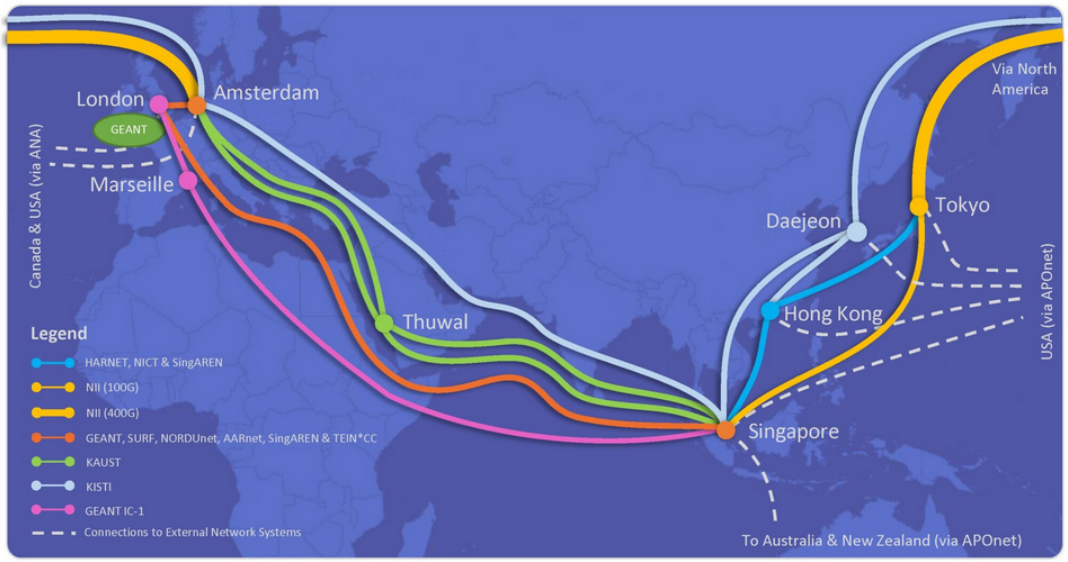

Figure 2. Artist's impressing of the AER topology map (version 23 April 2025)

Figure 3. Worst day in the current history of AER (image courtesy of Francis Lee (SingAREN))

Another example includes REANNZ coming to the rescue to the University of Hawaii, when multiple faults on submarine cables to mainland USA happened simultaneously.

3.2 Affordability

While bandwidth in some parts of the world is rather affordable, it is acknowledged that in other parts this is not the case. Or worse, the required bandwidth might not be available at all[6]. This hampers resiliency of the GREN system as a whole with impact far beyond the specific geography. For example, while the North Atlantic Ocean has been a rather competitive area, other areas, in particular in the Southern Hemisphere are significantly less so.

Coordination of investment and maximisation of the return on investments, for example via GXP breakouts, is ever more essential in areas where systems cost is high. Furthermore, a shared understanding that systems in all regions contribute to the stability of the GREN as a whole, and, in particular, the role that longer and less obvious routes have in maintaining system stability, is essential. This to ensure that investment is supported at a global level for areas where local capacity (for investment) is lacking.

As part of the process to maximise return, stimulating R&E Networks creation in developing countries is important as they can contribute to GREN capacity.

3.3 Dispelling myths

The WG members find it important to dispel a number of myths that hamper the thinking around GREN Resilience, including:

- “Somebody else will fix this”,
- “Submarine cables are repaired quicky”[7],

[6] Security of supply, i.e. is an R&E Network able to acquire bandwidth, is a steadily rising concern.

[7] Unlike terrestrial cables, submarine cable cuts/faults take much longer to repair, sometimes several weeks but often many months. This is due to a combination of reasons: Obtaining jurisdictional permits; the availability of marine maintenance vessels and crews; and the ship’s steaming time to collect spare parts and then sail to the repair site itself. Due to a widely recognised shortage of marine maintenance operators, a cable fault might join a queue of scheduled repairs. Even with a repair exercise underway, it is not uncommon for what appears to be a single cut/fault to turn into more than one damaged section of cable, especially if the cable has been severely stretched or ‘hit’ multiple times – all of which can add significant delay to the time to repair and restore services. Clearly, the longer it takes to

- "It has worked well for so long, so no need to worry about it", and
- "Satellites will come to the rescue when there is a major outage on submarine cable in a region".

