

Kibernetinis saugumas: nacionalinės ir tarptautinės dimensijos sąsajos



Rimas Ališauskas

Pagrindiniai principai

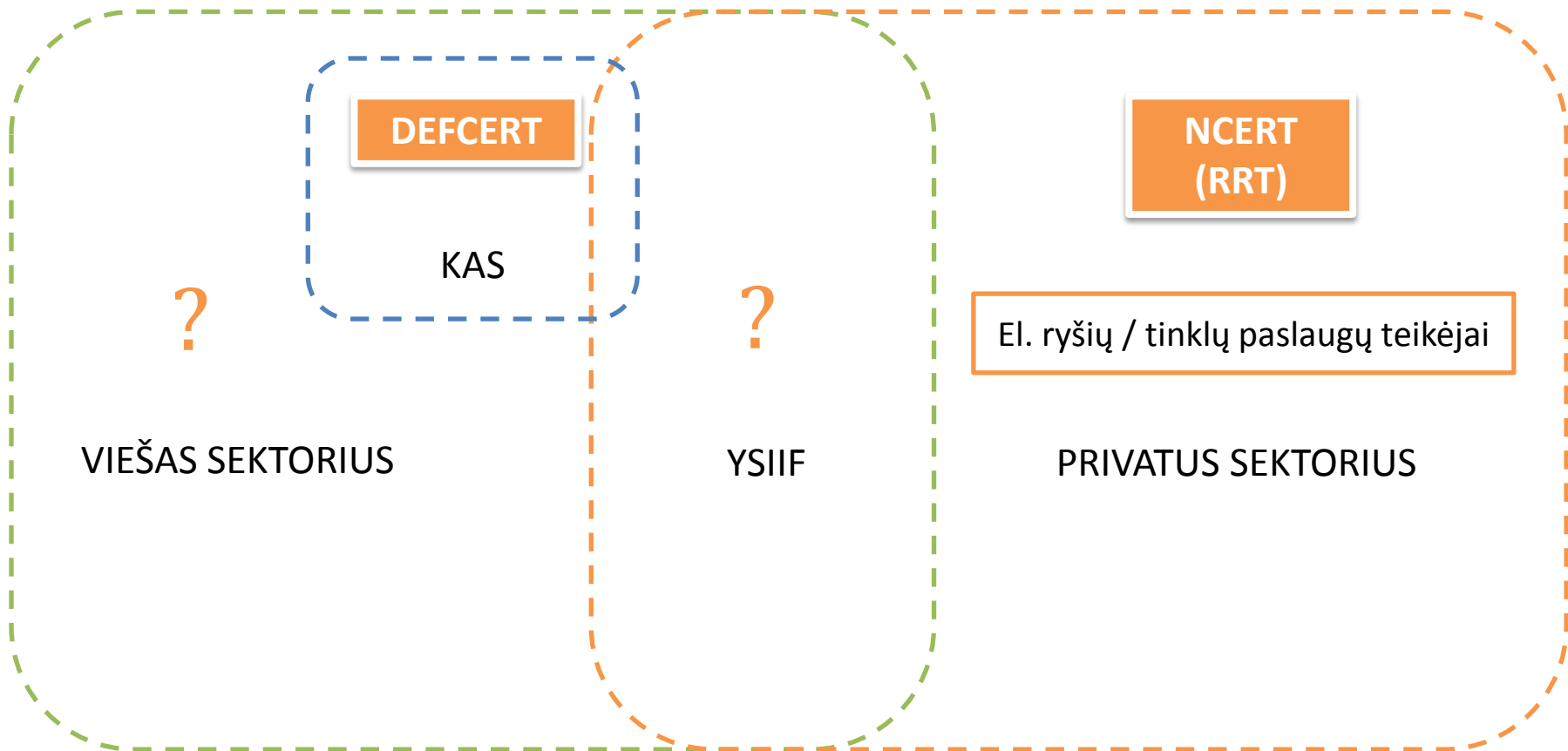
1. Principas, kad niekas mūsų negins, jei patys nesiginsime galioja ne tik fizinėje, bet kibernetinėje erdvėje

