

og mentale

# Digitale sikkerhetsutfordringer

## Betraknninger fra et operatørspesktiv



Frode Hommedal

Teknisk direktør

PwC.no/Cyber

Oktober 2020



Eller:

Fra utfordring  
til ulykke i den  
digitale hverdagen

Igjen...



**Twitter:** @FrodeHommedal  
**Hashtag:** #Digital2020

# Frode Hommedal

Teknisk Direktør  
PwC.no/cyber

Teknolog som gjennom snart to tiår har tatt reisen fra utvikler og teknisk analytiker til taktisk og strategisk rådgiver innen operativ cybersikkerhet.

**"Claim to fame"**

13 års erfaring med "incident response" for myndigheter og kritisk infrastruktur.



---

NORWEGIAN  
NATIONAL SECURITY  
AUTHORITY

Frode Hommedal – PwC.no/cyber



**Twitter:** @FrodeHommedal | **Hashtag:** #Digital2020

# Frode Hommedal

Teknisk Direktør  
PwC.no/cyber

Har en del erfaring med øvelser.

- IKT-o8
- NATO og EU
- Øvelse Bukkesprang
- Cyberøvelser i kraftsektoren

Brenner for øving og læring.



---

NORWEGIAN  
NATIONAL SECURITY  
AUTHORITY





# pwc.no/cyber

Fra serverrom til styrerom

PwC satser på cybersikkerhet fordi vi er et selskap som ønsker å bidra til å løse de største utfordringene i samfunnet.

Rollen vi søker er å være *trusted advisor* for norske virksomheter som trenger støtte til å møte og løse sikkerhetsutfordringene samfunnet står overfor.

“

*Famous for strategy, relevant in crisis.*

– Grant Waterfall (PwC)





# pwc.no/cyber

Fra serverrom til styrerom

Målet vårt i *Cyber & Privacy* er å bidra til å lukke gapet mellom det operative og toppledelsen ved å være tilstede *fra serverrom til styrerom*.

- Strategi, risiko\* og transformasjon
- Etterretning, overvåkning og respons

“

*PwC praised for “Innovation, vision, and the ability to engage executives are key differentiators”.*

– Forrester Wave



Selv jobber jeg stadig oftere med transformasjon,  
samtidig som jeg prøver å være *relevant in crisis*.



Dette er «hackerne» i PwC's Red Team. De bor nærmest serverrommet.

Anyway...

Målet med dette  
foredraget er å grave  
litt mer i begrepet  
**digitale utfordringer**.

Så la oss hoppe i det.





# Problembeskrivelse



Vi har digitalisert i stor fart, men digital sikkerhet har ikke blitt adoptert i samme tempo.

“

*We put every critical system on the backbone of the Internet, but the Internet wasn't ready for it.*

– Melissa Hathaway



Vi slåss mot folk, ikke  
mot «datavirus».

“

*You don't have a malware  
problem, you have an  
adversary problem.*

– Kevin Mandia, CEO I Mandiant (2012).



Omfanget er stort,  
har vært det lenge, og  
rammer store verdier.

“

*[Cybercrime is] the greatest transfer of wealth in history.*

– Gen. Keith Alexander, dir. for NSA (2012).



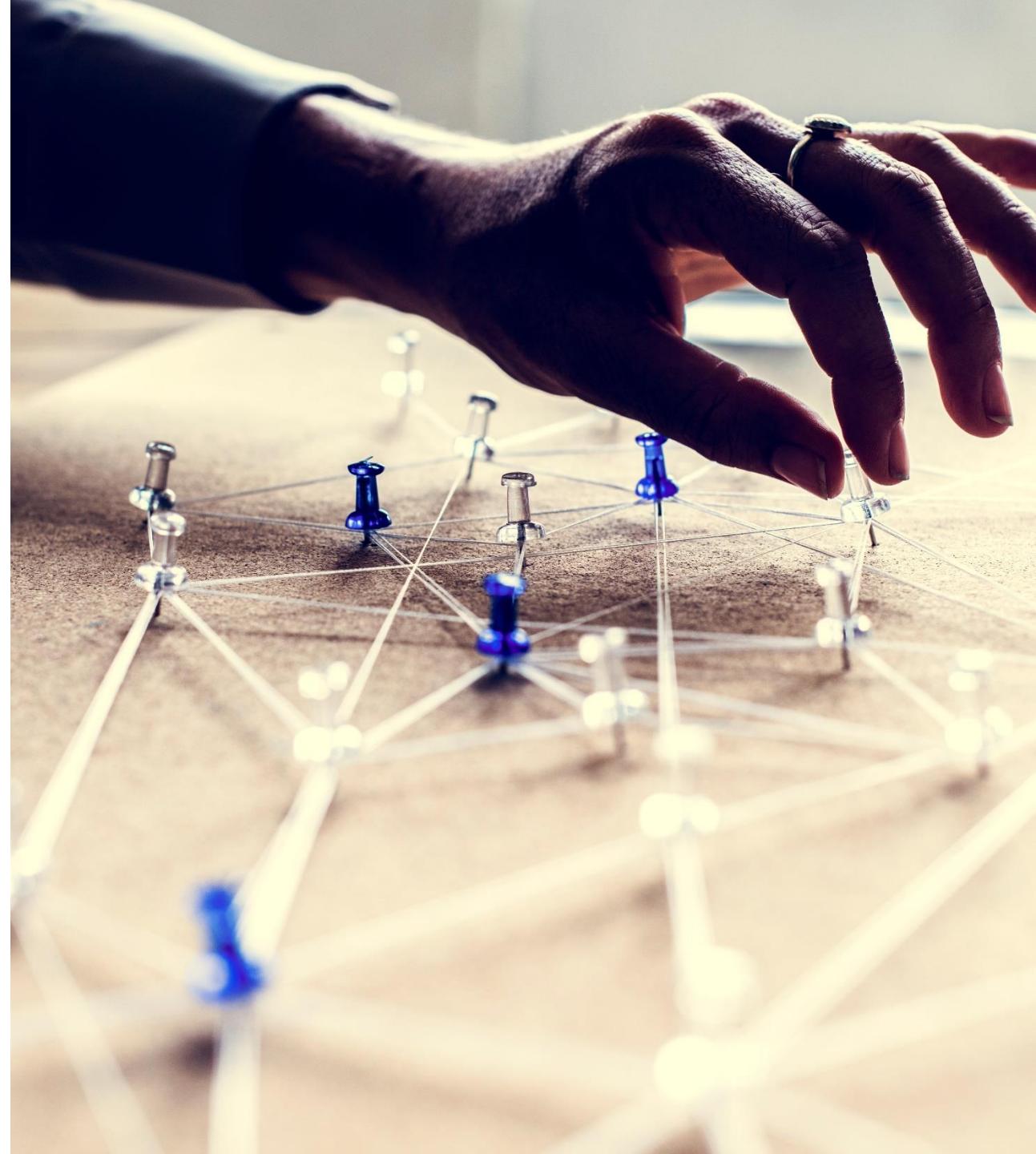
I tillegg er en av hovedutfordringene:

Vi tenker i lister når vi jobber med sikkerhet. Sjekklister.

“

*Defenders think in lists.  
Attackers think in graphs.  
As long as this is true,  
attackers win.*

– John Lambert (Microsoft)



Min erfaring med  
sikkerhetshendelser  
er at virksomhetene  
~~nesten~~ aldri hadde  
«sikkerheten på stell»

Manglende oversikt og kontroll. Manglende oppdateringer.  
Manglende segmentering. Manglende tilgangsstyring.

