



# Cross-Border CII Dependencies

Regional Cybersecurity Forum  
Sofia, Bulgaria

Kadri Kaska  
29 November 2016

This briefing is a product of the NATO CCD COE.  
It does not represent the opinions or policies of NATO and is designed to provide an independent position.

# About NATO CCD COE



Enhance cyber defence capability,  
cooperation and information sharing  
among NATO, Allies, and Partners



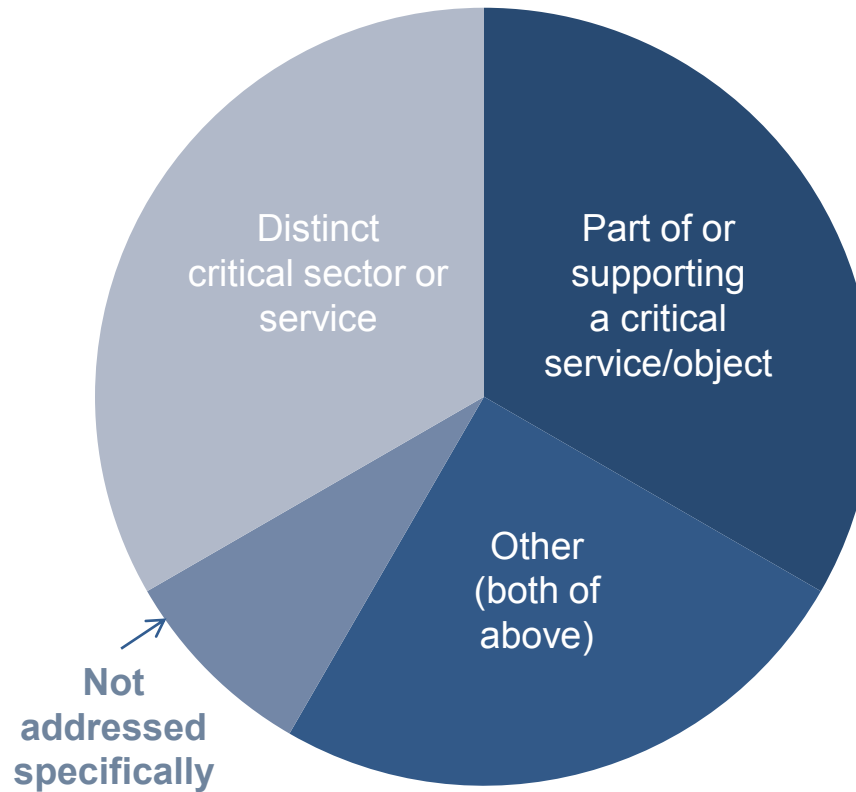
# Introduction



- Increasing reliance of vital services on cross-border CII
  - Potential source of instability even for countries that have addressed the issue domestically
- One of the least explored areas of cyber vulnerability
- Research
  - Existing state of knowledge in academic and security research
  - National awareness and remedies
  - Open source + survey

