Norwegian
Communications
Authority

Diversified Challenges Call for Diversified Responses

BEREC Stakeholder Workshop on Network Resilience

Johan Foldøy, Chief Engineer, Security Department, Nkom

A collection of incidents and challenges against networks and systems, during the latest years

A few words:

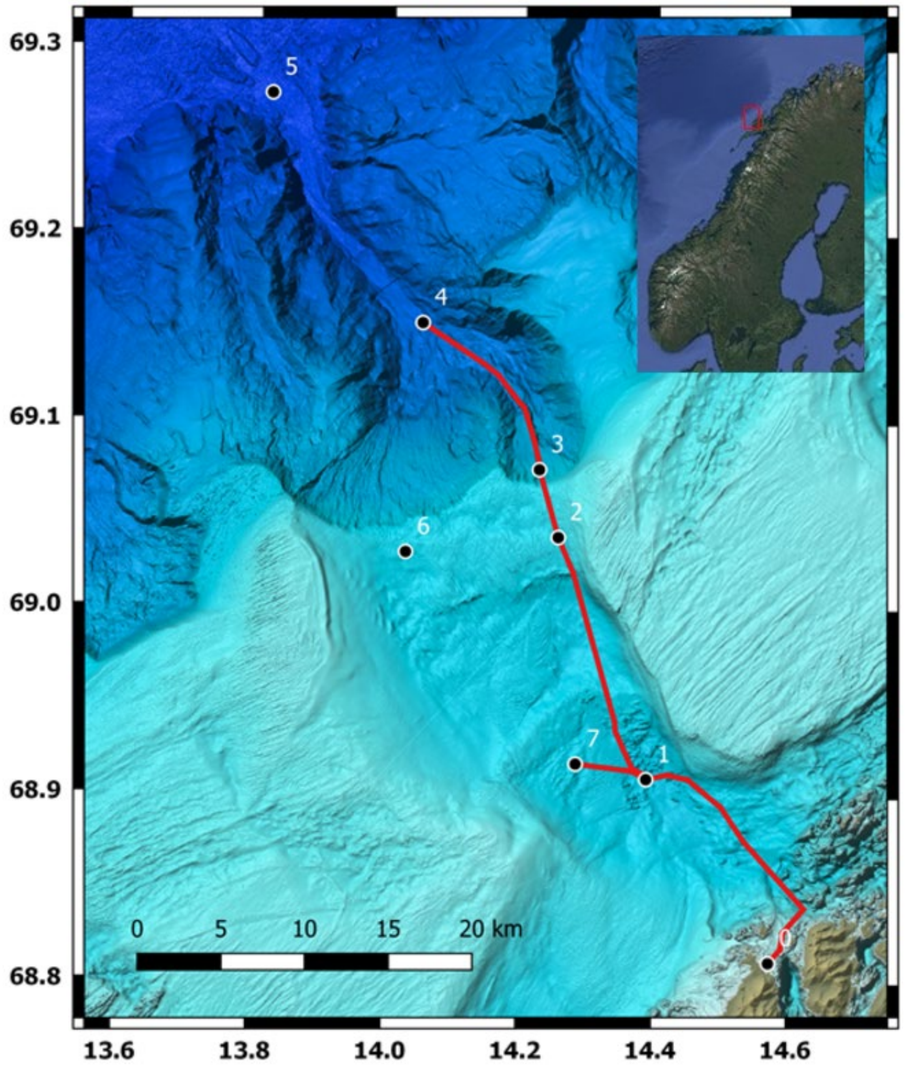
- all incidents are described to a certain level of detail, and can be found in public sources

- presentation focuses on infrastructure and systems that relate to electronic communication networks

- … but other infrastructure sees challenges as well

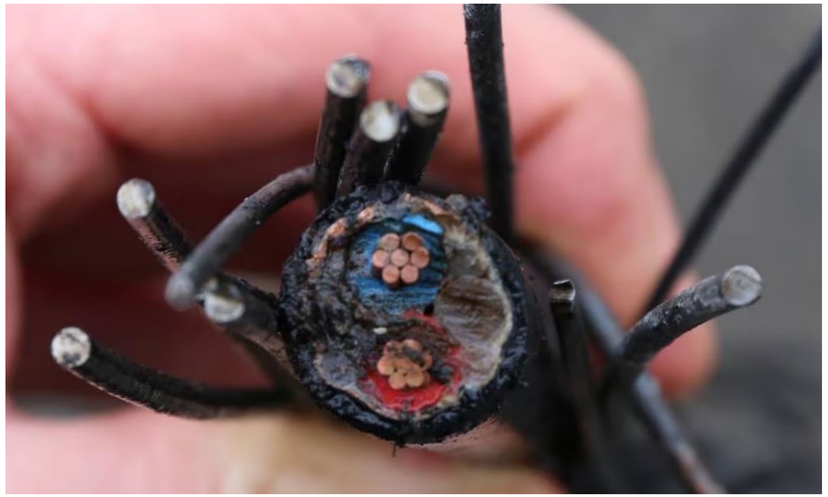
- cyber incidents are left out but there is “a lot” of it…

2021: Scientific cable outside Vesterålen goes off-line



April 2021: A submarine cable was cut off Vesterålen. 4.3 kilometers of the cable disappeared. It was later found, about 11 kms from its original location.

