Dubex:

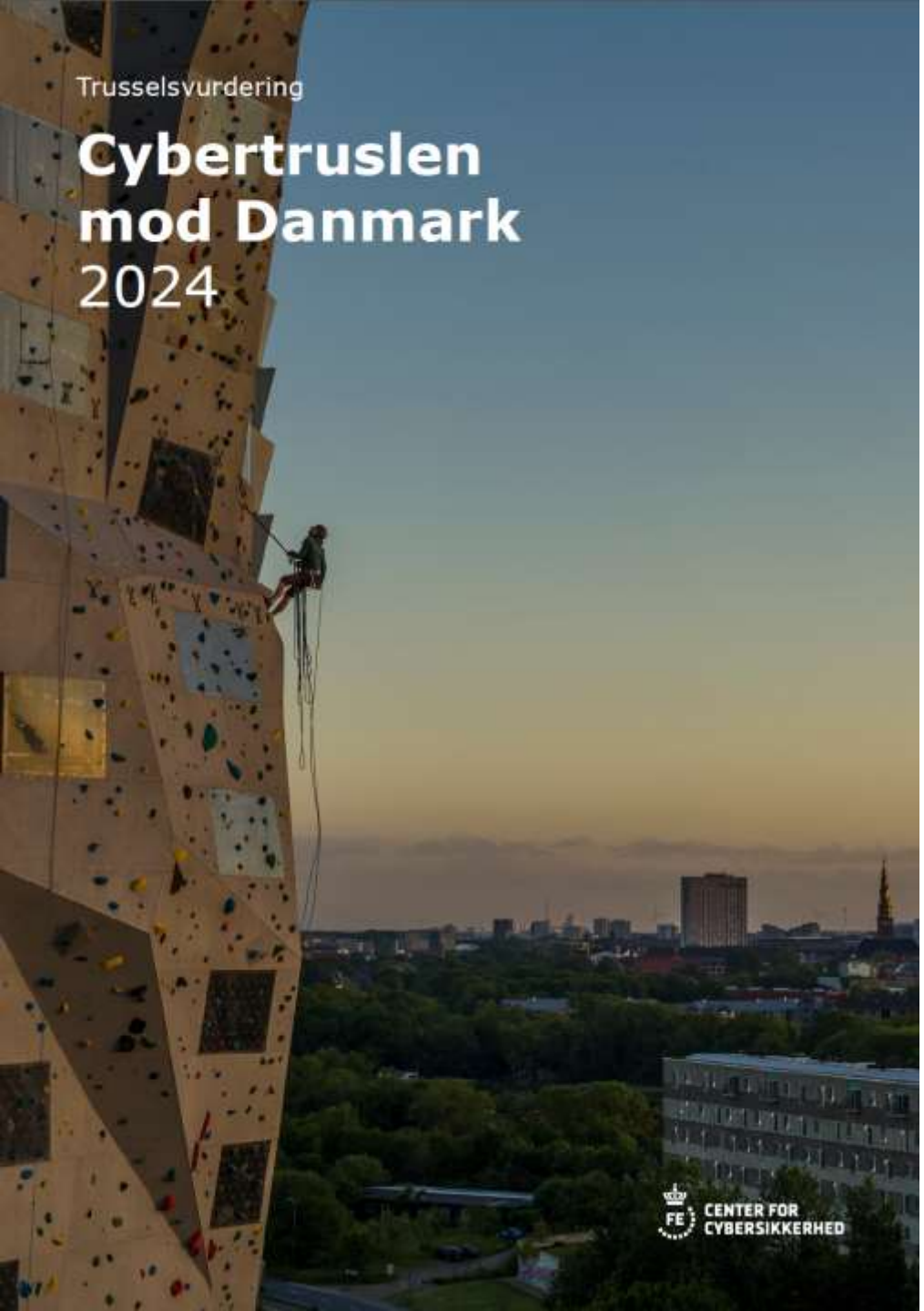
KL’s Dialogforum for it-leverandører og konsulenthuse

Cybersikkerhed i Kommuner

Jacob Herbst, CTO, Dubex A/S

KL’s Mødecenter

Den 22. november 2024



HOVEDVURDERING

- TRUSLEN FRA CYBERSPIONAGE MOD DANMARK ER **MEGET HØJ**

  Organisationer med viden om dansk udenrigs- og sikkerhedspolitik er særligt udsatte. Også dansk kritisk infrastruktur og Forsvaret er i fremmede staters søgelys, når de udfører cyberspionage.

  Truslen fra cyberspionage mod Danmark kommer primært fra Rusland og Kina. Begge stater har betydelige cyberkapaciteter, som de bl.a. bruger til at udføre cyberspionage mod mål i Danmark og udlandet.

- TRUSLEN FRA CYBERKRIMINALITET MOD DANMARK ER **MEGET HØJ**

  Cyberkriminalitet rammer bredt og alle dele af samfundet.

  CFCS vurderer, at der i 2023 var flere ransomware-tilfælde i Danmark end hidtil, og at det også gælder internationalt.

- TRUSLEN FRA CYBERAKTIVISME MOD DANMARK ER **HØJ**

  Cyberaktivistiske angreb, der løbende har ramt danske mål, understreger, at truslen mod danske virksomheder og myndigheder er blevet en del af normalbilledet.

  Truslen fra cyberaktivisme mod Danmark udspringer primært fra pro-russiske cyberaktivister. CFCS vurderer, at nogle pro-russiske cyberaktivister har forbindelse til den russiske stat.

- TRUSLEN FRA DESTRUKTIVE CYBERANGREB MOD DANMARK ER **MIDDEL**

  Truslen kommer primært fra russiske statslige hackere. Det er dog mindre sandsynligt, at Rusland i den nuværende situation vil gennemføre destruktive cyberangreb mod Danmark, hvor hensigten er at skabe alvorlige og omfattende konsekvenser for samfundsvigtige funktioner.