**Gjentatte røde  
revisjonsrapporter.**



«Men altså, vi kan jo ikke forvente at alt er grønt...»

# H.D. Moore's Law

Alt du trenger for å utvikle digitale angrep ligger klar for nedlasting på nett.



*Casual Attacker power  
grows at the rate of  
Metasploit.*

– Joshua Corman

```
=[ metasploit v4.16.4-dev
+ - - -=[ 1679 exploits - 962 auxiliary - 296 post
+ - - -=[ 496 payloads - 40 encoders - 10 nops
+ - - -=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

msf > banner

```
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMN$                                           vMMMM
MMMN\l   MBBBBB           BBBB  JBBBBB
MMMN\l   BBBBNNN           NNNNNNNNN  JNNNNN
MMMN\l   BBBBNNNNNNnnnnnNBBBBNNNNNNNNNNNN  JBBBBB
MMMN\l   BBBBNNNNNNNNNNNNNNNNNNNNNNNNNNNN  jBBBBB
MMMN\l   BBBBNNNNNNNNNNNNNNNNNNNNNNNNNNNN  jBBBBB
MMMN\l   BBBBNNN           BBBB  jBBBBB
MMMN\l   BBBBNM           BBBBN  jBBBN
MMMN\l   BBBBN            BBBBN  jBBBN
MMMN\l   BBBBNM           BBBBN  jBBBN
MMMN\l   BBBBN            BBBBN  jBBBN
MMMR?MMNM           ?MMNM   .dMMMMM
MMMMNm`?MMM          `?MMM   MMMM` dMMMMM
MMMMMMNN?MM          ?MM     MM?  NBBBBBBN
MMMMMMNNNNMMNNNNNNNNe           JBBBBBNNNNNN
MMMMMMNNNNNNNNNNN,           eBBBBBBNNNNNNNN
MMMMNNNNNNNNNNNNNNNNNNNx      MMMMMNNNNNNNNNN
MMMMMMMMNNNNNNNNNNNNNNNn+.+MMNNNNNNNNNNNNNNNNNN
                                         https://metasploit.com
```

Metasploit er programvare du kan laste gratis ned fra Internett som hjelper deg å gjennomføre et teknisk cyber-angrep.

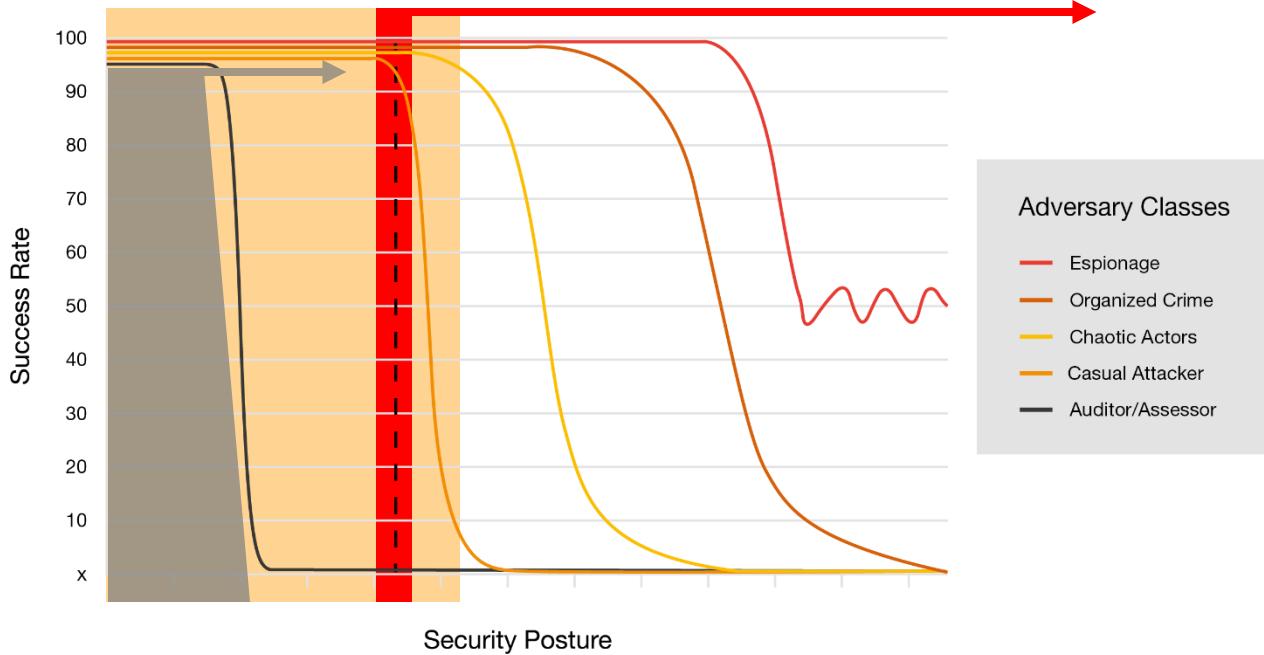
```
=[ metasploit v4.16.4-dev
+ - - -=[ 1679 exploits - 962 auxiliary - 296 post
+ - - -=[ 496 payloads - 40 encoders - 10 nops
+ - - -=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

msf > banner

# «Metasploit»

# «Casual attacker»

# «Revisoren»

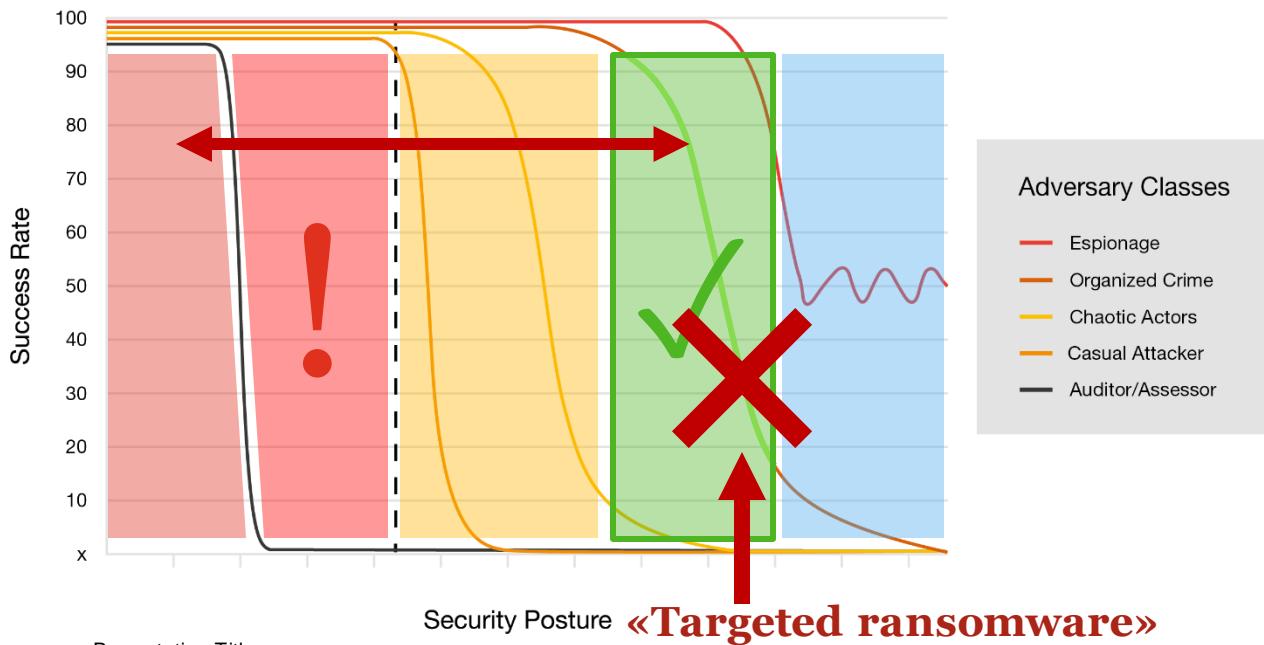


Revisoren er  
den enkleste  
«motstanderen»  
å overvinne.

