Optimising Denmark's cyber emergency:

CONCLUSIONS & RECOMMENDATIONS

Jorge Ivan Contreras Cardeño
Head of the Impact Area of Resilience

CONCLUSIONS 1/2

The Russian cyber threat in Ukraine is significant and widely recognized by Danish stakeholders.

Telecom and energy are high-value targets; disruption can cascade across sectors and society.

Ukrainian testimony: telecom outages endanger civilians and, in worst cases, cost lives.

Denmark's authorities have an alternative medium to coordinate during outages.

Gap: Most citizens lack substitutes to reach family, colleagues, authorities, or critical digital services (banking, healthcare, appointments).

Bottom line: Hardening telecom is not only about uptime—it's about public safety. Treat telecom resilience as a societal safety issue, not just a technical KPI.

DBI

CONCLUSIONS 2/2

Plan for cascading failures (telecom + energy): coordinate operators and energy providers.

Borrow proven mitigations from Ukraine: alternative power sources, multiple SIMs/carriers, wider satellite systems use where appropriate.

Ensure critical services (banking, healthcare, public sector) develop low- or no-connectivity fallbacks (offline workflows, in-person options, phone trees, action cards).

Launch public preparedness guidance (checklists, neighborhood comms plans, emergency contact cards).

Run cross-sector exercises and red-team scenarios focused on destructive cyberattacks and prolonged telecom outages.

RECOMMENDATIONS

- **ORGANIZATIONS**
- *Develop the organizational ability to make flexible plans*
- *Education, transparency, communication, and practice*
- *U*nderstand and discuss the regulations in the sector and make a conscious gap analysis for compliance.

RECOMMENDATIONS

- TELECOMMUNICATIONS PROVIDERS

National Roaming for crisis situations

Prolonged operation capacity during energy outage.

Shared threat intelligence & Emergency simulations

Flexibility is a new value to develop

DBI

RECOMMENDATIONS

- **POLICY MAKERS**
- *Build support communities.*
- *Clear responsibilities for the protection of critical infrastructure*
- *Mandatory compatibility with cybersecurity measures for products aimed at critical infrastructure sectors.*

FUTURE RESEARCH

- Mapping interdependencies between critical sectors
- Identify and implement alternative communication methods not only for the organizations and authorities but also for the citizens.
- Design preparedness guidelines for the population based on learnings from the private sector.
- Research is needed to understand how to properly design attack simulations so that they address the specific security requirements, current competencies, and governance challenges.

DBI

FUTURE RESEARCH

Deepen cross-sector and cross-border understanding of challenges.

Foster collaborative interpretation and innovation (regulations).

Secure sustained funding for long-term impact (partnerships)

RESILIENCE CENTER DENMARK

NEWS EVENTS ABOUT US NETWORK

Contact DA

WHEN THE UNEXPECTED OCCURS, WE HELP KEEP DENMARK UP AND RUNNING.

Resilience Center Denmark strengthens the development of knowledge and solutions through innovation that can help companies meet new demands for increased resilience. The center unites the efforts of the seven Danish GTS institutes to promote the growth and export of resilience technology, and ultimately to strengthen Denmark's resilience.

QUESTIONS?

jcc@dbigroup.dk
+45 50809644
www.linkedin.com/in/jorgecontrerasdk