Satellite based services remain orders of magnitude behind in term of both cost and capacity, compared to submarine cable systems, to carry large amounts of data between continents. Because of this, satellites do not offer an alternative to fiber when it comes to the support of R&E traffic. It is therefore important to have a clear view of what level of services is required by the R&E community in situations in which there is a disruption, weighing this against what services can be offered to the R&E community at sustainable costs, and whether satellite networks could play a role in this context, e.g. for human contact between R&E Networks' Network Operation Centres (NOCs). This is for further study.

It is important to note that required services for the R&E community may not be limited to pure networking (defined as the routing layer and below). It may be needed to ensure that other areas of the infrastructure, such as servers or software remains functional to ensure workflow and communication remain available. This discussion between services required and services affordable is part of a broader discussion about science as a critical infrastructure. The discussion on what is required as a minimal set of services needs to take place at national and international levels.

4. Conclusion and Recommendations

Per-system GREN resilience is strong thanks to sound engineering and routing implemented on these systems. However, significantly improving overall resilience by adding raw capacity alone would cost hundreds of millions of EUR/USD and deliver diminishing returns without complementary measures.

Priorities to further increase overall GREN Resilience:

- **Human resilience**: strengthen relationships and contact paths; broaden operational knowledge; run regional crisis exercises.
- **Route resilience in procurements**: consider existing topology (submarine systems and CLSs in use by the GREN today, backhaul, and GXP locations) to avoid common elements as much as possible; be prepared to trade a little extra round-trip time (RTT) for substantially more resilience; coordinate and explore collaboration ahead of new submarine investments.
- **GREN-level resilience**: formalise shared metadata and standardise tooling; establish a decision framework for traffic triage; expand longitudinal diversity by adding GREN systems with Africa and with South America; periodically align planning schedules across GREN Systems.
- **Learn**: Every time an outage occurs in one of the GREN Systems, small or big, be prepared to learn from the outage and share the lessons learned among the key people that run the GREN Systems.

The recommendation from the GREN Resilience WG, in this final report, to the GNA-G Leadership Team is to establish a standing group, with a mandate to guard and increase GREN resilience and to publish an annual "GREN Resilience Report" covering: (1) the state of the GREN (with year-on-year changes) and (2) recommended actions. Initial activities could include liaising with the Business Continuity (BC) group, defining traffic prioritisation schemes, conducting a shared inventory of R&E-owned resources and metadata in automatable formats (a potential collaboration with the GNA-G GREN Map WG), and analysing dependencies on external platforms (e.g., Zoom). Appendix C lists a number of more detailed measures that can be input to the establishment of such group.

repair a submarine cable, the greater the risk to the resilience of the overall GREN, as was explained at the start of the section 'Characterisation of disruption events'.

Appendix A. Case study Blue Raman – Oman – Perth

On 6 September 2025, several submarine cable systems in the Red Sea were cut or damaged—the second multi-cable incident after February–March 2024. Affected systems reportedly included SMW4 and IMEWE near Jeddah, Saudi Arabia, as well as FALCON GCX and EIG. None of these carried R&E traffic at the time, unlike the 2024 incident when three R&E cables were cut. The Red Sea remains a chokepoint of concern.

Cables must traverse narrow and geopolitically sensitive waterways (e.g., Bab el-Mandeb and the Strait of Malacca). Many Europe–Asia/Australasia routes pass through these areas, raising risk concentration.

GÉANT has procured capacity on the newer Blue-Raman systems (developed by Google with Sparkle and regional partners). While Blue-Raman does not entirely avoid the Red Sea, it does avoid major chokepoints such as Egypt, offering a more resilient alternative path.