...og er trolig den som  
utvikler seg saktest.

Mens «casual attacker power»  
utvikler seg stadig hurtigere.

En revisjon beviser  
ikke god sikkerhet,  
men kan bevise dårlig.



Dårlig og vet det.

! Dårlig, men vet det ikke!

På bedringens vei.

✓ God sikkerhet.

Svært god sikkerhet.

**NB:** I 2020 er «god sikkerhet» faktisk helt nødvendig, og gapet mellom «compliant» og «god» må lukkes.

# Revisoren er den egentlige førstelinjen din.

Revisoren er den første trusselaktøren du må klare å bekjempe før du går videre til neste nivå og går løs på aktørene i trusselbildet ditt.



## VIKTIG MELDING:

Dersom revisoren finner feil  
hos deg kan jeg love deg at

reelle trusselaktører  
vil finne langt flere.

Dette er ett av mine favorittsitter.

“

*Risk comes from not knowing what you're doing.*

– Warren Buffett



Min påstand er altså er  
når det kommer til

## «cyber risk»

så vet vi veldig ofte ikke  
hva vi holder på med.



# Dette er vår største digitale utfordring.

At vi ikke vet hva vi holder på med.



Som er skikkelig dumt, siden ...

Vi kan faktisk  
«sikre oss helt»  
mot cyberangrep.

(Mer om det siden)



Problemet er at  
vi forstår ikke  
egentlig teknologien  
vi omgir oss med.



Og at vi har  
**problemer**  
med å snakke på tvers  
av disipliner og linjer.



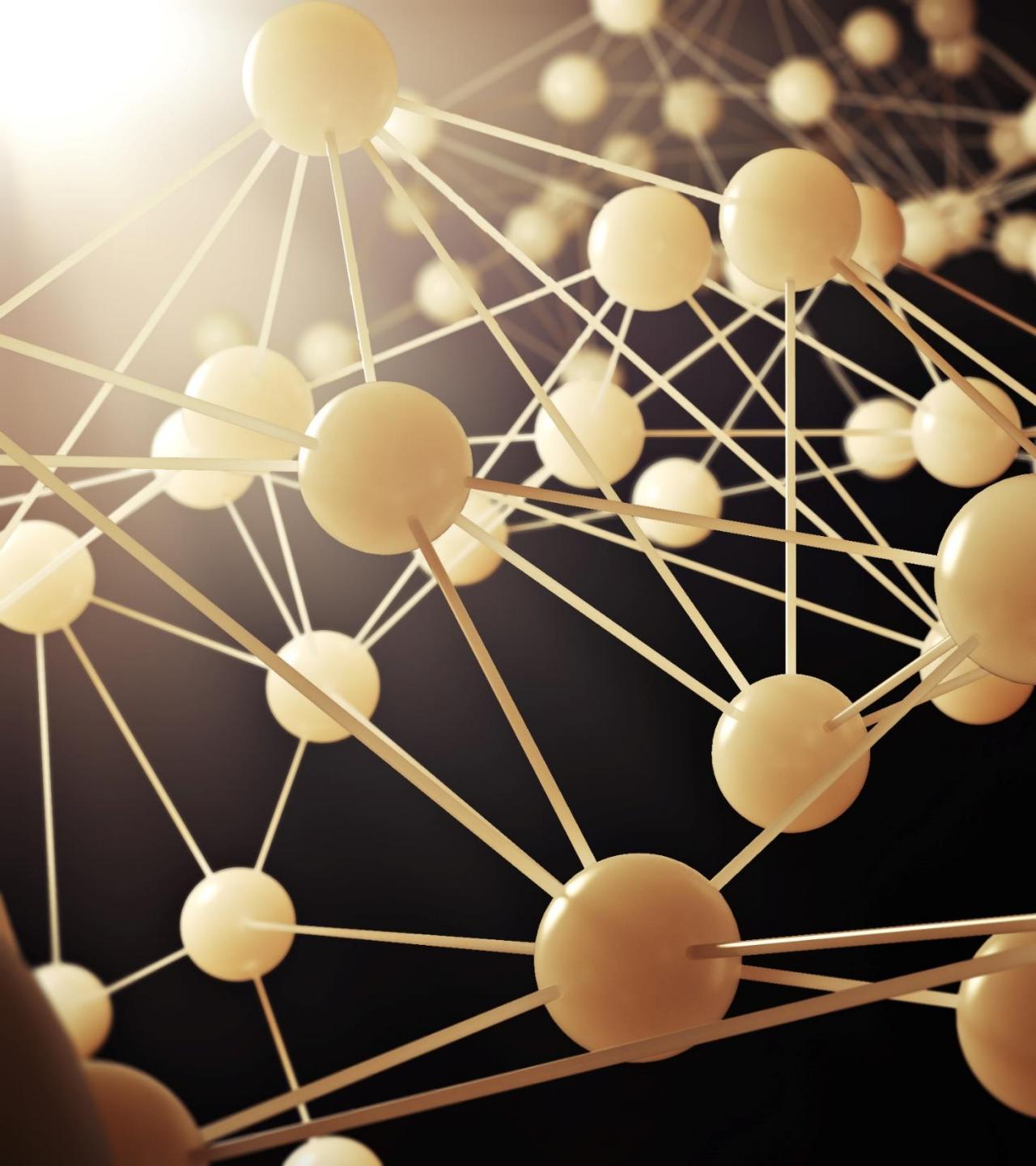
På toppen av dette  
har vi kollektivt en  
**ganske dårlig  
forståelse**  
for trusselaktørene  
i det digitale rom.



I tillegg finnes  
det ofte heller  
**ingen god  
oversikt**  
over hvilke verdier  
virksomheten består av.

Strategier og planer. Data og informasjon. Prosesser.

IKT-systemer, tjenester og applikasjoner. Folk.



Så hvordan kan vi  
**beskytte oss**

når vi ikke skjønner hva som trenger beskyttelse, hvorfor det trenger beskyttelse og hva det trenger å beskyttes mot?

For å repetere:

“

*Risk comes from not  
knowing what you're  
doing.*

– Warren Buffett



Derfor ender vi ofte med  
«Kobra Kai» mot «Karate Kid»



Alt for ofte  
klarer vi ikke  
å forsvare oss slik  
vi burde i 2020.







## Det digitale trusselbildet

# Det finnes grovt sett fire kategorier **trusselaktører:**

- Etterretningsbyråer
- Kriminelle
- Aktivister
- Terrorister

«Innsidere» faller inn under en av de fire andre kategoriene avhengig av motiv og hvem de jobber for.



Det finnes grovt sett  
fem kategorier for  
motivene deres:

- Sabotasje
- Spionasje
- Påvirkning
- Økonomisk vinning
- Infrastruktur

Her vil det ofte være noe overlapp.



For de fleste virksomheter er  
den mest relevante trusselen

# økonomisk motiverte kriminelle



Disse aktørene  
bruker grovt sett  
tre metoder:

- Datainnbrudd
- Sosial manipulering
- Rekruttere en «innsider»

Av og til kan det være overlapp.