  Flere fremmede stater har kapacitet til at udføre destruktive cyberangreb mod Danmark. Truslen fra destruktive cyberangreb kan stige med kort eller uden varsel, hvis fremmede staters intentioner om at ramme danske mål ændrer sig.

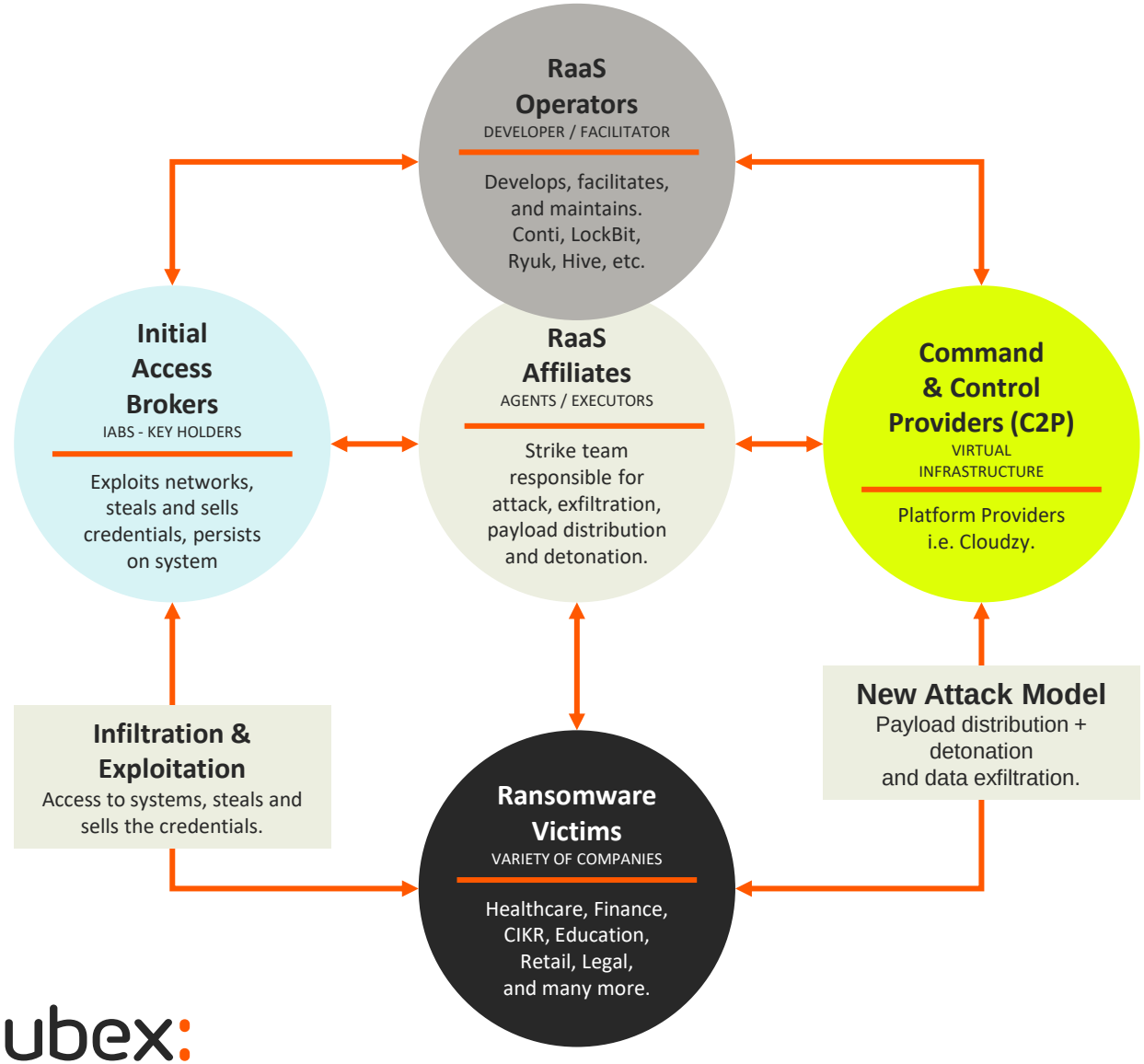
- TRUSLEN FRA CYBERTERROR MOD DANMARK ER **INGEN**

  CFCS har fulgt truslen fra cyberterror siden 2016 med fokus på militante ekstremister og vurderer, at ingen aktører aktuelt har kapacitet til eller intention om at udføre cyberterror mod Danmark.

