



Cyberforsvaret

Cybertrusselen –
Forsvarets perspektiver og håndtering av trusselbildet

Generalmajor Roar Sundseth
Sjef Cyberforsvaret



Cyberdomenet

- Hva er Cyberdomenet? Et militært perspektiv...
- En erkjennelse i Langtidsplanen for forsvaret av 2012
 - Hvilke konsekvenser har erkjennelsen av et nytt domene?
 - Hvordan tilpasser Forsvaret seg det nye domenet?
 - Hvordan påvirkes Forsvaret av det nye domenet?
- Cyberforsvaret – Ett tilsvaret til et trusselbilde

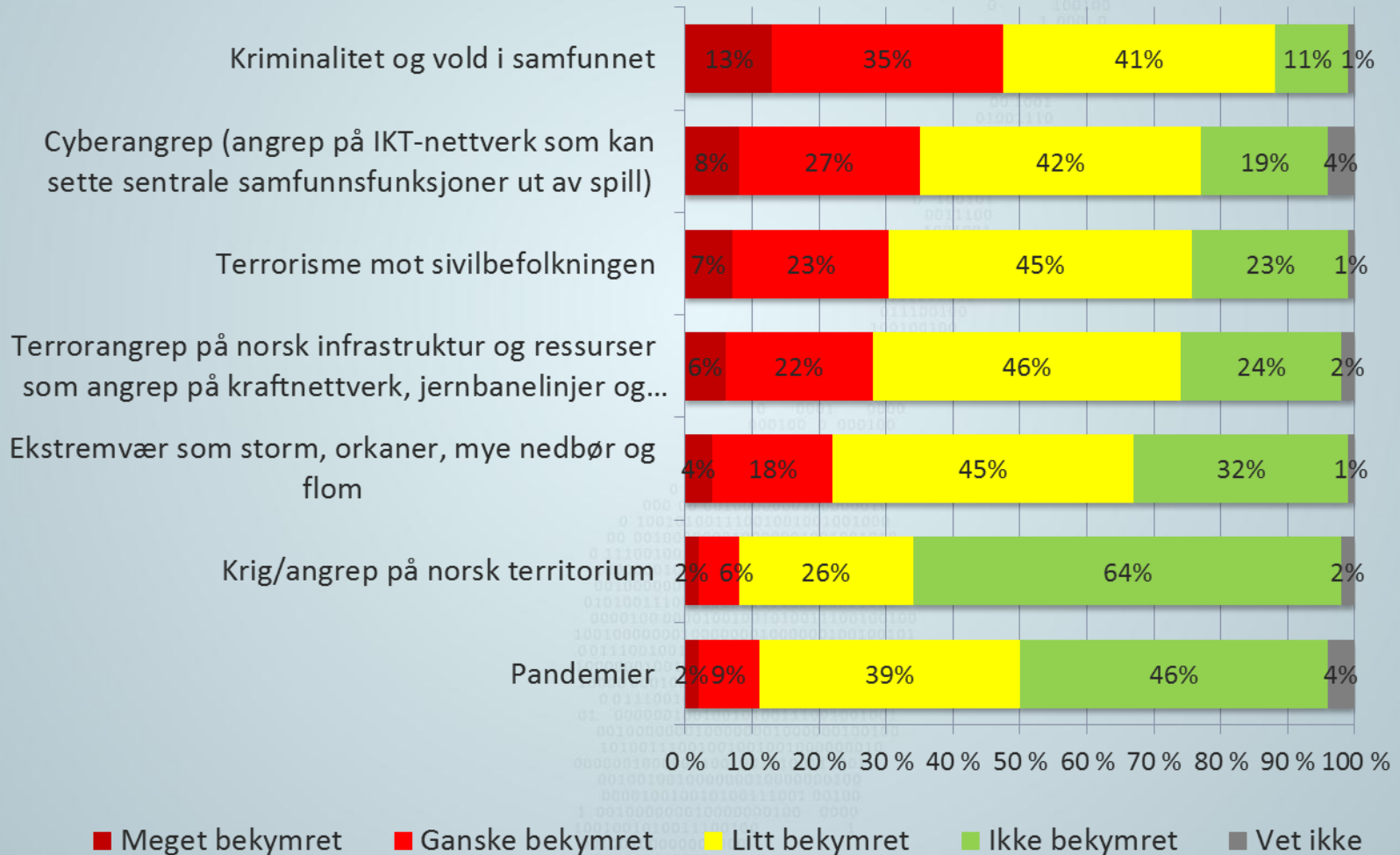


Hva er Cyberforsvaret?