The cable connects nodes and sensors that monitor chemical conditions of the deep sea. It also measures maritime acoustic activity for the Institute of Marine Research (HI) and the Norwegian Defence Research Institute. A trawler was nearby when the incident occurred, according to media.



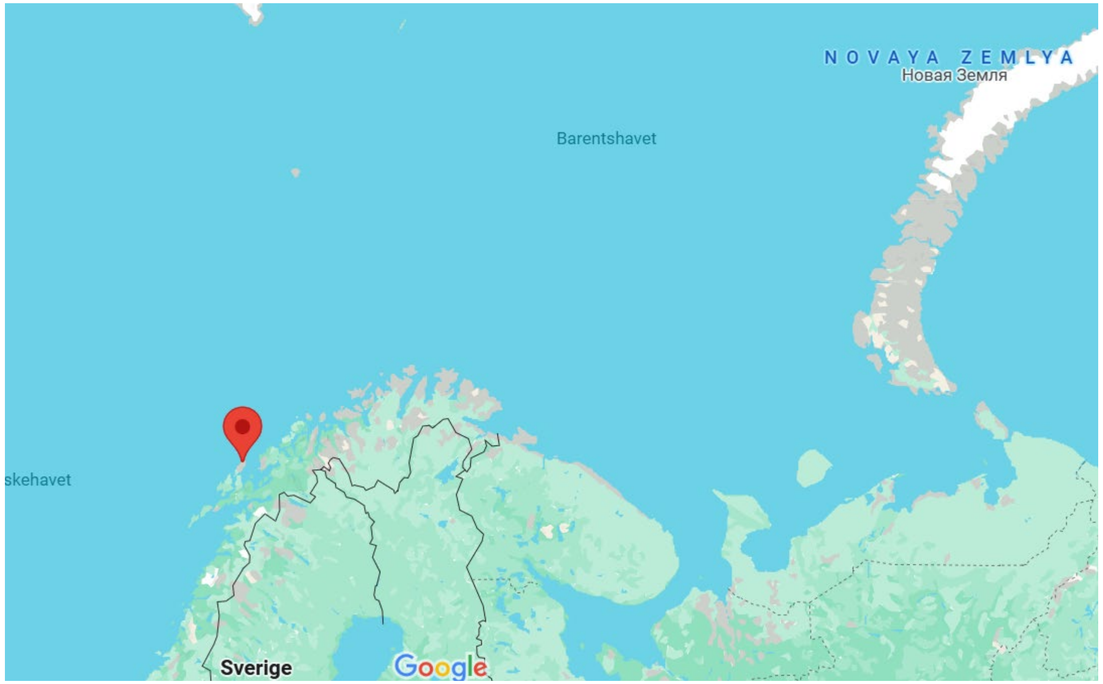
2022: An optical cable, connecting Svalbard to the mainland, fails.

The cable(s) carry vital communications to and from the mainland: internet, mobile networks traffic, as well as the traffic from more than 150 antennas located at Svalsat, the world's largest satellite ground station.

A trawler had, according to available AIS-data, crossed the area more than 20 times prior to the fault.

When located, the damaged cable showed sign of damage due to pressure/crushing.