Udgivelsesdato, 20. september, 2024

https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/

Velorganiserede cyber-kriminelle



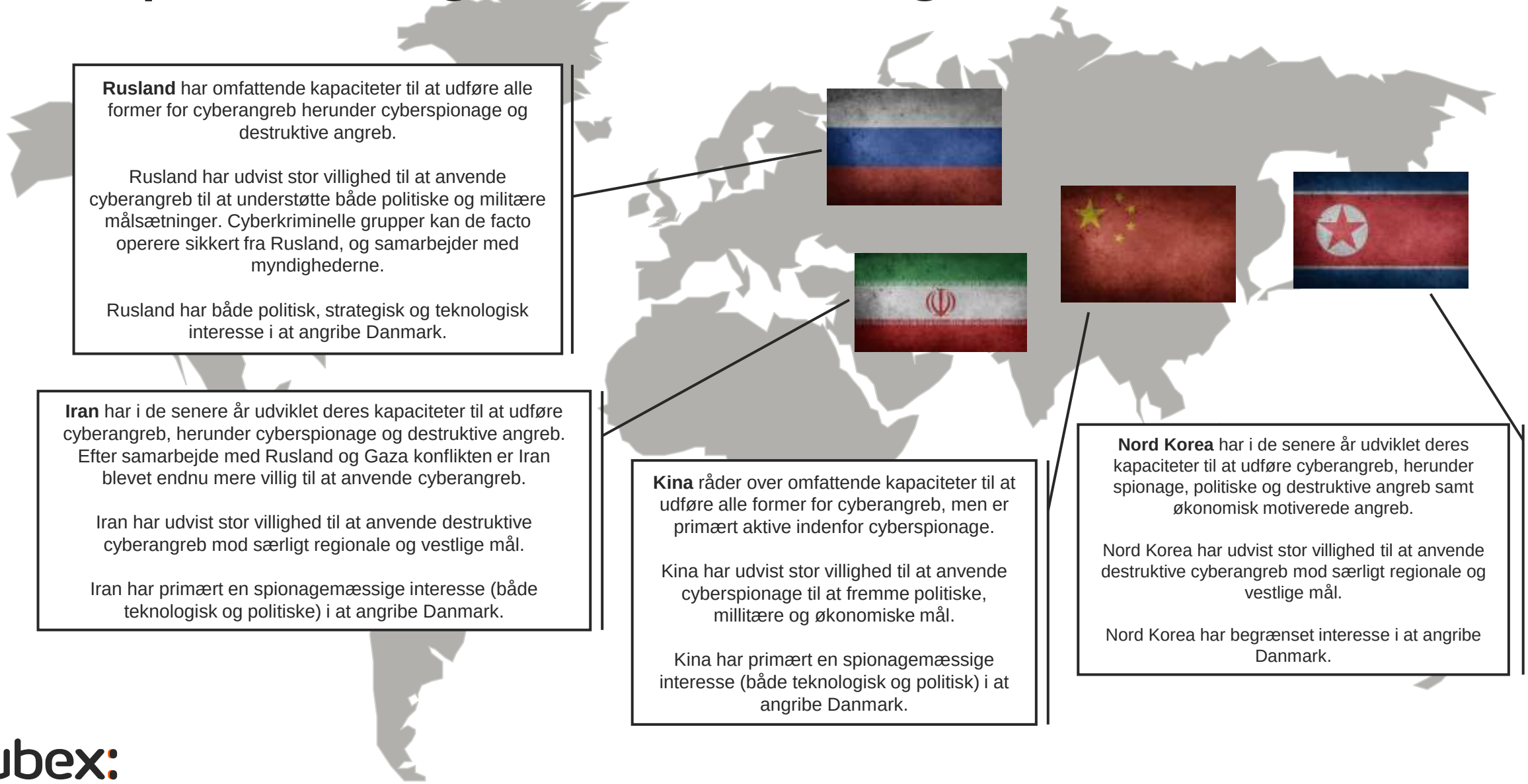
Seksdobbelt afpresning

1. Låsning af data
2. Tyveri af data & trusler om offentliggørelse
3. Denial-of-service angreb
4. Kontakt til kunder og samarbejdspartnere
5. Kontakt til konkurrent for at sælge data
6. Anmeldelse til tilsynsmyndigheder

Chainalysis oplyser, at ransomware-ofre i 2023 betalte hackerne $1.1 milliarder - en ny rekord.

Dubex:

Geopolitik & globale statslige aktører



Rusland har omfattende kapaciteter til at udføre alle former for cyberangreb herunder cyberspionage og destruktive angreb.

Rusland har udvist stor villighed til at anvende cyberangreb til at understøtte både politiske og militære målsætninger. Cyberkriminelle grupper kan de facto operere sikkert fra Rusland, og samarbejder med myndighederne.

Rusland har både politisk, strategisk og teknologisk interesse i at angribe Danmark.

Iran har i de senere år udviklet deres kapaciteter til at udføre cyberangreb, herunder cyberspionage og destruktive angreb. Efter samarbejde med Rusland og Gaza konflikten er Iran blevet endnu mere villig til at anvende cyberangreb.

Iran har udvist stor villighed til at anvende destruktive cyberangreb mod særligt regionale og vestlige mål.

Iran har primært en spionagemæssige interesse (både teknologisk og politiske) i at angribe Danmark.

Kina råder over omfattende kapaciteter til at udføre alle former for cyberangreb, men er primært aktive indenfor cyberspionage.

Kina har udvist stor villighed til at anvende cyberspionage til at fremme politiske, millitære og økonomiske mål.

Kina har primært en spionagemæssige interesse (både teknologisk og politisk) i at angribe Danmark.

Nord Korea har i de senere år udviklet deres kapaciteter til at udføre cyberangreb, herunder spionage, politiske og destruktive angreb samt økonomisk motiverede angreb.

Nord Korea har udvist stor villighed til at anvende destruktive cyberangreb mod særligt regionale og vestlige mål.

Nord Korea har begrænset interesse i at angribe Danmark.

