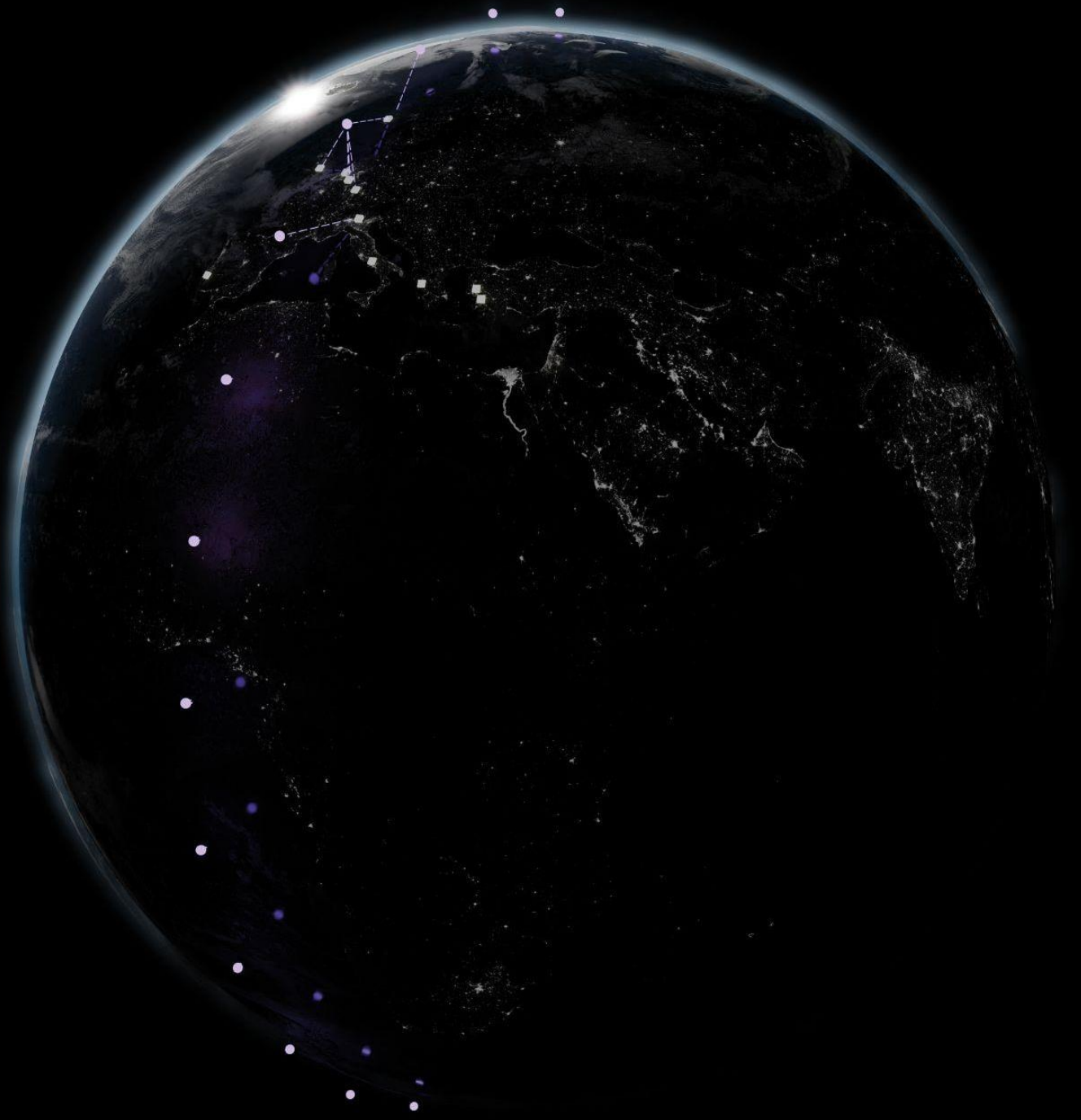
Case Study: A NATO QUANTUM CONSTELLATION



ATLAS

A toolkit by aegiq

ATLAS

Case Study: A NATO Quantum Constellation

Keeping the Alliance safe in post-quantum world

The resilience of the NATO alliance depends fundamentally on data security and privacy. Quantum Key Distribution (QKD) is a powerful tool for this purpose, and global key distribution and synchronisation is only possible via satellites.