For å hente ut økonomisk verdi bruker de som oftest disse fire taktikkene:

- Svindel
- Utpressing
- Digitalt tyveri & bankran
- Misbruk av datakraft

Også her kan det være overlapp.



For øyeblikket er trolig  
målrettet utpressing,  
også omtalt som  
**targeted  
ransomware**  
den farligste trusselen.



«Å beregne **sannsynligheten** for at en alvorlig kriminell handling som terror vil ramme Norge, hvor den vil ramme, og i hvilken form den vil ramme, er en **umulig øvelse.**»

– NSM

«Derfor benyttes det vi kaller en **dimensjonerende trussel**. Med andre ord, hva er det farligste scenario vi er villige til å beskytte oss mot?»

– NSM

# Targeted ransomware

bør absolutt legges til grunn som dimensjonerende trussel.

For dere husker kanskje denne.







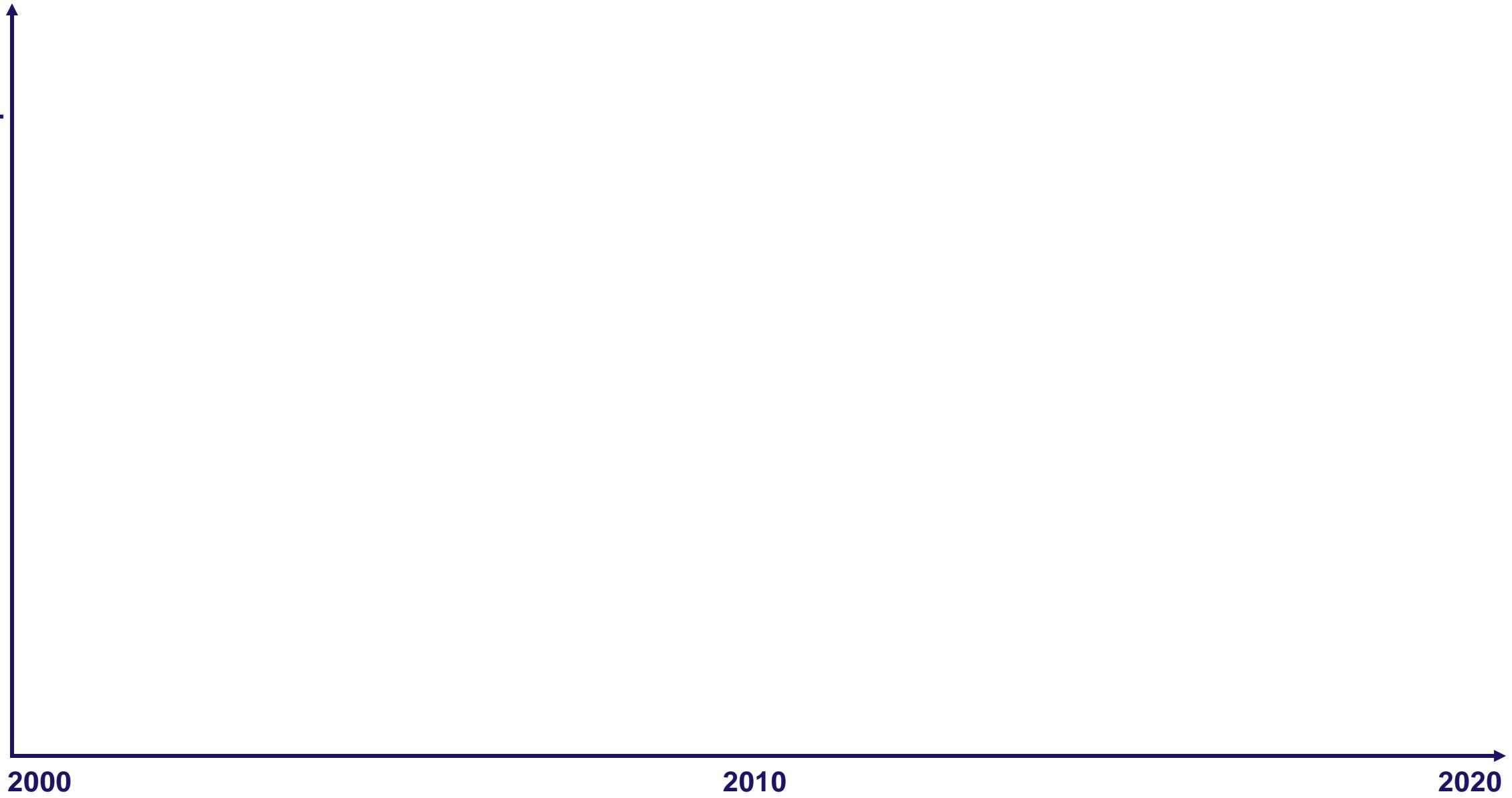
State-of-the-art

Advarsel:

Ikke noen fasit.

Min mening – og det er konseptet som er viktigst, ikke nivåene.