Dubex:

Ruslands cyberoperationsgrupper

- Rusland er en stærk cyberaktør med lang erfaring
- Bred vifte af mål
  - Spionage og rekognosceringsaktiviteter
  - Angreb mod forsyningskæder og service udbydere
  - Målrettede angreb mod kritisk infrastruktur
- Angrebsmetoder - Bruger mange forskellige TTP'er
  - Destruktive malware- og ransomware-operationer
  - DDoS-angreb
- Påvirkning, desinformation og propaganda
- Kombiner forskellige koordinerede angreb i cyber- og fysisk domæne for at nå sine strategiske mål
- I øjeblikket de fleste angreb på Ukraine, risikoen for følgeskader er reel (NotPetya)

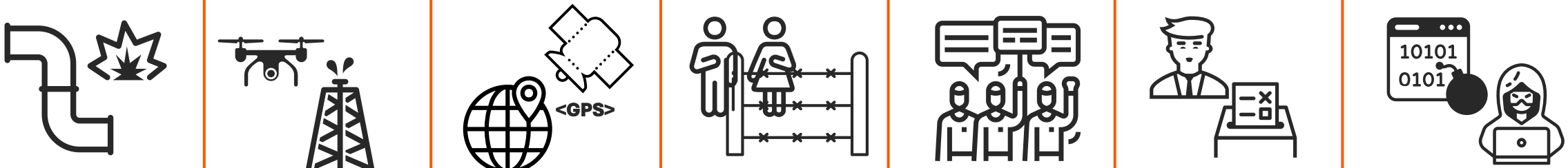
FSO	FSB	SVR	GRU
Russian Federal Protective Service	Federal Security Service of the Russian Federation	Foreign Intelligence Service	Main Directorate of the General Staff
	ACTINIUM Phishing, data theft **BROMINE** Data theft **KRYPTON** Reconnaissance, phishing TURLA	**NOBELIUM APT29** Password spray, phishing (Ukrainian and NATO member diplomatic targets)	**STRONTIUM** Data theft, phishing (military targets) Sandworm **IRIDIUM APT 29** Destruction: FoxBlade wiper; CaddyWiper, Industroer2 **DEV-0586** Destruction: WhisperGate wiper, data theft, influence operations

Cyberkriminelle aktører

Dubex:

Russisk hybridkrig - refleksiv kontrol

Hybridkrig



Sabotage | Intimidering | Chikane | Flygtninge | Protester | Politikere | Cyberangreb

Dubex:

Refleksiv kontrol er et koncept, hvor man påvirker en modstanders beslutninger ved at påtrykke dem antagelser, der ændrer den måde, de handler på

Geopolitik og hybridkrig på Internettet

En ny ustabil og udfordrende geopolitisk virkelighed

Magtfulde lande med autokratiske ledere og geopolitiske ambitioner

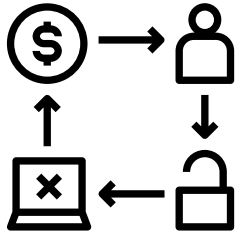
Økonomi, energi og teknologi anvendes som våben

Globalisering i bakgear – kontrol med fokus på kortere supply chains

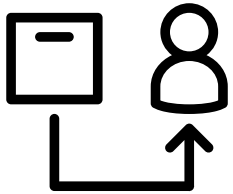
Kriminelle grupper finder beskyttelse i – og hjælper - autokratiske lande

Hybridkrig på Internettet

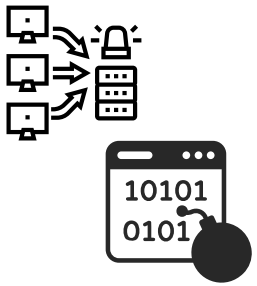
Spionage



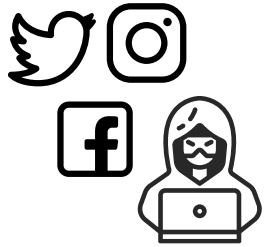
Kriminalitet som våben



Supply Chain



Destruktive angreb



Desinformation & Påvirknings-angreb

Cyberwar

Dubex:

Alle typer orgnaisationer er nødt til at forholde sig til at ændrede geopolitiske forhold også ændre trusselsbilledet væsentligt i negativ retning…