Blue-Raman lands in Oman, which also hosts the Oman–Australia Cable (OAC) connecting diagonally across the Indian Ocean to Perth. OAC avoids Indonesia/Singapore and the southern approaches to the Red Sea. AARNet and GÉANT are exploring a collaboration to create a diverse Perth–London path using OAC and Blue-Raman—potentially valuable for future SKA traffic between Western Australia and Europe. Figure 4 shows both in a schematic diagram.

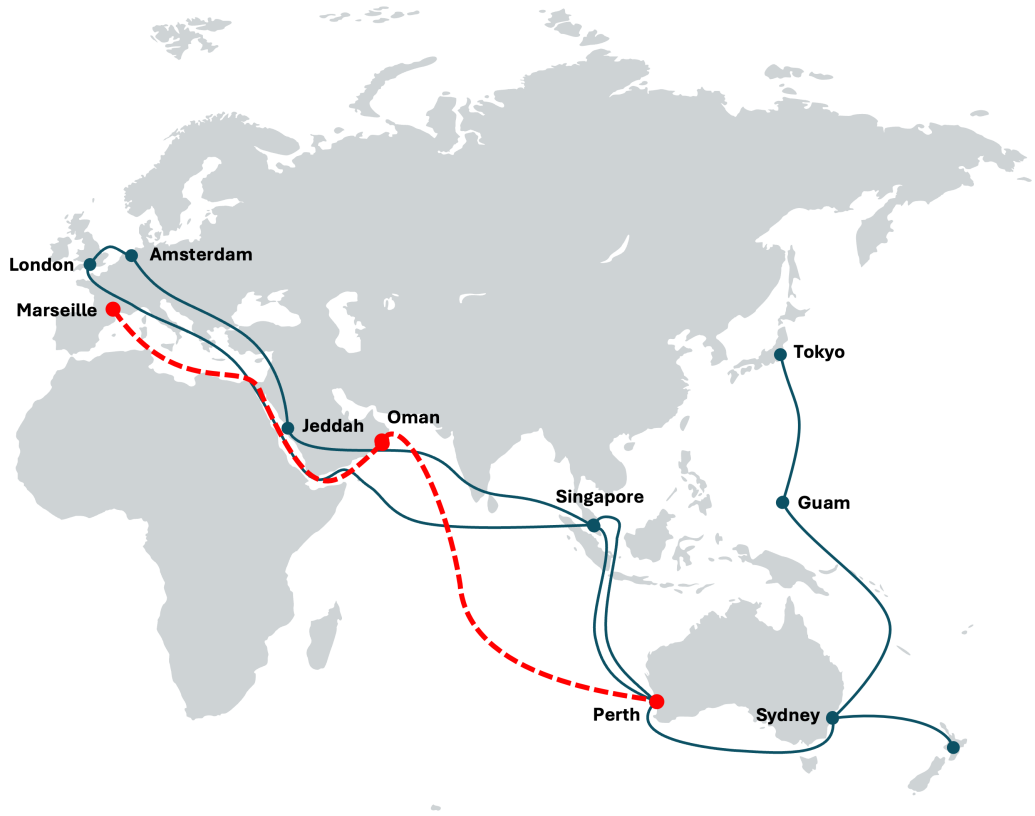

Figure 4. Blue-Raman/OAC (Marseilles-Perth) schematic overview

Appendix B. Case study Polar Connect

Polar Connect is an initiative to build a submarine system between Northern Europe and East Asia via the Central Arctic Ocean, near the geographic North Pole (see Figure 5). The goal is a shortest-path Europe–Japan corridor, with potential landings in Canada, South Korea, and the USA. As the first system on this route, Polar Connect could catalyse further Arctic connectivity and significantly improve global Internet resilience.