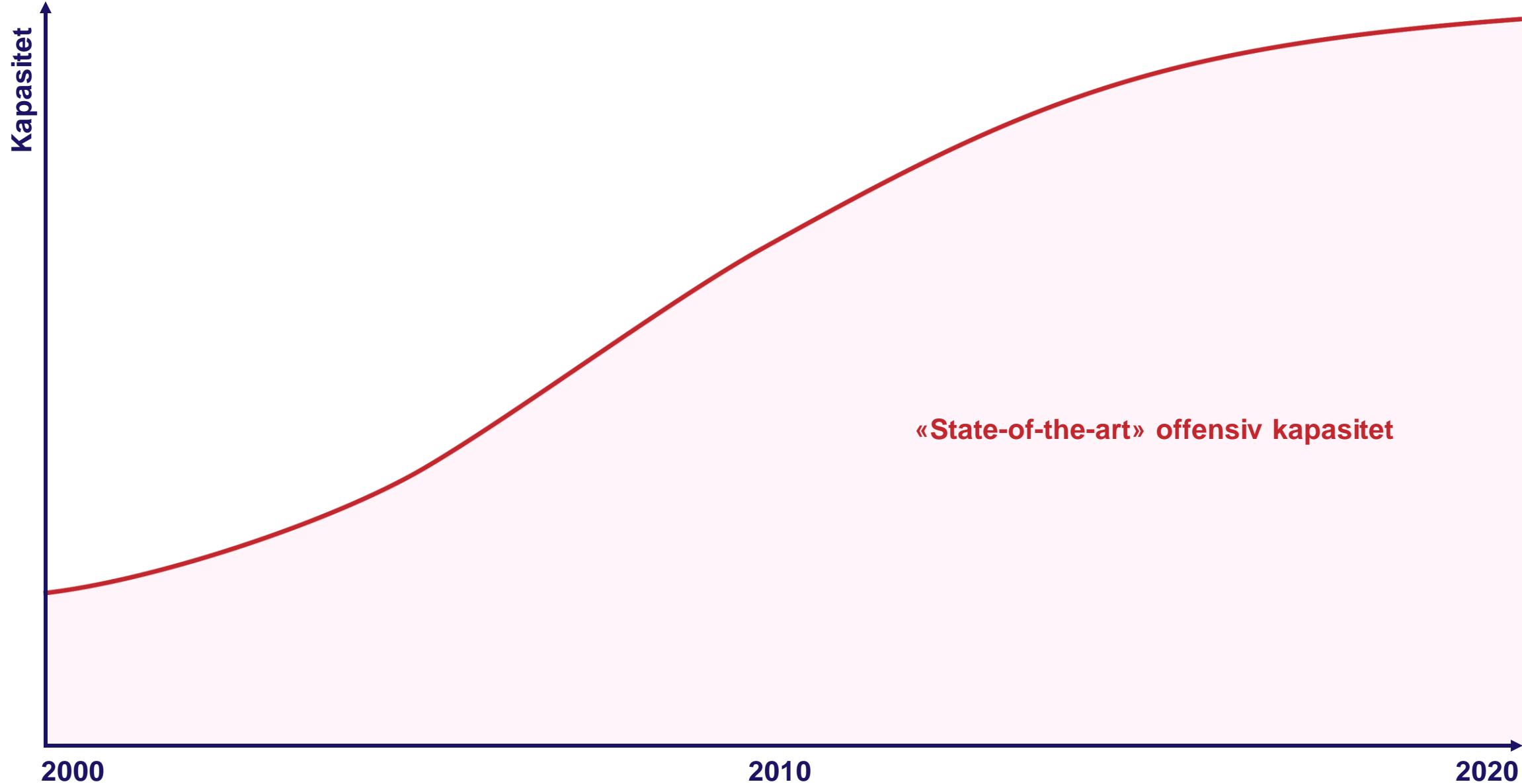
Kapasitet

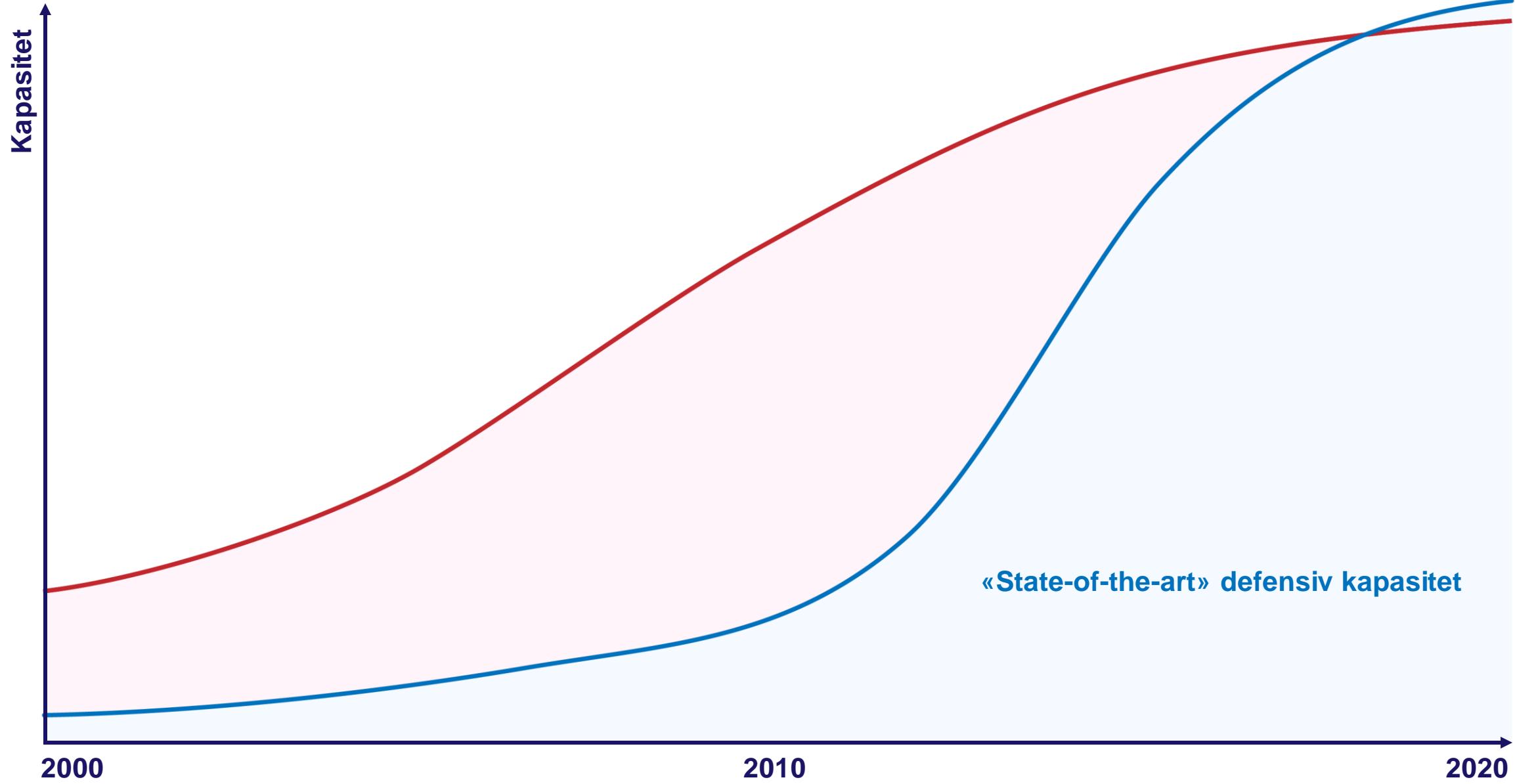


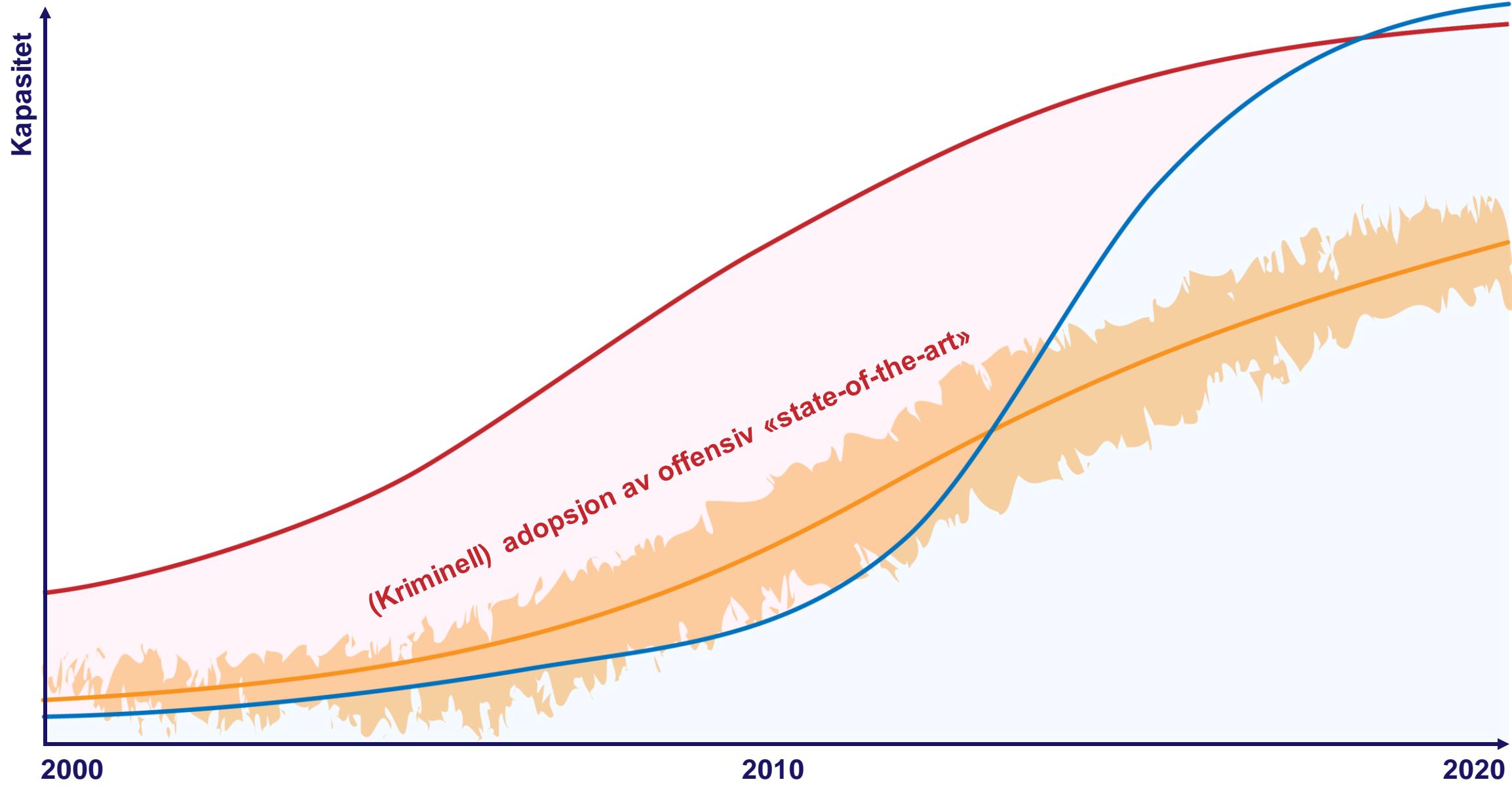
2000

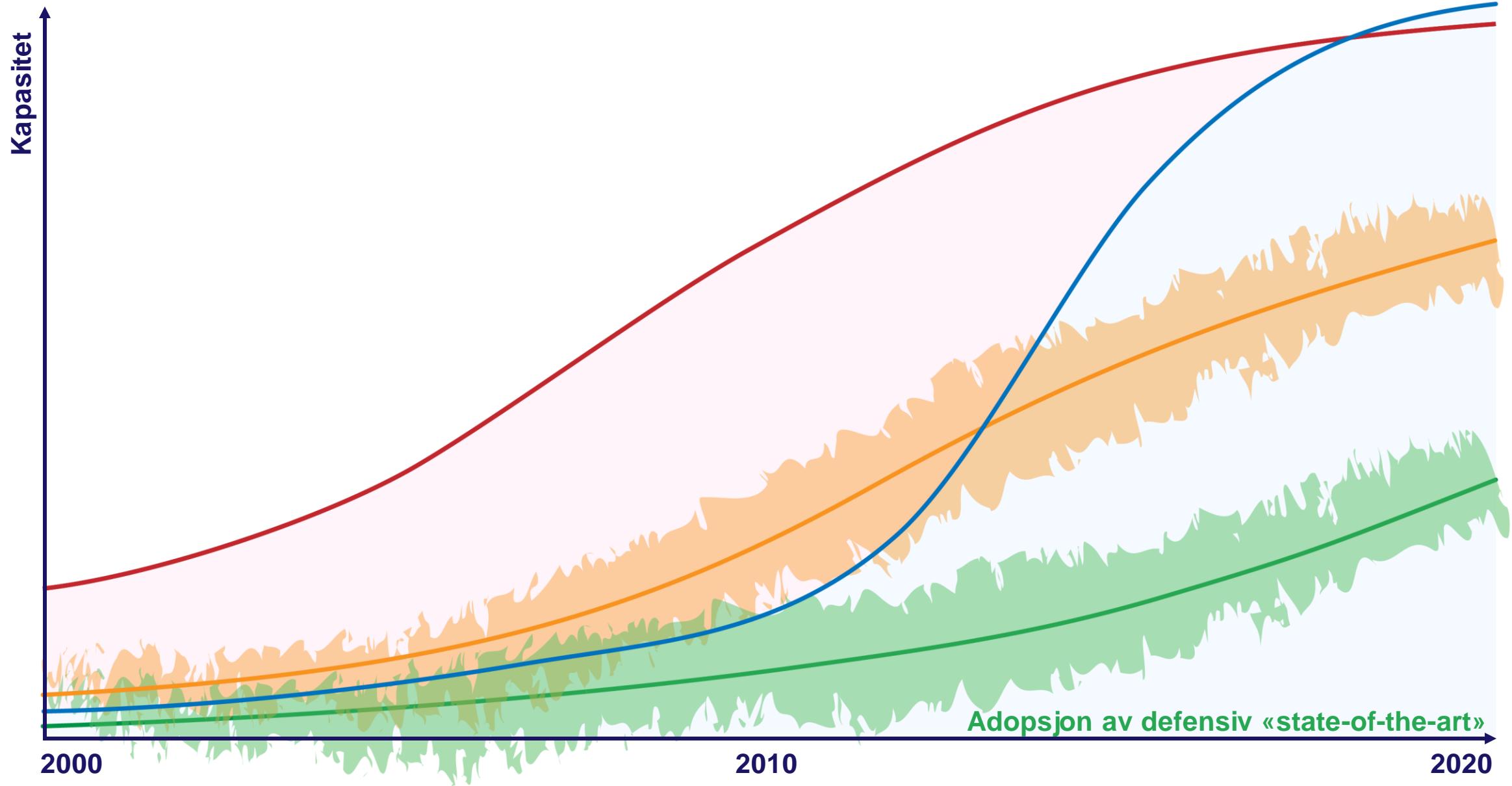
2010

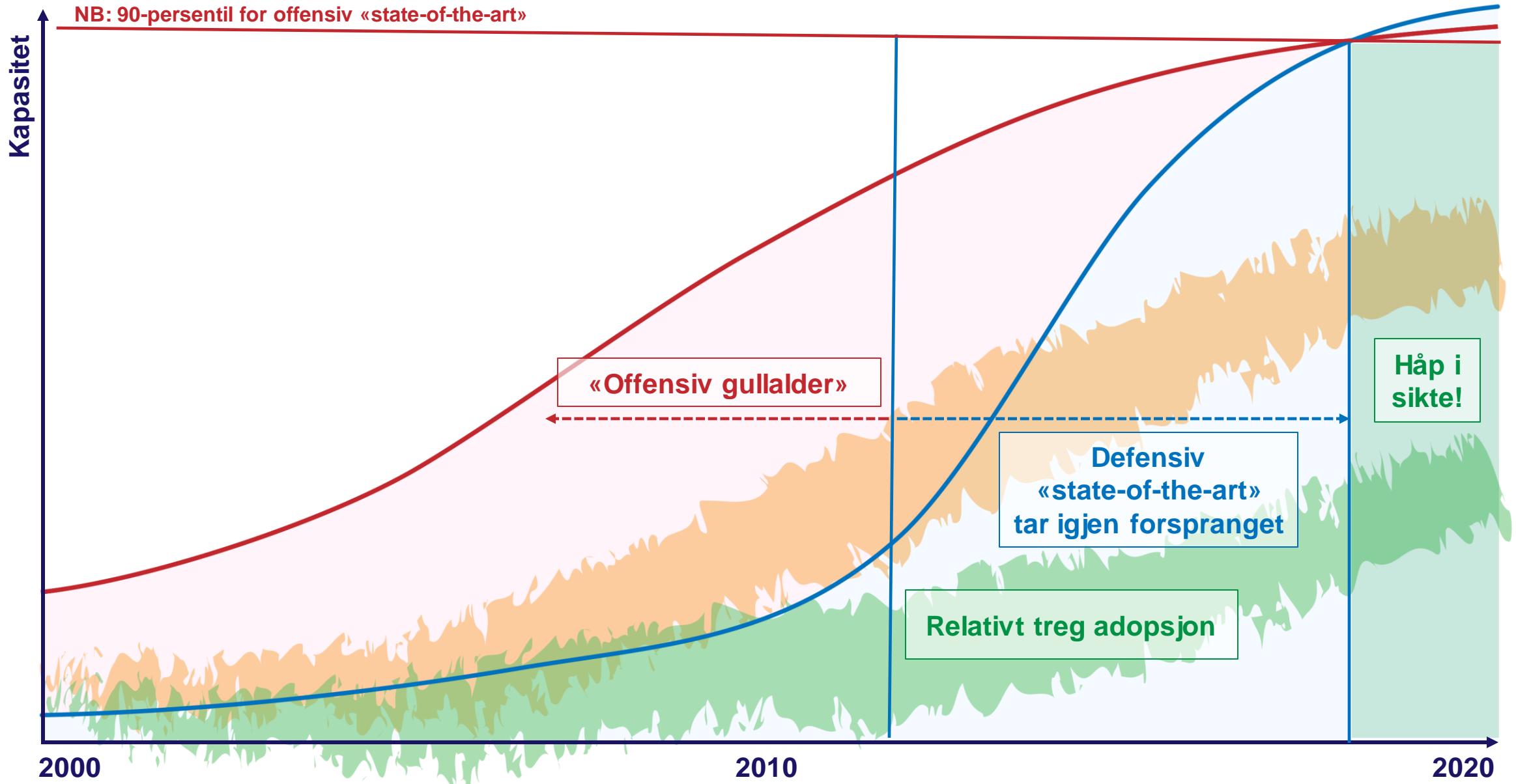
2020

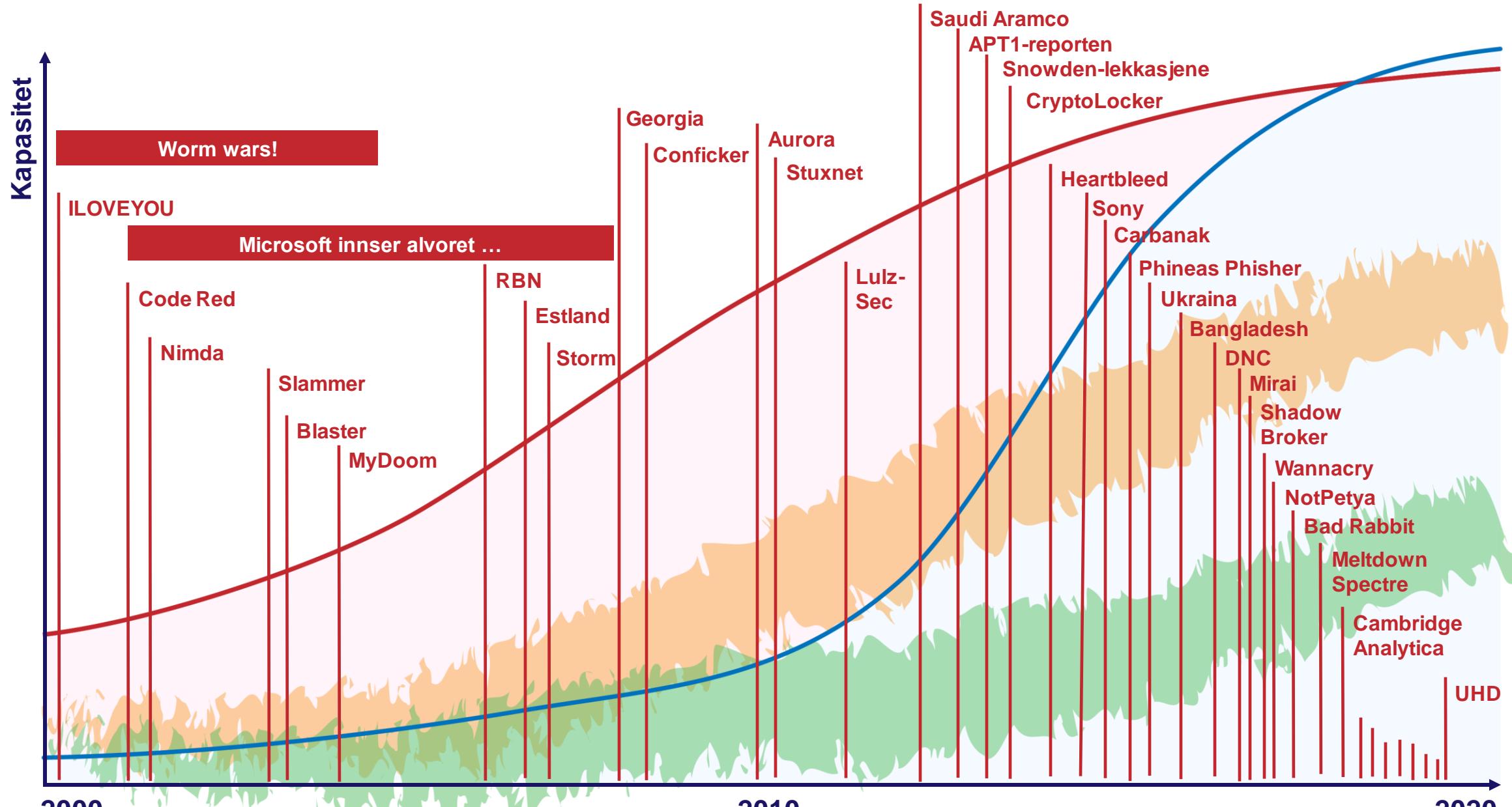










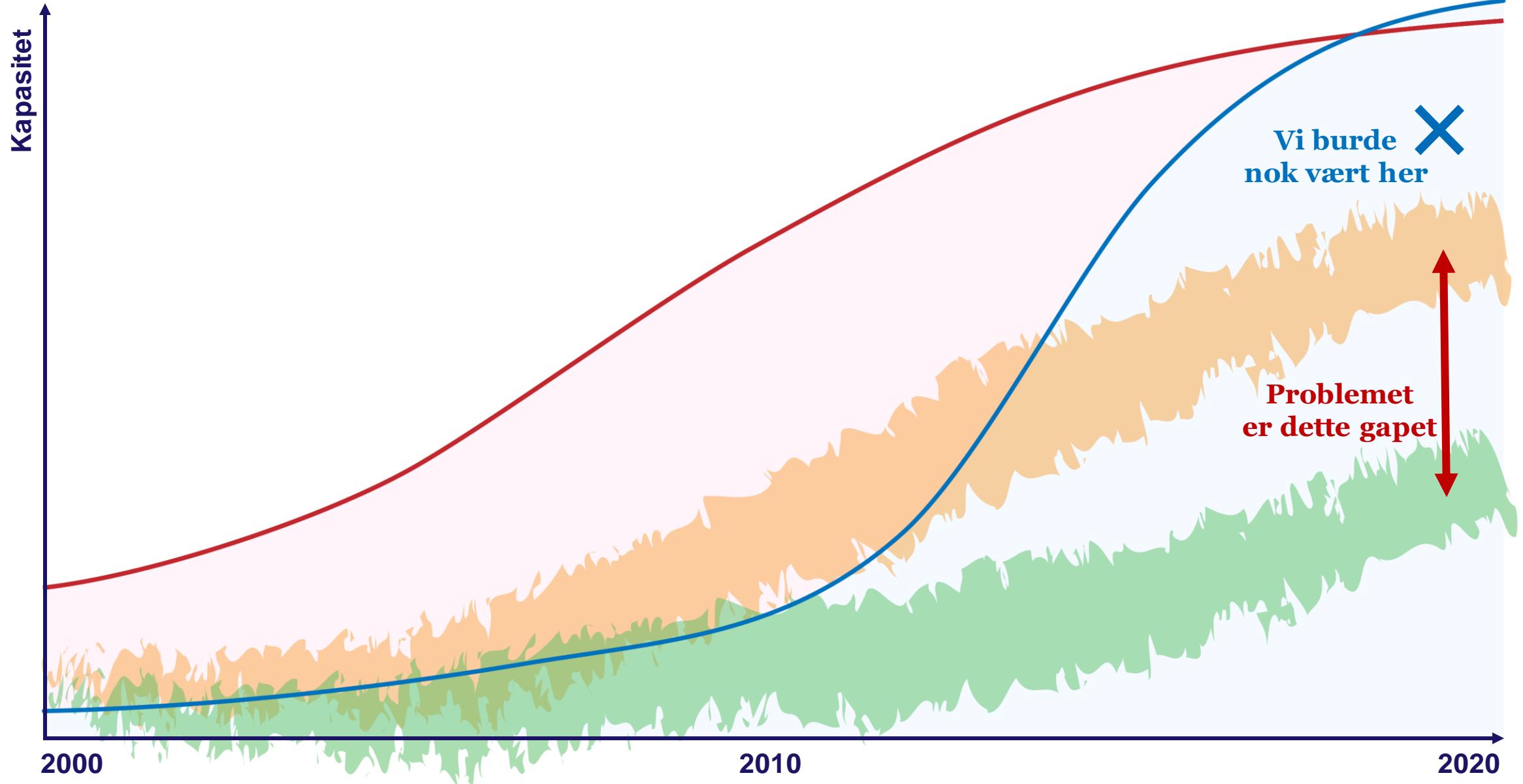


Konklusjon:

Trusselbildet eskalerer

– fortsatt.

Hvordan bekjemper vi et  
så dramatisk trusselbilde?



Mye av tiltakene vi ikke innfører er forebyggende.  
