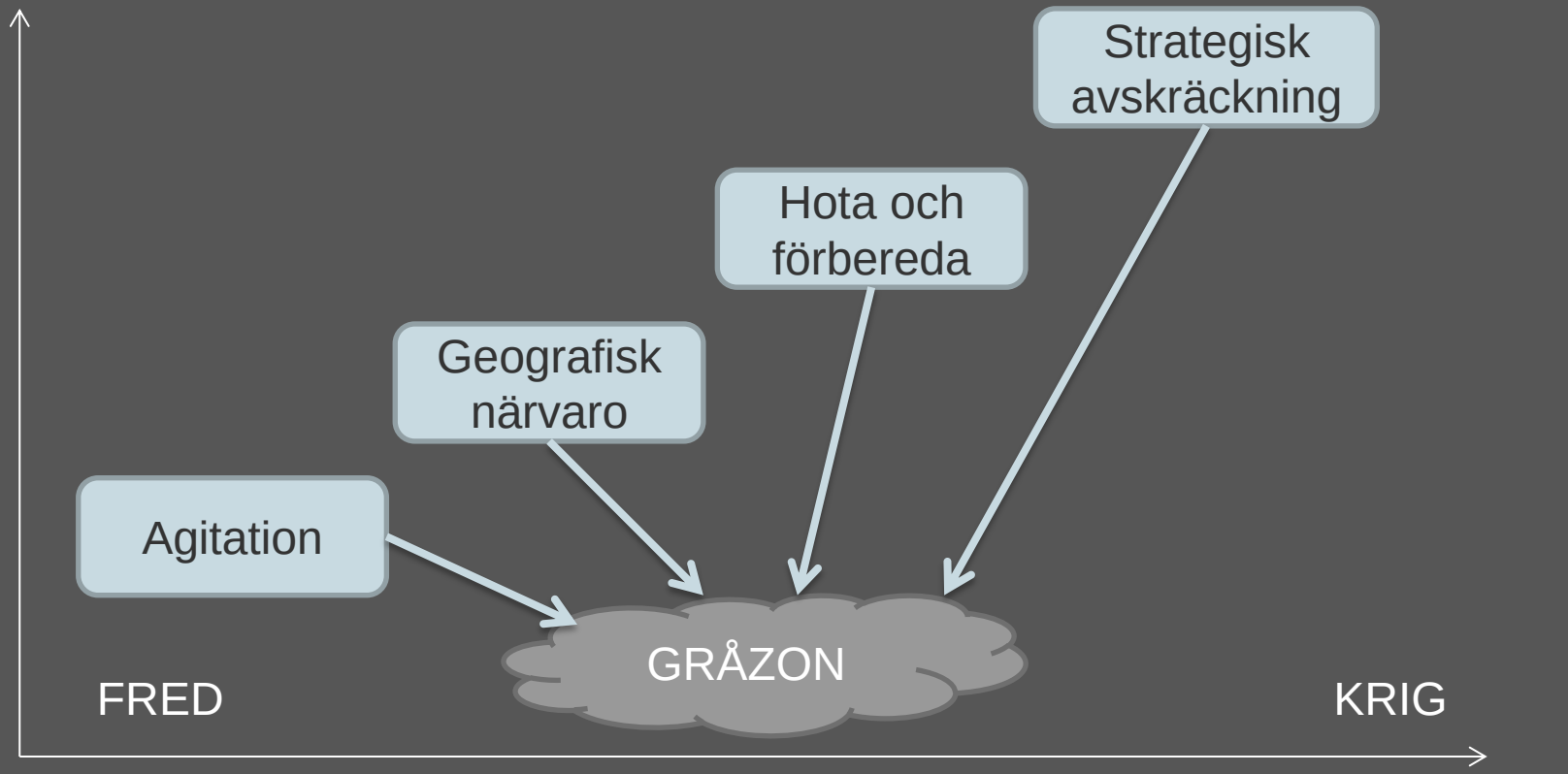
IT-hot, informationssäkerhet och IT-säkerhet

Tomas Borg

Antagonistiskt hot mot Sveriges säkerhet

- Höger respektive vänsterextrem terrorism
- Islamistiskt motiverad terrorism (våldsbejakande islamister)
  - Cirka 300 bekräftade resenärer
  - Mål; allmänhet, militär, polis och rättsväsende
- Ensamagerande
- Organiserad brottslighet

Militärt angrepp



SVENSKA KRAFTNÄT

Antagonistiskt hot mot Sveriges säkerhet

Underrättelseverksamhet och/eller Spionage

SVENSKA KRAFTNÄT

Operationer mot svenska intressen

- Försvarsindustrin
- Energi
- Telekommunikation
- Finans

SVENSKA KRAFTNÄT

Aktörer

- Statliga
- Icke statliga
  - Cyberkriminella
  - Ideologiskt motiverade hackare
  - ”Crime-as-a-service”

SVENSKA KRAFTNÄT

Metoder

- Informationsinsamling sker via:
  - Öppna källor
  - Insider
  - Elektroniskt angrepp/cyberoperationer

SVENSKA KRAFTNÄT

Dimensionerande hotbild

Bedömningen är att resursstarka aktörer med stor förmågebredd utgör det dimensionerade hotet när ansvariga för viktiga elinfrastrukturer utformar och kravställer informations- och IT-säkerhetsfunktioner.