NATO SATCOM Services 6th Generation (NSS6G) service still relies on classical encryption, vulnerable to future advances in quantum computing, and radio communications which may be easily intercepted. Free Space Optical (FSO) quantum communications mitigate these risks, either through key distribution, or eavesdropper detection on classical FSO laser communications systems.

We offer an example of cost-benefit analysis and a blueprint of a NATO QKD constellation carried out using the Atlas® toolkit.

Requirements for a resilient global network

To ensure effectiveness and resilience, a NATO QKD network must:

1. Generate key material[1] during a satellite overpass of an optical ground station (OGS).
2. Collate the generated key material over the entire network to maintain a global reserve of key material in each location.
3. Offer sufficient redundancy to ensure that the network retains enough cryptographic keys to last several months of downtime[2].

Figure 1. A depiction of 3 satellite orbits around the Earth produced by Atlas for the NATO constellation. These orbital trajectories offer maximal coverage of NATO sites in Europe and North America.

[1] Key material means sequences of bits known only to legitimate parties, used to build encryption keys of any length.
[2] Months of downtime might be required due to poor weather or visibility, satellite failure, or denial of service attacks.

Implementation

- First, the ground segment is defined within Atlas, using GPS coordinates of each OGS.
- Satellite orbital trajectories are then defined to ensure maximum OGS coverage.
- A cost-benefit analysis can then be performed by modelling the impact of constellation size and hardware specifications.
- For each network topology[3], Atlas calculates all possible FSO links between network nodes and evolves the network over time.

Figure 2. A map produced by Atlas showing the locations of the subset of NATO structures used as Optical Ground Stations (OGS) in the model. The subset includes existing NCI Agency satellite radio frequency communication installations.

- Link performance is evaluated for every satellite overpass, reporting secure bits generated, anticipated errors, impact of weather and cloud cover, and malicious activity sensing (eavesdropping probability).
- The hardware used to transmit the quantum payload during each overpass influences the link performance. Conventional QKD utilises attenuated pulsed lasers to approximate a single photon source, but Atlas can contrast this to more novel technological approaches.
- Atlas evaluates improved single link performance for a true quantum light source[4] compared to a conventional laser-based QKD.

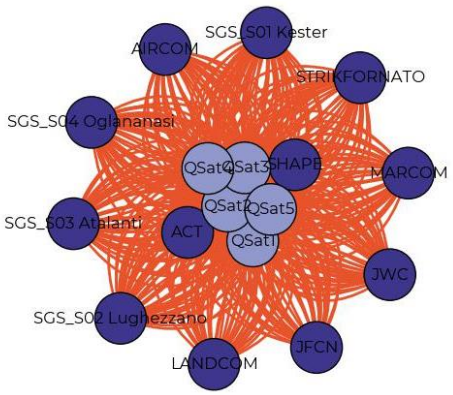


Figure 3. Atlas output of all FSO links in a network of 5 satellites over a 48 hour window.

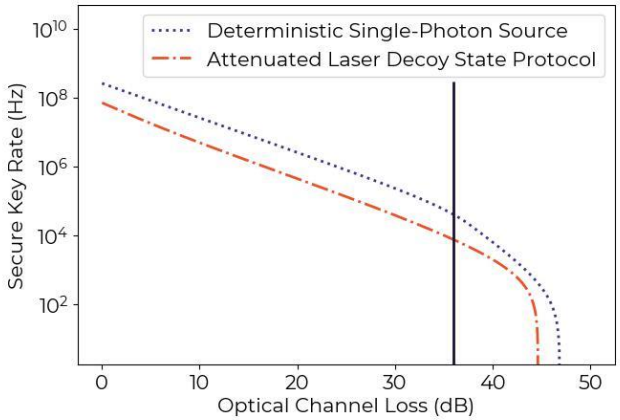


Figure 4. Atlas output showing link performance as a function of channel loss, caused by atmospheric scattering and absorption, diffraction and pointing errors.