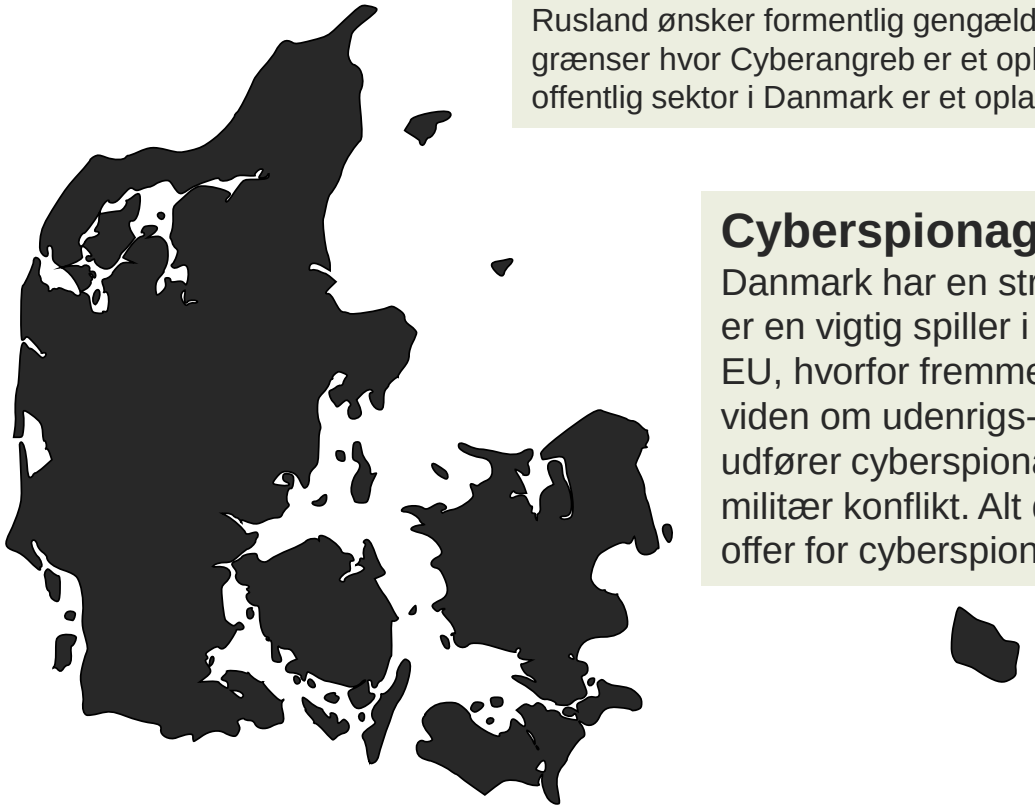
Trusler mod Danmark – offentlig sektor

Kriminelle - afpresning

Kriminelle grupper bliver stadig mere aggressive i deres angreb, hvor særlig forskellige former for ransomware o.a. afpresning typisk anvendes og ofte udløser store økonomiske gevinster til forbryderne. Cyberkriminelle udnytter sårbarheder f.eks. svage passwords eller svagheder i forsyningskæder. Grupperne opererer ofte i samarbejde med eller under beskyttelse af fremmede stater. Offentlige myndigheder og hospitaler anses som oplagte ofre.

Cyberaktivister

Aktivist grupper der gennemfører forskellige former for angreb med fokus på opmærksomhed. Grupperne opererer ofte i samarbejde med eller under beskyttelse af fremmede stater.



Hybride trusler - Russisk hybridkrig mod vesten

Danmark er et af de lande der har støttet Ukraine mest. Udsigt til mulige afslutning af kamphandleringer og USA der trækker sig fra Europa.

Rusland ønsker formentlig gengældelse, at markere sig og afprøve grænser hvor Cyberangreb er et oplagt værktøj til gråzone angreb. Den offentlig sektor i Danmark er et oplagt mål.

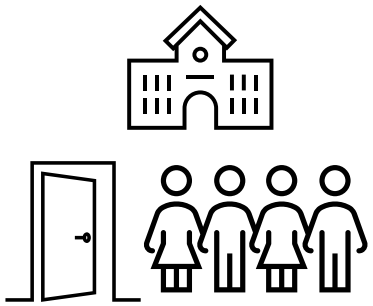
Cyberspionage

Danmark har en strategisk position ved Østersøen, er en vigtig spiller i arktisk og medlem af NATO og EU, hvorfor fremmede stater forsøger at stjæle viden om udenrigs- og sikkerhedspolitik. Rusland udfører cyberspionage for at forberede sig på en militær konflikt. Alt dette gør Danmark til at oplagt offer for cyberspionage

Dubex:

Særlige udfordringer for kommunerne

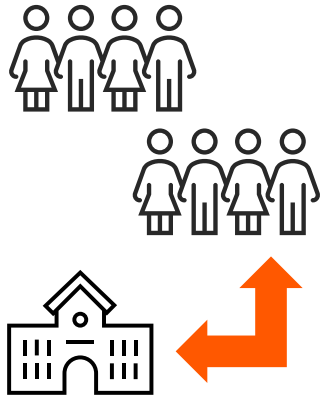
Fysisk sikkerhed



Kommunale institutioner har ofte offentlig adgang og derfor typisk dårlige fysisk sikkerhed sammenlignet med virksomheder.

Det gør det nemt at få adgang til steder hvor der er placeret følsomt it-udstyr.

Troværdighed



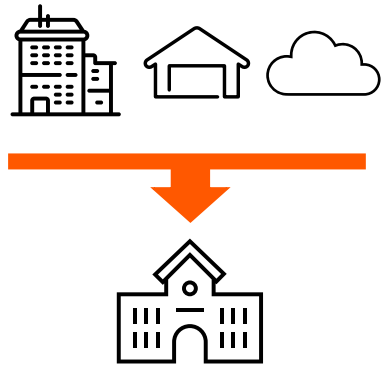
Digitalisering i kommunerne forudsætter at borgerne har tillid til de kommunale it-løsninger.

Hvis tilliden undergraves af kompromittering af personlige data eller utilgængelige systemer forsvinder tilliden

Følsomme data

Kommunerne behandler og opbevare store mængder meget følsomme oplysninger om borgerne, herunder navne, adresser, CPR-numre, helbredsoplysninger som potentielt har stor værdi for kriminelle o.a.

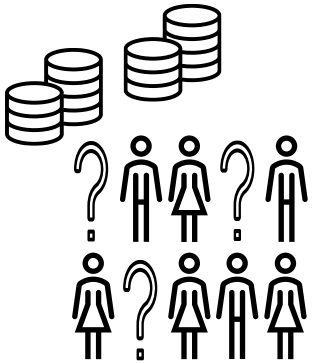
Leverandører



Kommunerne anvender en lang række forskellige it-leverandører til at levere kritiske it-services.

Sikkerheden i forhold til disse services er kritisk for kommunernes samlede it-sikkerhed.

Ressourcer



Kommunerne har begrænsede sikkerhedsbudgetter og underbemandede sikkerhedsafdelinger.

Den offentlige sektor har svært ved at betale konkurrencedygtige lønninger, har ikke tilstrækkeligt med ressourcer og en generel mangel på midler.