Nationell RSA för elsektorn 2016

SVENSKA KRAFTNÄT

Informationssäkerhet

Informationssäkerhet syftar till att information skall vara

> Konfidentiell

> Riktig

> Tillgänglig

SVENSKA KRAFTNÄT

När det gäller driftsystem

Informationssäkerhet syftar till att information skall vara

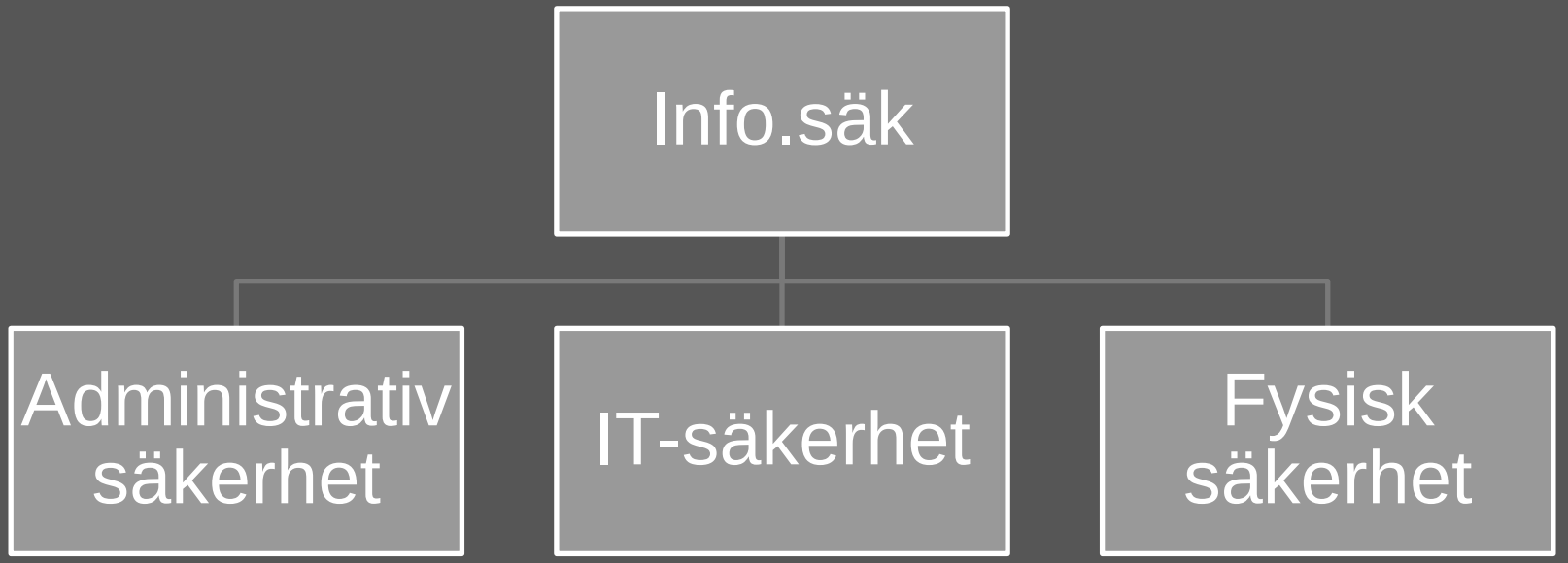
> Tillgänglig

> Konfidentiell / Riktig

Detta påverkar utformandet av IT-säkerhetsåtgärder för kontroll- och driftsystem.

SVENSKA KRAFTNÄT

Detta sker genom



SVENSKA KRAFTNÄT

IT-säkerhet i SCADA / ICS

SVENSKA KRAFTNÄT

IT-säkerhet i SCADA / ICS

Teorin bakom IT-säkerhet skiljer sig inte från annan säkerhet.

> Identifiera det skyddsvärda

> Identifiera hotaktörer

> Identifiera sårbarheter

> Implementera skyddsåtgärder

SVENSKA KRAFTNÄT

IT-säkerhet i SCADA / ICS

De tre viktigaste punkterna

1. Ha koll på vad som händer!

   > Loggar

   > IDS

   > Honeypot

SVENSKA KRAFTNÄT

IT-säkerhet i SCADA / ICS

De tre viktigaste punkterna

2. Sektionera nätet!

- > Brandväggar
- > Air gap
- > Logiskt skilda nät

SVENSKA KRAFTNÄT

IT-säkerhet i SCADA / ICS

De tre viktigaste punkterna

3. Kontrollera behörighet och åtkomstpunkter!

- Användare
- Administratörer
- Fjärråtkomst

SVENSKA KRAFTNÄT

IT-säkerhet i SCADA / ICS

Stor skillnad mellan olika elbolags IT-arkitektur gör det svårt att ge generella rekommendationer.

SVENSKA KRAFTNÄT

Vad säger FOI?

NCS3: Internetanslutna styrsystem i Sverige

Författare: Hannes Holm
Ort: Linköping
Sidor: 43
Utgivningsår: 2017
Publiceringsdatum: 2017-04-05
Rapportnummer: FOI-R--4415--SE

FOI

SVENSKA KRAFTNÄT

Ytterligare hjälp på vägen

> *SVK hotkatalog IT-/Cyberhot*

> *SVK vägledning IT-säkerhetsarkitektur*

> *SVK utbildning i IT-/Cybersäkerhet för SCADA / ICS*

SVENSKA KRAFTNÄT