

# New challenges in security communications

Kimmo Manni

Managing Director, State Security Networks Ltd



- Background for the heading: there are "conventional", concrete challenges (natural phenomena, strikes, disruptions, information security problems, war, etc.), for which we are "used to" preparing, i.e. for which we have a fairly stabilised range of means



- There are also challenges that have featured heavily in the news in recent years, but for which preparation has required extensive debate on the necessary means; it is only very recently that actual planning and implementation of actions have taken place.
- These "new" challenges include the partly intertwined risks and threats caused by, for example, changes in ownership of telecommunications infrastructure, globalisation of systems and business operations, long outsourcing chains and other changes in operational structures
- The question is one of protecting critical infrastructure against the consequences of changes and turning points



"Conventional" threats,  
for which we have  
already had contingency  
plans for several  
decades



Impact and means  
assessed

"New challenges", for  
which we have only  
recently found means  
for preparation

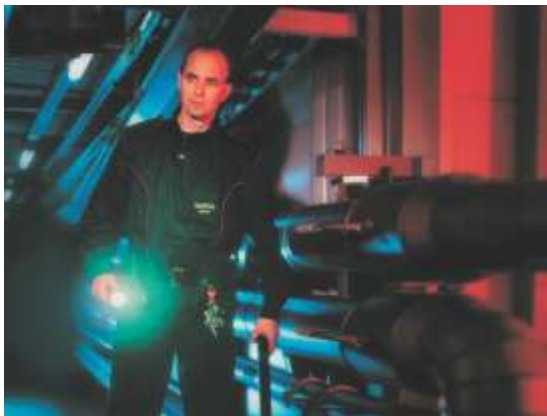


Impact difficult to  
analyse

**Security communications**

# Ownership of telecommunications infrastructures and related changes

- What is the buyer's agenda?
- Ownership often international, making it difficult to establish a background
- The problem is not the clarity of the revenue generation model, but the potential lack of one



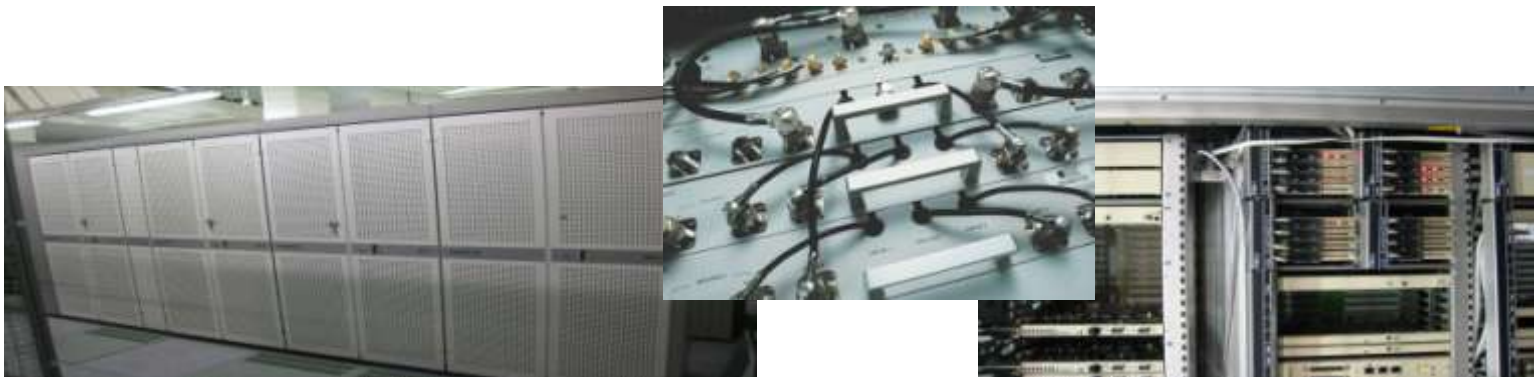
# Management of subcontracting chains and related changes

- Who do you work with and how can their operations be monitored?
- Management of networks and networking is difficult in a state of constant change
- Who will invest in preparedness in competitive tendering?



## Changes in technology and resulting impact on business structures and models

- Implementation often outsourced; ways of processing data and the location of data repositories may change
- Risks associated with turning points and the reliability of new technology
- Management of system integration
- High product development costs necessitate international markets and an extensive clientele for technology
- Failure by supplier may dramatically reduce life cycle



## Impact of globalisation

- Difficulty of recognising risks in the long chains involving numerous international players
- Structural changes are often irrevocable
- Significant cultural differences in operations and the approach to preparation
- The financial crisis demonstrated that instead of the actual operator or partner, the actual risk may be their financiers or guarantors



## Reaction and preparation opportunities available to society

- The above-mentioned challenges can be identified as key motives for recent authority projects aimed at ensuring communication security:
- TELVE
- TUVE
- Other projects (e.g. SOPIVA, KRIVAT)



# TELVE

- Working group appointed by the Ministry of Transport and Communications proposed in 2009 that the state acquire sufficient ownership and control of critical telecommunications networks components
- The state launched the operations of Leijonaverkot Oy, a subsidiary of State Security Networks, at the turn of the year (2010/2011)
- The company has begun implementing the policies outlined by the TELVE working group
- The TELVE operations of the new company connected to operations within the VIRVE network and the TUVÉ project

- TUVE is a project charged with implementing a high level of preparation in security authorities' data communications solutions
- The purpose is to elevate the level of protection and usability of data communications used by security authorities and to remove various dependencies of individual service providers
- Key objectives include the storing of critical data in Finland and the efficient monitoring and control of critical systems in Finland
- The TUVE project also affects the operation of both the VIRVE network and State Security Networks Ltd and subsidiaries

## Other projects

- The SOPIVA project, through the National Emergency Supply Agency and its cooperation networks in particular, has aimed at developing methods to PREPARE for the above-mentioned new challenges using AGREEMENTS
- The KRIVAT project of the Ministry of Transport and Communications and the National Emergency Supply Agency has been looking into the exchange of information among 24/7 CONTROL ROOMS FOR CRITICAL INFRASTRUCTURE and related security measures



## Summary

- The State Security Networks group actively supports all the above-mentioned projects by authorities and aims at acting as a strategic tool, owned by authorities, for preparing for these threats



Thank you!

Suomen Erillisverkot Oy

Tekniikantie 4 B

PL 357, 02151 Espoo

Puhelin 0207 400 500

Telefax 0207 400 501

[www.erillisverkot.fi](http://www.erillisverkot.fi)