Vi hadde spart mye ressurser dersom vi hadde vasket våre digitale hender litt oftere.

“

*An ounce of prevention  
is worth a pound of cure.*

– Benjamin Franklin



Dessuten:

Det hjelper ikke  
å bare ha «IT-folk»  
og «GRC-folk» når  
du skal slåss mot  
digitale trusler.

Du må ha dine  
egne «hackere».

Både **røde** og **blå**.





## Oppsummering



Den største digitale  
sikkerhetsutfordringen  
vi møter som samfunn  
er ikke truslene.

Det er at vi ikke  
gjør en bedre jobb  
med å sikre oss.



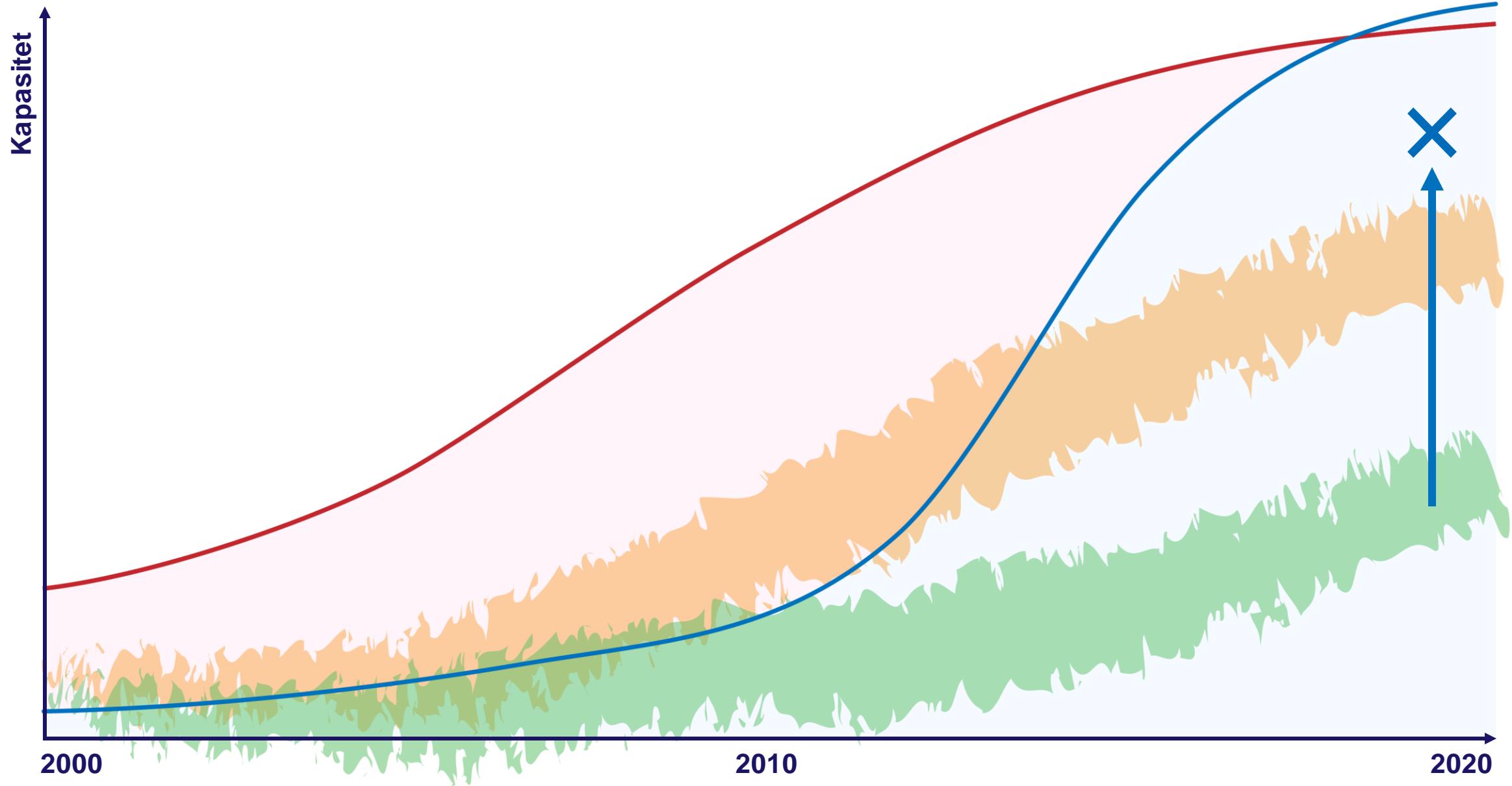
Dessverre viser  
det seg gjentatte  
ganger at **veien**  
til god sikkerhet  
for mange både er  
**lang og humpete.**



## VIKTIG MELDING:

Uten nok FART langs denne veien  
vil man heller aldri klare å ta igjen

kriminell adopsjon av  
offensiv state-of-the-art.



Dessverre viser  
det seg gjentatte  
ganger at **veien**  
til god sikkerhet  
for mange både er  
**lang og humpete.**





**pwc.no/cyber**  
*Fra serverrom til styrerom*

Vår ønske i PwC er  
å kunne bidra til at  
flere virksomheter  
lykkes med den  
reisen, på vei mot  
et sikrere samfunn.



# Lykke til og takk for oppmerksomheten

**Frode Hommedal**  
Teknisk direktør  
[pwc.com](http://pwc.com)

Ta gjerne kontakt dersom du har  
**spørsmål eller kommentarer.**

**Twitter:** @FrodeHommedal  
**Hashtag:** #Digital2020

**frode.hommedal@pwc.com**

© 2020 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.