- Cyberforsvaret er en militær organisasjon som skal drifte, sikre og forsvare Forsvarets datasystemer, nettverk, og høyteknologiske plattformer mot angrep i og fra det digitale rom.
- Cyberforsvaret er en militær styrkeprodusent, som produserer unik spisskompetanse i form av militære dataingeniører og ledere.
- Cyberforsvaret leder den teknologiske utviklingen av Forsvaret, og implementerer ny teknologi og nye konsepter innenfor sikre operative rammer.
- Cyberforsvaret er en organisasjon med unik kunnskap og kompetanse som settes på prøve hver dag. Vi har en ambisjon om å dele denne kunnskapen og kompetansen gjennom aktivt samarbeid og dialog med relevante aktører i Norge.



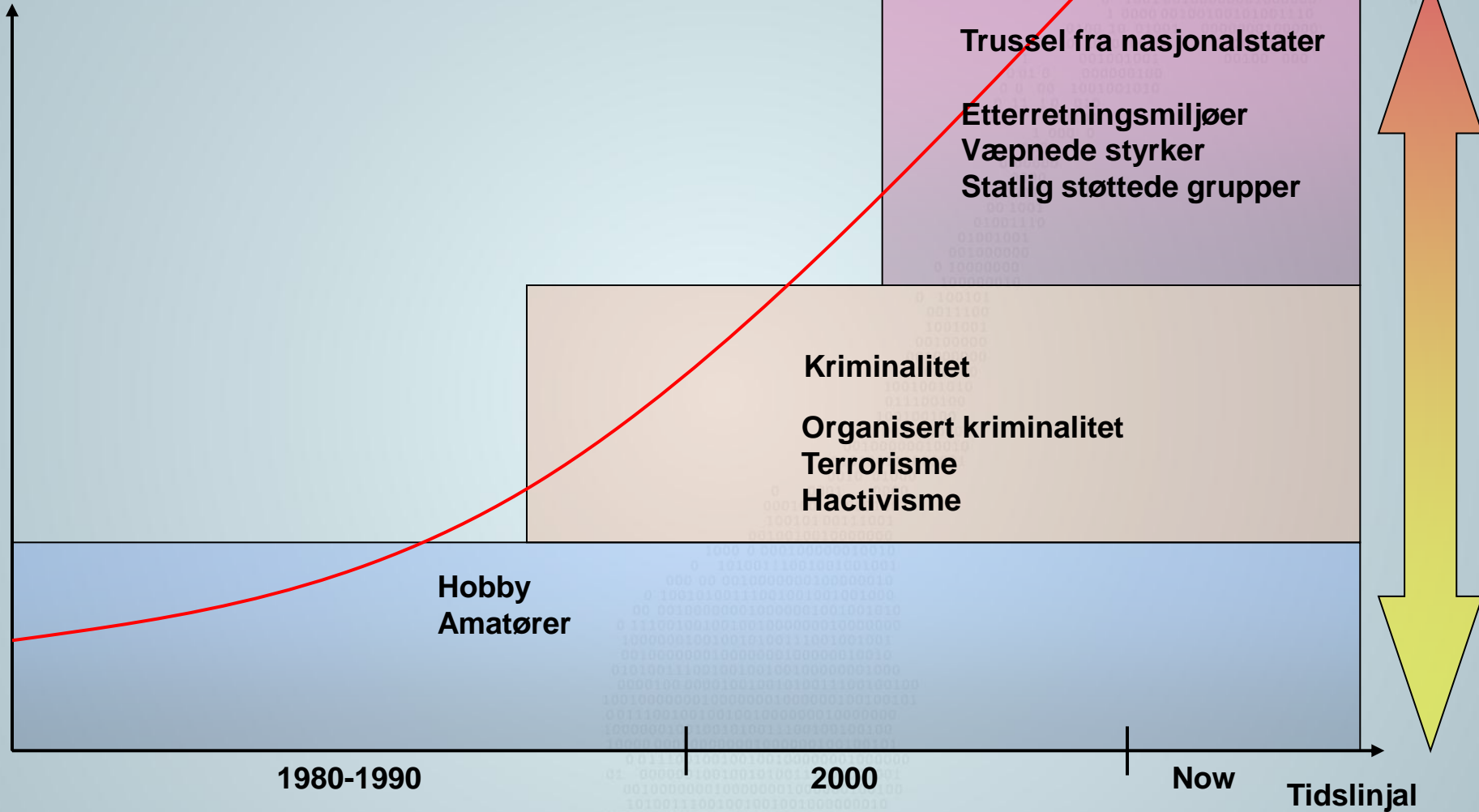
Hvor bekymret er du for følgende trusler mot nasjonal sikkerhet?