[3] Particular way to interconnect satellites and/or ground stations with direct point-to point links.
[4] Deterministic single-photon or entangled-pair sources are needed, like Aegiq's iSPS®.

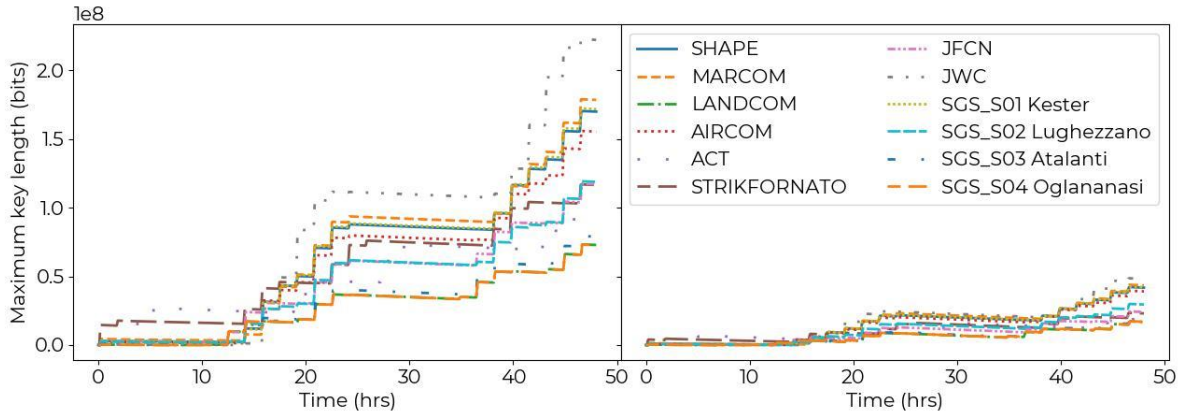


Figure 5: Atlas output showing the amount of key material (number of secure bits) distributed to each OGS over 48 hours for a constellation of 5 satellites. Left panel shows the case of satellites with high performance Aegiq iSPS hardware, right panel shows the case of attenuated pulsed laser sources.

Cost-benefit analysis

- To identify an optimum network topology, Atlas assumes an average key material depletion rate of 1,000 bits per minute per OGS[5].
- Under this requirement, and the technology constraints, Atlas reports that a constellation of 5 satellites carrying high performance quantum light sources offers a highly responsive and fast network, with significant redundancy of at least a factor of 12, enough such that the network would be resilient against significant denial of service attacks; extended poor weather inhibiting link performance; or maintenance and downtime of satellites. It could also cope with future increases in the key material usage rate by an order of magnitude, ensuring operational longevity.
- A constellation of 5 satellites installed with lower performance attenuated laser sources would lead to a reduction in cryptography capacity provision by a factor of at least 2, while only marginally reducing the cost by a factor of 0.75. Similarly, a cheaper solution consisting of a single satellite would reduce the service provision by a factor of at least 4. Both of these constellations would be more susceptible to downtime, and may have to be augmented with new satellites over time to keep up with increasing demand.

Number of satellites in constellation	Hardware on board	Uptime to build 3 months of key material (hours)	Estimated deployment cost factor	Redundancy per ground location[6]
1	iSPS	210 - 1140	x1	2 – 10
5	Laser-based	150 - 380	x4	6 – 17
5	iSPS	50 - 190	x5	12 – 51

[5] Key material can be used for different purposes, for example for conventional AES-256 message encryption, or an uncrackable one-time pad cipher

[6] Calculated as the ratio of the bits remaining vs bits used at each OGS after 48 hours, at a rate of 1000 bits used for encryption per minute per OGS.