# National concept of CII

## CII approach in national law



# Critical sectors/services



IT and  
communications

Energy

Finance

Transport

Public security  
and public order

Water  
management

Food supply

Health and  
medical services

# Cross-border dependency



IT and  
communications

Energy

Finance

Transport

Public security  
and public order

Water  
management

Food supply

Health and  
medical services

Media

Government  
administration

*Legend:*  
substantial to critical  
minimal to substantial  
none to minimal

# Risks of cross-border dependency



- Natural and man-made hazards

## **TECHNOLOGICAL**

- Lack of technical expertise
- Sector-specific concerns

## **FINANCIAL**

- Funding of security systems

- Legal differences/ loopholes

## **LEGAL/ PROCEDURAL**

- Failure to take an all-hazards approach

- Different threat perceptions

## **SOCIAL/ CULTURAL**

- Different security cultures
- Lack of trust and information

# Remedial measures



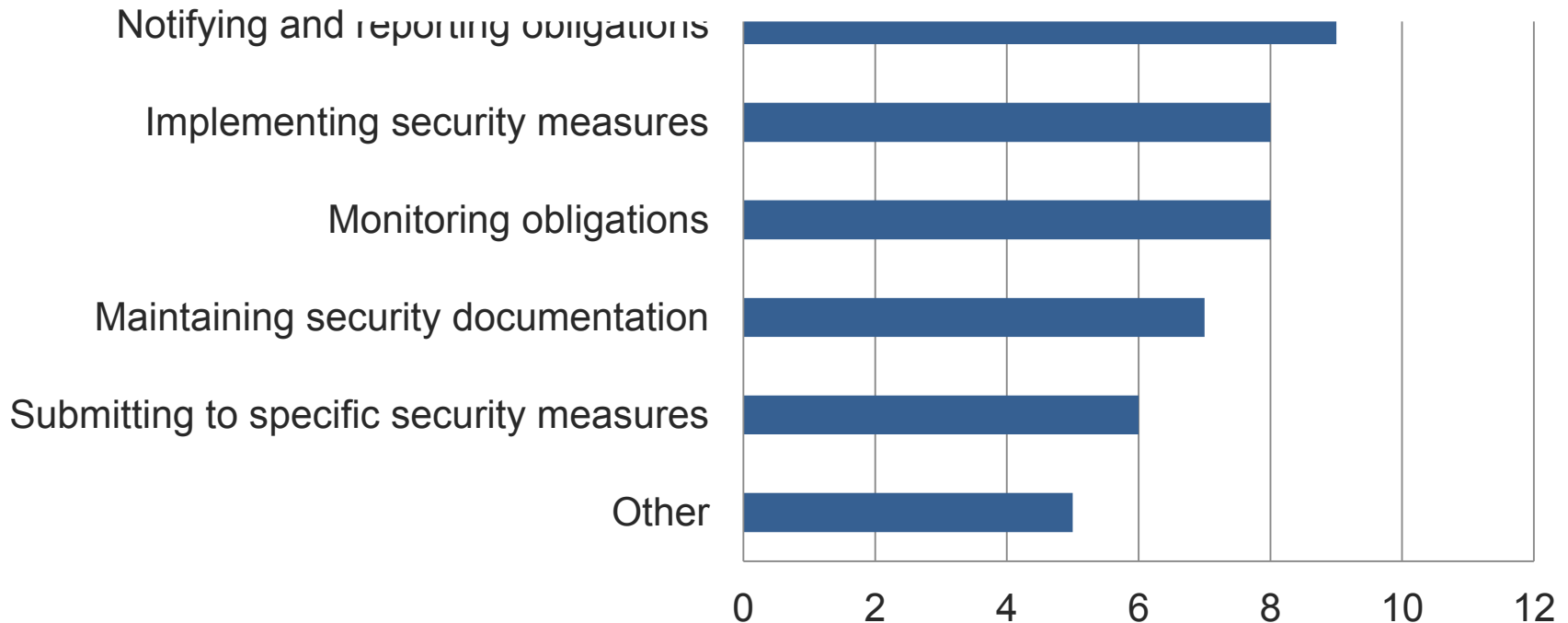
- All have legal instruments that address CI dependencies
  - Very few have specific, legally backed remedies related to cross-border CII
- National cyber security strategy
  - Many objectives supporting indirectly
  - Only one nation expressed a specific objective
    - “Interdependencies between vital services, including cross-border dependencies, must be constantly mapped and managed”
- All-hazards threat and risk assessments



# Operator responsibilities



## Legal obligations of responsible entities/individuals

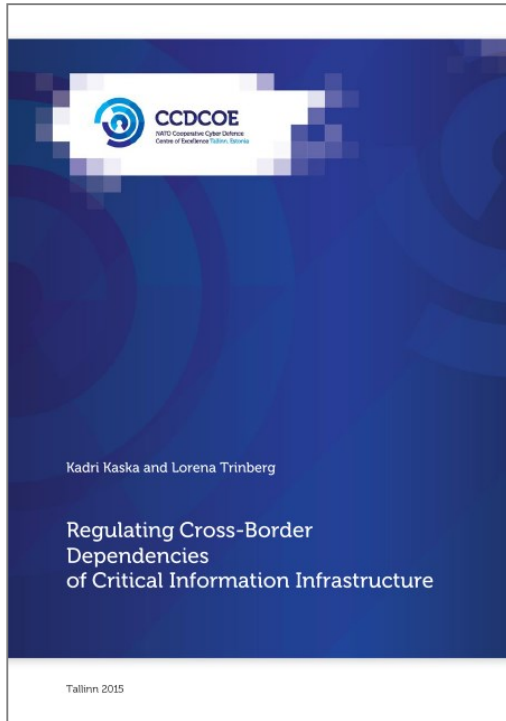


# National authorities



- Coordinating authorities for CIIP
  - NCSC or national CERT; occasionally, sectoral regulators
  - Functional relationship to national CIP coordinator
  - Role in crisis situations
- Relationship to operators
  - Assist CI operators, provide guidelines, etc.

# Publication



[https://ccdcoe.org/  
publication-library.html](https://ccdcoe.org/publication-library.html)

- Summary of findings
- PART I:  
12 country delineation
  - National C(I)I process
  - Responsibilities of actors
  - Cross-border remedies
  - Contacts
- PART II:  
Annotated Bibliography

# CONTACT

Kadri Kaska  
kadri.kaska@ccdcoe.org

Lorena Trinberg  
lorena.trinberg@ccdcoe.org

Filtri tee 12, 10132 Tallinn, Estonia +372 717 6800