Trender og utviklingstrekk

- Stormaktene vil ikke kunne dominere Cyberspace.
- Nasjonalstater vil forbli den dominerende makten i Cyberspace
- Cyberspace vil være en utfordring for nasjonalstater.
- Mindre nasjoner vil i større grad kunne prosjektere myk og hard makt gjennom Cyberspace.
- Relevant, balansert og tillitsverdig nettforsvar og informasjonssikkerhet vil være en utfordring for alle.

Påvirkningsgrad



En risikoanalyse for Norge

- Tommelfingerregel: Jo mer teknologisk avansert en nasjon er, jo større er trussel og konsekvens for cyberangrep.
- Norge er en teknologisk avansert nasjon, og vi søker løpende å bruke datasystemer for å spare kostbare årsverk.
- Hva er sårbart?
 - Finansnæringen, banker, børs
 - Petroleumsindustrien
 - Strømproduksjon og elektrisk infrastruktur
 - Næringsliv og kommersielle interesser
 - Forsvaret

Hvordan tenker vi om Cybertrusselen

- Kompetanse og kunnskap er nøkkelen
- Forsvarbar infrastruktur er viktig
- En økende trussel hvor mange allerede er på etterskudd
- En naturlig og integrert del av enhver militær operasjon
- Utstrakt behov for samarbeid – mellom alle gode krefter
 - Cyberforsvaret er på mange områder 'støttende' for andre
 - Bistandsinstruksen og Cyberforsvarets rolle
 - Hvilke kapasiteter kan CYFOR bidra med når anmodningen kommer?



Spørsmål Kommentarer

```

010
0 1001
0 1 00 11100
100 1 001 01001001
0 1 001 11 00100100100
1 0000 0001000000010
00000 100100 101001
11001 0010010010 0000 0
01000000001000 00
01 0 010010100111001 0
0 1001 00100000001000000 0
1 0000 00100100101001110
0100 10 01001 00000000100000
0 0 100000010 01001010011
1 001001001 00100 000
0 01 0 000000100
0 0 00 1001001010
0 11 10 010
0 100100
1 000 0
0001
0 00000
0100
00001
00 1001
01001110
01001001
001000000
0 10000000
100000010
0 100101
0011100
1001001
00100000
001000000
0 1000000
1001001010
011100100
100100100
00 000100000
00100000010010
01020011001001
0010 01000
0 0001 0000
000100 0 000100
100101 00111001
0010010010000000
1000 0 000100000010010
0 10100111001001001001
000 00 0010000000100000010
0 00100000010000001001001010
0 111001001001001000000010000000
100000010010010100111001001001
001000000010000000100000010010
010100111001001001001000000001000
0000100 00001001001010011100100100
10010000000100000001000000100100101
001110010010010010000000010000000
10000001001001010011100100100100
10000 000100000001000000100100101
0 01110010010010010000000010000000
01 000000010010010100111001001001
0010000000100000001000000100100
101001110010010010010000000010
000000100000010010010100111001
0010010010000000100000000100
0000100100100111001 00100
1 001000000010000000100 0000
1001001010011100100 1
00100100000001000
0000100000010
010010100
111001

```