2024: The world’s largest GNSS stress-test takes place at Bleik, Vesterålen area

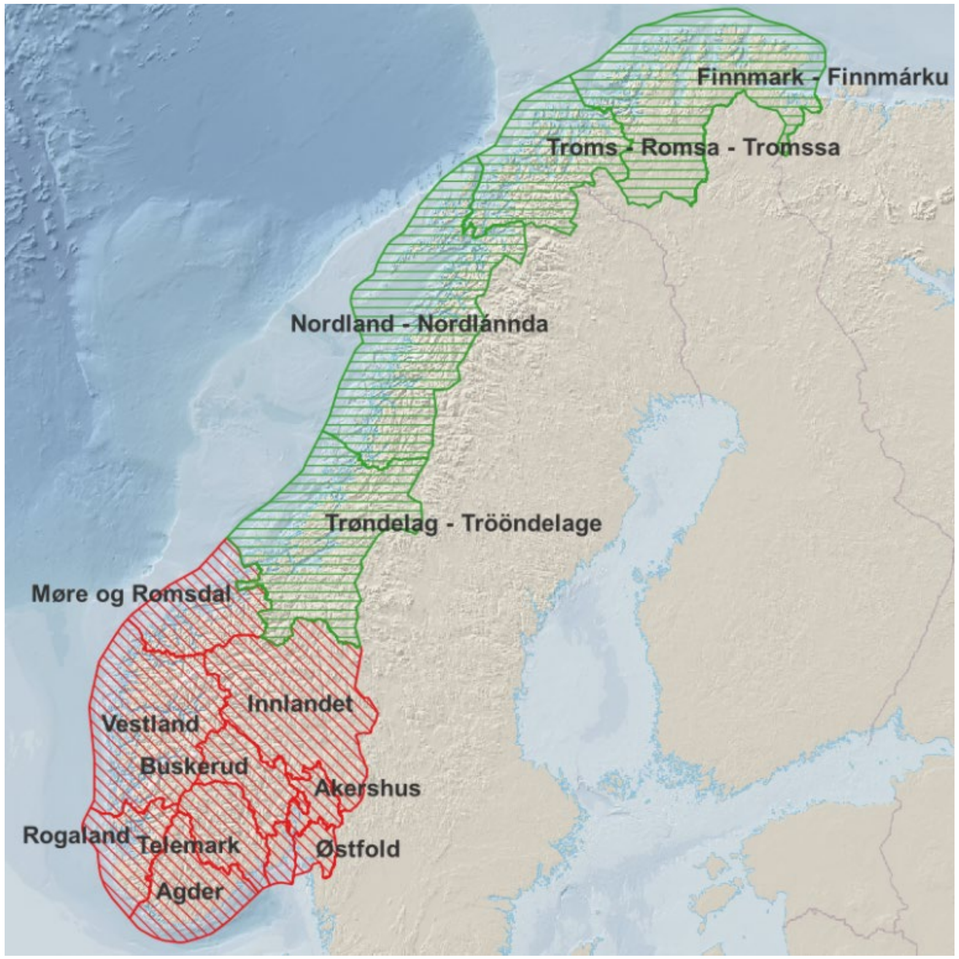


In September 2024, parties from all over the world met in Vesterålen to participate in a comprehensive jamming test.
During the test, organizations and companies will experience how their own timing and navigation systems react to so-called jamming.

Prior to the start of the exercise, a fiber cable connecting important equipment, was hampered.

The cable was not easily accessible.

Regional risk- and vulnerability analyses



- Both changes in the security policy situation and climate challenges emphasize the need for a secure and robust digital infrastructure:
  - Need for continuous work to strengthen the security and robustness of the digital foundation.
  - As part of this, Nkom carries out regional risk- and vulnerability analyses.
  - The analyses are an important basis for the work to strengthen the digital foundation.
  - The regional analyses map infrastructure that is important for both national and regional communications. It is particularly important to carry out these analyses for potentially vulnerable regions.

Examples from the la

Nkom proposal: Security plan 2025-2030 > Secure and robust electronic infrastrucure in a new era

Focus areas

1. Strenghten recilience in Mobile networks
   - Increased battery backup and redundant transmission to targeted base station locations
   - Increased cooperation between power and ecom sector
2. Continued ongoing regional risk and vulnerability analyses covering all regions in Norway. Basis for measures to strengthen regional and national networks
3. Stengthening redundancy and autonomy in transmission networks
4. Ensure that commercial mobile operators use several autonomous transmission networks
5. National and regional protection of critical communication infrastructure and services
   - Use of mountain facilities for physical protection of critical infrastructure
   - National control of communication services
   - National and regional autonomy

Security plan 2025-2030 proposal, continued:

Focus areas

6. Increased resilience to GNSS outages
   - Secure and robust time
   - Jamming tests and development of new methods for prevention, detection, and handling of interference
   - Assess the potential to use mobile networks for precise positioning
7. Increased capacity against data/cybercrime and attacks
8. Investigate and test the use of direct mobile satellite communication as a supplement to mobile and fixed networks
9. Enhanced preparedness
   - Test and implement national roaming as a preparedness measure
   - Conduct a pilot project for restoring mobile coverage in the event of service outages
   - "Strengthen preparedness across sectors (civil sector/defense sector, power/communications, authorities/commercial)"
   - Establish «best practices» for handling data attacks

Present and future challenges

- Dependencies and concentration in value and supply chains
- Sabotage
- Change management
- Marine fiber cables
- Extreme weather
- Cyber attack
- Insider threat