Dubex:

Risikoen ved cyberangreb i det offentlig

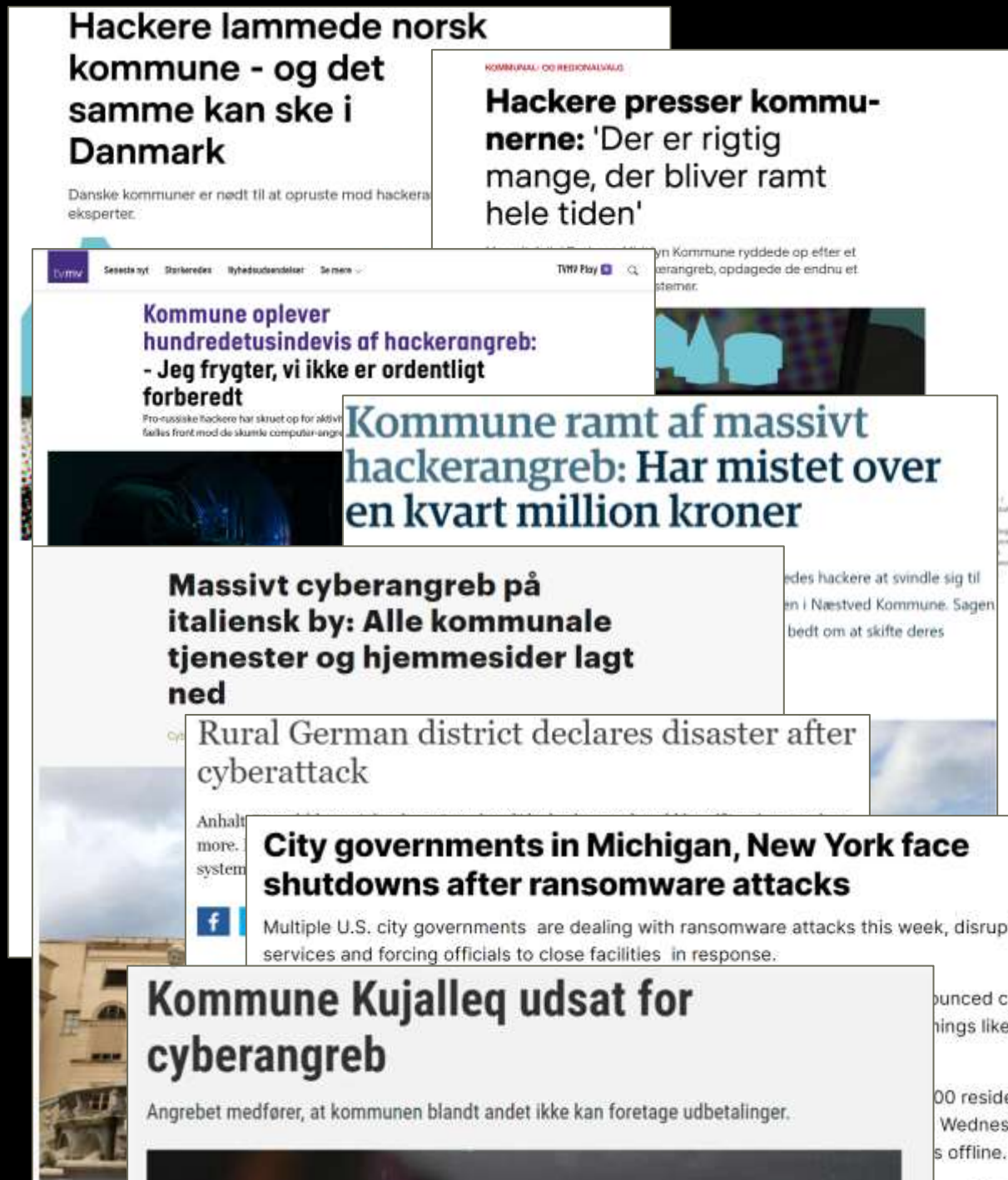
Omkostninger til håndtering af sikkerhedshændelser	**Mistede, stjålne og/eller manipulerede data og personoplysninger**	**Mistet tillid fra borgere til det offentlige – rammer sammenhængskraften i det danske samfund** **Misinformation**
Tab af produktioner og produktivitet	**Kompromittering og offentliggørelse af kritiske data om borgere**	**Mistet mulighed for gevinster ved digitalisering** **Manglende muligheder for at leverer på velfærdsforventninger**
Manglede mulighed for at leverer kritiske services til borgere **Dødsfald**	**Mistede data i systemer der ikke kan reetableres**	**Sikkerhed omkring kritisk infrastruktur og samfundskritiske it-systemer undergraves**

Dubex:

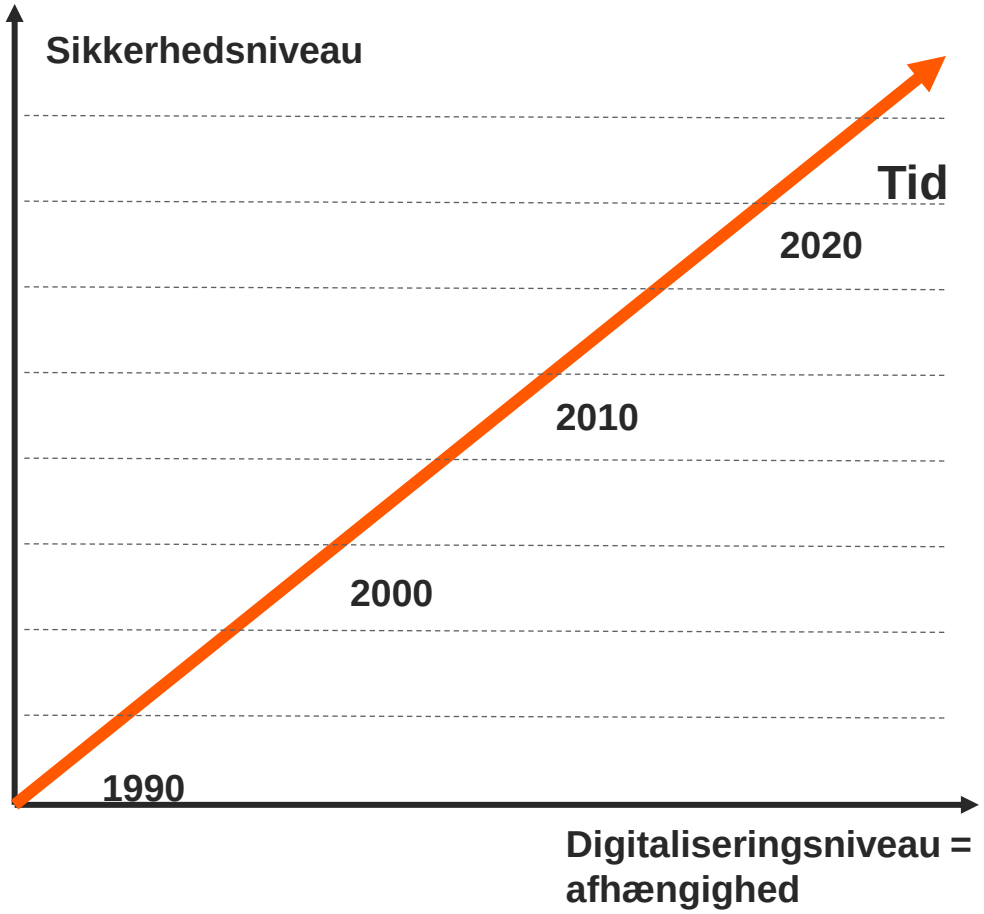
Konsekvenser - kommuner

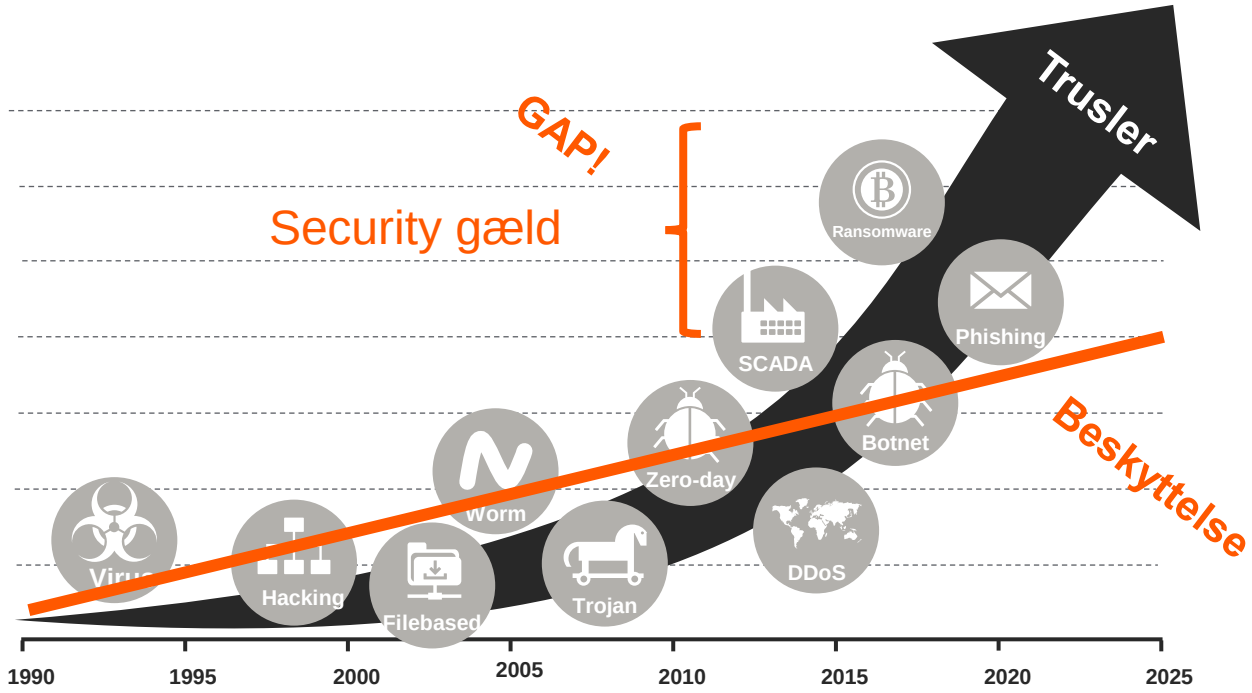
- Manglende mulighed for at yde kerneservices
- Manglende mulighed for sagsbehandling
- Manglende mulighed for håndtere udbetalinger
- Tyveri og læk af personfølsomme oplysninger
- Omkostninger til reetablering og Incident Response
- Tab af tillid fra borgerne til det offentlige

Dubex:



Den aktuelle sikkerhedssituation

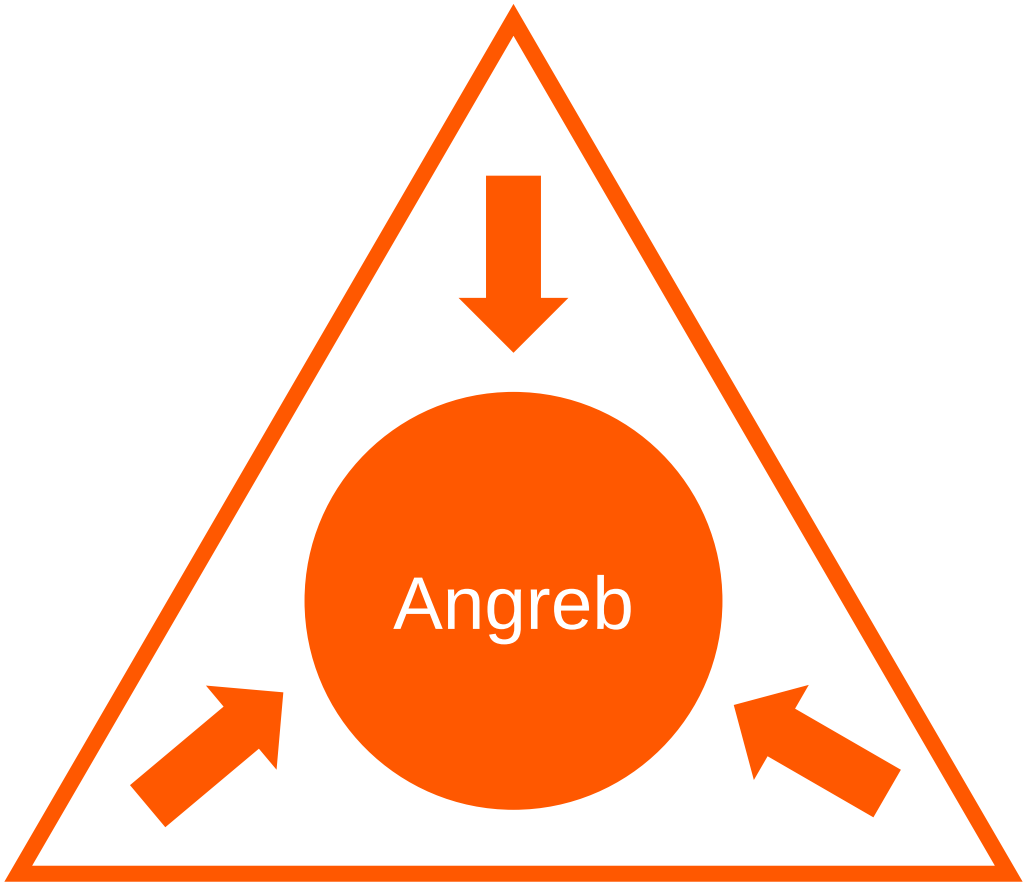




Digitaliseringsniveau og sikkerhedsniveau følges ad … men pt. vokser truslerne hurtigere.

Dubex:

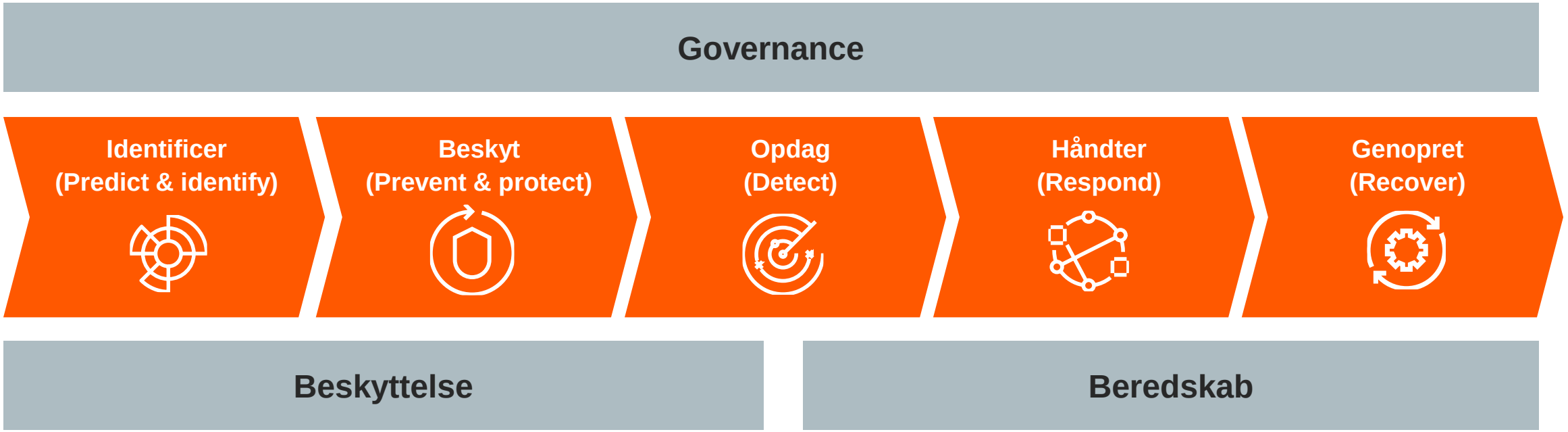
Aktør & motiv



Evner & metoder

Mulighed

Dubex:


Governance
Identificer
(Predict & identify)
Beskyt
(Prevent & protect)
Opdag
(Detect)
Håndter
(Respond)
Genopret
(Recover)
Beskyttelse
Beredskab

Dubex:

NIS2

- Væsentlig forandret trusselsbillede – og større erkendelse af problemet omkring cybersikkerhed

- Omfatter flere sektorer og enheder
- Strenge sanktioner og konkrete højere bøder
- Krav om risikostyring og udvidede krav til sikkerhedsforanstaltninger
- Fokus på at styrke sikkerheden i forsyningskæden

- NIS2 skal harmonisere implementeringen mellem medlemsstaterne

- A European cybersecurity strategy, including the **establishment of a joint Cybersecurity Unit**, a Review of the Security of Network and Information Systems (NIS) Directive[13] and giving a push to the **single market for cybersecurity**.

Krav til sikkerhed i NIS2

Krav til ledelsen (Artikel 20)		Effektiv risikostyring (Artikel 21)				Hændelsesrapportering (Artikel 23)	
Kompetencer	Ansvar	Risikoanalyse & Politikker	Kontroller	Beredskab	Opfølgning	Håndtering	Rapportering

Du

Tak!

Jacob Herbst, CTO

jhe@dubex.dk

+45 2083 0430

AlwaysOn

Cyber attack?

24/7 Incident Response

+45 32 83 04 03

Dubex A/S

Gyngemose Parkvej 50

DK-2860 Søborg

Denmark

www.dubex.dk

+45 3283 0430

info@dubex.dk

Follow us on X (Twitter), LinkedIn and Facebook