2. Niekas nežinos, ką ir kaip ginti, jei patys neplėtosime pajėgumų

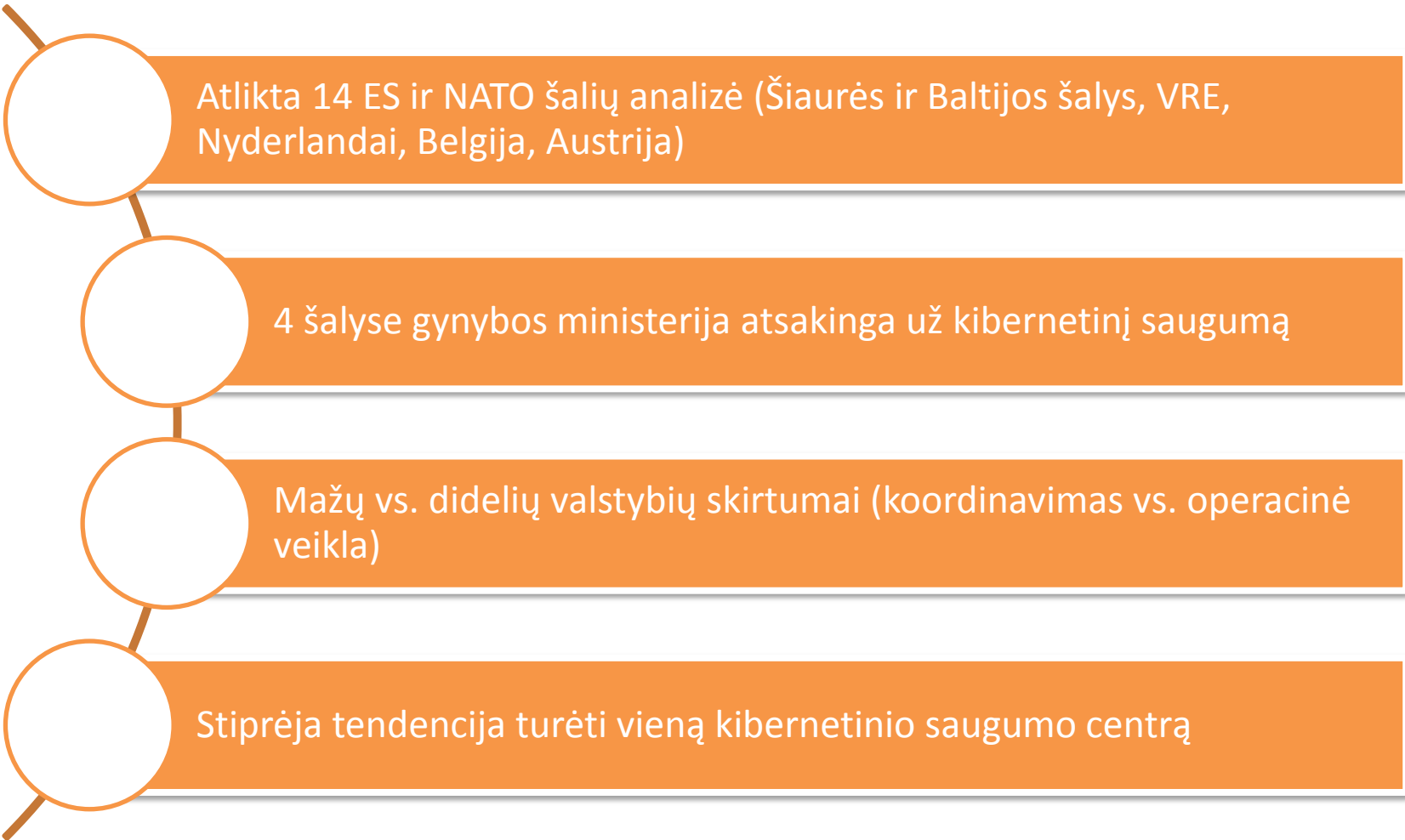
3. Neturime ir neturėsime pajėgumų vieni atsilaikyti didesnės kibernetinės krizės, ar sudėtingų kibernetinių atakų atvejais