The initiative is led by the Nordic NRENs, i.e. the publicly owned entities the Swedish Research Council (VR), NORDUnet, Sunet (Sweden), CSC (Finland), Sikt (Norway), DeiC (Denmark), RHnet (Iceland), and the Swedish Polar Research Secretariat, with support from the EU's CEF Digital Programme. Funding supports design, planning, de-risking, and feasibility studies toward a resilient, future-proof digital corridor.

Because the Central Arctic Ocean is largely unexplored, any previous desktop study work is limited. Surveys in the Central Arctic Ocean with Swedish icebreaker Oden (in collaboration with a Canadian partner) have been executed in the summer of 2025 and additional survey have been planned in the summers of 2026 and 2027 to investigate priority areas for the potential cable route. A full desktop study is expected in 2028, followed by a marine survey in 2029. The Ready-for-Service target for the Polar Connect submarine cable system is in 2031 or soon thereafter.

Figure 5 Artist's impression of the future Polar Connect submarine cable system

Appendix C. Detailed areas of interest for increasing GREN Resilience

Areas of interest for increasing the resilience of the GREN include:

- Technical resilience, i.e.:
  - Using more diversity in the use of submarine cable systems,
  - Using multiple locations for one GXP,
  - Adding one or more GXPs in a region, e.g. Perth,
  - Exploring and using the potential of interconnections (trunks) between GXPs, and
  - Using new submarine cable routes, even if the latency is a little larger.
- Human resilience, i.e.:
  - Ensure senior operations people involved in a GREN System know each other's various contact details (this area of interest warrants A) an analysis of what communication methods are likely to be available during an outage and B) making sure operations people have access to these methods, e.g. satellite phone backups in case fixed or mobile networks are affected by the outages as well),
  - Ensure more R&E Networks people (operations and architects) know about the GREN System's details, and
  - Ensure that GREN Resilience has oversight.
- Service resilience, i.e.:
  - Ensure technical measures are taken that the crucial network services, such as BGP and NTP, continue to run on the GREN, in case of a major disaster, and
  - Pro-actively decide on and have the playbook ready for the service delivery portfolio of the GREN, i.e. what services do we want to continue in case of a major disaster.

Appendix D. Contributors

Contributors to the WG:

- Osamu Akashi (NII/SINET)
- Albert Astudillo (REUNA)
- Arno Bakker (SURF)
- Rodrigo Bongers (RNP)
- Sebastiano Buscaglione (GÉANT)
- Yukihiro Fujimoto (NII)
- Simon Peter Green (SingAREN)
- Ivana Golub (PSNC)
- Aluizio Hazin (RNP)
- Naoya Kitagawa (NII)
- Richard Klinger (CANARIE)
- Michal Krsek (CESNET)
- Francis Lee (SingAREN)
- Ajay Makan (SANReN)
- Kodai Motohashi (KDDI)
- Alex Moura (KAUST)
- Edward Moynihan (Indiana University)
- Hirotaka Sato (KDDI)
- Keith Slater (GÉANT)
- David Wilde (AARNet)
- Chris Wilkinson (Internet2)

Co-chairs of the WG:

- Steve Maddocks (AARNet)
- Harold Teunissen (SURF)
- Erik-Jan Bos (NORDUnet)

Appendix E. Abbreviations

AER	Asiapacific Europe Ring
ANA	Advanced North Atlantic collaboration
APOnet	Asia Pacific Oceania Network
BGP	Border Gateway Protocol
CLS	Cable Landing Station
CEF	Connecting Europe Facility
DNS	Domain Name System
EIG	Europe India Gateway
EU	European Union
FIU	Florida International University
GNA-G	Global R&E Network Advancement Group
GREN	Global R&E Network
GXP	Global R&E Exchange Point
IMEWE	India-Middle East-Western Europe
NOC	Network Operations Centre
NREN	National Research and Education Network
NTP	Network Time Protocol
OAC	Oman-Australia Cable
RTT	Round-Trip Time
R&E	Research & Education
SACS	South Atlantic Cable System
SKA	Square Kilometre Array
WACS	West Africa Cable System
WG	Working Group

#####