

# Security in the Greenlandic teleinfrastructure

Hans-Henrik Grabe | grabe@nanoq.gl

# Answers (the quick and easy)

- More resources
- Redundancy
- Expanding Capacity

# Perspectives



Structure



Collaboration

Technology



Economy

Knowledge






# Structure

- Compliance with legislation
- Regulatory mandates
- Risk management requirements
  - Certification – ISO 27000 & ISO 42001
- Emergency preparedness
- Contingency planning
- Mandatory incident reporting
- Disclosure requirements
  - for the acquisition of critical network components





# Economy

- Political prioritizing
- Investments
- Operation & Maintenance

- International investments
  - Risk assessments
  - Who is on our side?



# Collaboration

- Collaboration internally in Naalakkersuisut
- Locally, network, knowledge sharing
- International collaboration (NIS 2 group, Luxemburg etc.)
- Research institutions
- Reporting of incidents



# Knowledge

- Professional certifications
- Development of expertise
- Continuing education
- Professional vs professionalism

- Knowledge and understanding of emerging technologies
- Public awareness and campaigns for citizens


Technology
– ensuring confidentiality, integrity, availability, and authenticity
at all levels
Solutions adapted for your infrastructure
Safe and closed networks
Datacenters

# Perspectives



Structure



Collaboration

Technology



Economy

Knowledge






# Then a CSIRT for Greenland

## A team that works before, during, and after a cyber incident

### BEFORE

**Identifies potential threats**

Provides early warnings and advice on protective measures.

### DURING

**Coordinates the response**

Maintains situational awareness and supports affected stakeholders.

### AFTER

**Strengthens preparedness**

Shares lessons learned and follows up on identified vulnerabilities.



# Quantitative Intelligence Framework for Cyber Threat Forecasting

## Key Analytical Questions

1. **What is happening right now?**
2. **Which indicators are connected?**
3. **How likely is a specific event?**
4. **When is the event expected to occur?**
5. **How reliable is the forecast?**

### Data Sources

OSINT • CTI • CERT Advisories
Incident Reports • Time Series
Actor Relations • Partner Data

### Data Processing

- Normalization
- Deduplication
- Timestamping
- Source Quality
- Data Validation

### Feature Engineering

- Indicator Values
- Trends
- Time Lags
- Sequences
- Network Relationships

## Analytical Models

### A. Observation

- Anomaly Detection
- Change Point Detection
- Regime Detection

### B. Forecasting

- Logistic Regression
- Gradient Boosting
- Bayesian Analysis

### C. Timing

- Survival Analysis
- Time-to-Event
- Hawkes Processes

### D. Advanced Analytics

- Sequence Models
- Dynamic Networks
- Temporal Graph GNNs

### Model Integration & Validation

Model Fusion • Calibration • Uncertainty • Backtesting

### Analytical Output

Probability • Expected Timing • Risk Development • Evidence • Explanations • Model Performance

# Qualitative Intelligence Framework for Cyber Threat Foresight

## Key Analytical Questions

1. What is driving the situation?
2. Who is connected to whom?
3. Which futures are plausible?
4. What are the implications?
5. How confident is the assessment?

### Information Sources

OSINT • CTI • CERT Advisories
Expert Judgement • Interviews
Policy & Strategy Documents
Partner Reporting • Field Notes

### Source Evaluation

- Source Reliability
- Credibility Assessment
- Triangulation
- Contextualization
- Gap Analysis

### Structuring

- Thematic Coding
- Actor Profiling
- Key Assumptions
- Drivers & Uncertainties
- Relationship Mapping

## Analytical Models

### A. Understanding

- Thematic Analysis
- Timeline Analysis
- Key Assumptions Check

### B. Network Analysis

- Actor & Stakeholder Mapping
- Centrality & Brokers
- Dependency & Cascade Mapping

### C. Foresight

- Horizon Scanning
- Scenario Planning
- Weak Signal Analysis

### D. Structured Analysis

- Competing Hypotheses (ACH)
- Red Teaming
- Indicators & Warning

### Integration & Validation

Triangulation • Peer Review •
Confidence Levels • Bias Checks

### Analytical Output

Situational Picture • Scenarios • Key Drivers •
Warning Indicators • Strategic Implications • Confidence

# Integrated Intelligence Framework for Cyber Threat Assessment

## Key Analytical Questions

1. Do data and narrative agree?
2. What explains the signals?
3. Which futures are supported?
4. Where do methods disagree?
5. How robust is the combined view?

**Quantitative Inputs**

- Probabilities • Trends
- Anomalies • Time-to-Event
- Network Metrics
- Model Uncertainty
- Backtest Performance

+

**Qualitative Inputs**

- Scenarios • Drivers
- Actor Profiles
- Weak Signals
- Key Assumptions
- Expert Judgement

→

**Shared Frame**

- Intelligence Requirements
- Common Indicators
- Actor-Event Mapping
- Time Horizons
- Confidence Scale

## Integrated Analyses

**A. Evidence Fusion**
- Weighted ACH (scored)
- Bayesian Updating
- Expert-Elicited Priors

**B. Scenario Modelling**
- Scenario Probabilities
- Cross-Impact Analysis
- Monte Carlo Simulation

**C. Network Intelligence**
- Graph + Actor Context
- Centrality & Brokers
- Cascade Risk Scoring

**D. Early Warning**
- Model-Driven Indicators
- Scenario Signposts
- Anomaly-Triggered Review

**Cross-Validation**

Cross-Method Triangulation • Divergence Check • Backtesting

**Integrated Output**

Probability + Context • Scenarios with Likelihoods • Early Warning • Explanations • Confidence



# Conclusion

- Manage the perspectives as needed
- Build your organization – internally and externally
- Know your data and your bias
- Attention to emerging technologies (quantum etc.)
- Know your data – and your methodology
- Continues improvement – always learn!

NALUNAARASUARTAATEQARNERMUT AQUTSISUT

TELECOMMUNICATIONS AUTHORITY OF GREENLAND

# Qujanaq

Hans Henrik Grabe | grabe@nanoq.gl