**Turime plėtoti nacionalinius pajėgumus ir stiprinti ryšius su partneriais
(NATO, ES, dvišalis bendradarbiavimas)!**

Problema



Analizė



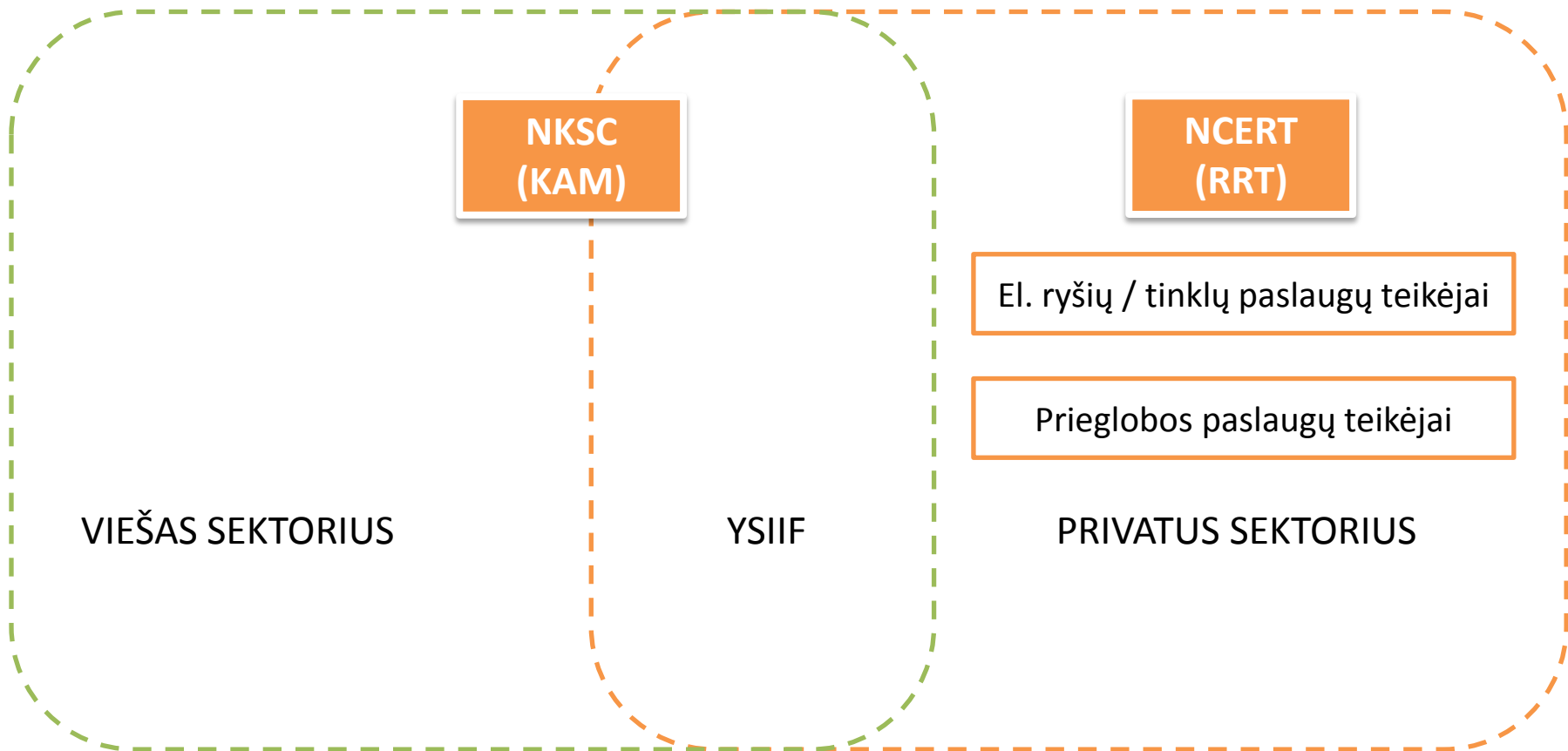
Atlikta 14 ES ir NATO šalių analizė (Šiaurės ir Baltijos šalys, VRE, Nyderlandai, Belgija, Austrija)

4 šalyse gynybos ministerija atsakinga už kibernetinį saugumą

Mažų vs. didelių valstybių skirtumai (koordinavimas vs. operacinė veikla)

Stiprėja tendencija turėti vieną kibernetinio saugumo centrą

KSĮ modelis



NATO parama

Dvišalis susitarimas su NATO kibernetinės gynybos valdymo agentūra dėl ekspertų komandos pasitelkimo

Kibernetinė gynyba turi būti kolektyvinės gynybos integrali dalis

Parama ne 5 straipsnio krizės atveju

Derybinė galia ir gebėjimai pasinaudoti parama priklauso nuo nacionalinių pajėgumų

Sudėtingos nuolatinės grėsmės (APT)

Šaltinis

- Pagrindiniai kūrėjai – valstybinės organizacijos

Taikinys

- Tikslinė grupė, jautri informacija, kritinė infrastruktūra

Sprendimas

- Reikalinga išimtinė kompetencija ir tarptautinis bendradarbiavimas

Kelias

- Nacionalinės kompetencijos ir pasitikėjimo tarp partnerių stiprinimas

Iššūkiai



Išvados

1. Principas, kad niekas mūsų negins, jei patys nesiginsime galioja ne tik fizinėje, bet kibernetinėje erdvėje

2. Niekas nežinos, ką ir kaip ginti, jei patys neplėtosime pajėgumų

3. Neturime ir neturėsime pajėgumų vieni atsilaikyti didesnės kibernetinės krizės, ar sudėtingų kibernetinių atakų atvejais

**Turime plėtoti nacionalinius pajėgumus ir stiprinti ryšius su partneriais
(NATO, ES, dvišalis bendradarbiavimas)!**