Lovtidende A

2022

Udgivet den 29. marts 2022

29. marts 2022. Nr. 381.

Bekendtgørelse om generel og udifferentieret registrering til og med den 29. marts 2023 og opbevaring til og med den 29. marts 2024 af trafikdata

I medfør af § 786 e og § 786 j, stk. 3, i retsplejeloven, jf. lovbekendtgørelse nr. 1835 af 15. september 2021, som ændret ved lov nr. 291 af 8. marts 2022, og efter forhandling med erhvervsministeren fastsættes:

Kapitel 1

Formål og anvendelsesområde

§ 1. Bekendtgørelsen har til formål at fastsætte regler om generel og udifferentieret registrering og opbevaring af trafikdata, idet der foreligger tilstrækkeligt konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, jf. bilag 1.

§ 2. Denne bekendtgørelse finder anvendelse på udbydere som defineret i § 2, stk. 1, nr. 1, i lov om elektroniske kommunikationsnet og -tjenester.

§ 3. Bekendtgørelsen finder ikke anvendelse for transport af radio- og tv-programmer.

§ 4. Bekendtgørelsen finder ikke anvendelse for andelsforeninger, ejerforeninger, antenneforeninger og lignende foreninger eller sammenslutninger heraf, der, inden for foreningen eller sammenslutningen udbyder elektroniske kommunikationsnet eller -tjenester til færre end 100 enheder.

Kapitel 2

Registrerings- og opbevaringspligt

§ 5. Udbydere skal i perioden fra og med den 30. marts 2022 klokken 12.00 til og med den 29. marts 2023 registrere følgende trafikdata om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation, der genereres eller behandles i udbydernes net:

1) Opkaldende nummer (A-nummer) samt navn og adresse på abonnenten eller den registrerede bruger.
2) Opkaldte nummer (B-nummer) samt navn og adresse på abonnenten eller den registrerede bruger.
3) Ændring af opkaldte nummer (C-nummer) samt navn og adresse på abonnenten eller den registrerede bruger.
4) Kvittering for modtagelse af meddelelser.
5) Identiteten på det benyttede kommunikationsudstyr (IMSI- og IMEI-numre).
6) Den eller de celler en mobiltelefon er forbundet til ved kommunikationens start og afslutning, samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen.
7) Tidspunktet for kommunikationens start og afslutning.

§ 6. Ud over de oplysninger, der er nævnt i § 4 i bekendtgørelse om generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet, skal udbydere i perioden fra og med den 30. marts 2022 klokken 12.00 til og med den 29. marts 2023 registrere følgende oplysninger om egne e-mail-tjenester:

1) Afsendende e-mailadresse.
2) Modtagende e-mailadresse.

§ 7. En udbyder skal i perioden fra og med den 30. marts 2022 klokken 12.00 til og med den 29. marts 2023 registrere følgende trafikdata om udbyderens egne internettelefonitjenester, der genereres eller behandles i udbydernes net:

1) Den tildelte brugeridentitet. Herved forstås et kundenummer, abonnementsnummer eller lignende oplysning, der identificerer slutbrugeren over for udbyderen under adgangen til internettet.
2) Den brugeridentitet og det telefonnummer, som er tildelt kommunikationer, der indgår i et offentligt elektronisk kommunikationsnet. Ved brugeridentitet forstås her alle de identificerende oplysninger, som udbyderen tildeler slutbrugeren under adgangen til internettet, herunder internetprotokol-adresse, source-portnummer og andre identificerende oplysninger.
3) Navn og adresse på den abonnent eller registrerede bruger til hvem en internetprotokol-adresse, en brugeridentitet eller et telefonnummer var tildelt på tidspunktet for adgangen.
4) Tidspunktet for kommunikationens start og afslutning.

§ 8. Kan de oplysninger, der er nævnt i §§ 5, 6 og 7, registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne.

§ 9. Registrering og opbevaring af de oplysninger, der er nævnt i §§ 5, 6 og 7, kan efter aftale med udbyderen

Justitsmin., j.nr. 2021-10-0758

på dennes vegne foretages af en anden udbyder eller af en tredjemand.

§ 10. De oplysninger, der er registreret i medfør af §§ 5, 6 og 7, skal opbevares i 1 år fra registreringstidspunktet.

Kapitel 3

Straf

§ 11. Overtrædelse af §§ 5, 6, 7 og 10 straffes med bøde.

Stk. 2. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Kapitel 4

Ikrafttrædelse

§ 12. Bekendtgørelsen træder i kraft den 30. marts 2022, klokken 12.00.

Stk. 2. Samtidig bortfalder bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen).

Stk. 3. §§ 5-7 ophæves den 30. marts 2023.

Stk. 4. §§ 1-4 og §§ 8-11 ophæves den 30. marts 2024.

Justitsministeriet, den 29. marts 2022

Nick Hækkerup

/ Louise Mariegaard

Bilag 1

Vurdering af muligheden for at fastsætte regler, der pålægger udbydere at foretage generel og udifferentieret registrering og opbevaring af trafikdata

1. Indledning

I medfør af retsplejelovens § 786 e, som indsat ved lov nr. 291 af 8. marts 2022, kan justitsministeren efter forhandling med erhvervsministeren fastsætte regler, der pålægger udbydere at foretage generel og udifferentieret registrering og opbevaring af trafikdata, når der foreligger tilstrækkeligt konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig. Regler om registreringspligt fastsat i medfør af retsplejelovens § 786 e kan fastsættes for en periode på højst ét år ad gangen, jf. bestemmelsens stk. 2, og oplysninger registreret i medfør af de fastsatte regler skal opbevares i ét år, jf. bestemmelsens stk. 3.

Med henblik på at kunne foretage vurderingen af, om der foreligger en alvorlig trussel mod Danmarks nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, har Justitsministeriet anmodet Rigsadvokaten, Politiets Efterretningstjeneste (PET), Center for Terroranalyse (CTA), Forsvarets Efterretningstjeneste (FE) og Center for Cybersikkerhed (CFCS) om at oplyse om relevante forhold, jf. *pkt. 2.*

Herudover har Justitsministeriet ved sin vurdering lagt vægt på indholdet af følgende offentlige analyseprodukter: CTA's Vurdering af terrortruslen mod Danmark 2022 af 29. marts 2022, PET's Vurdering af spionagetruslen mod Danmark af 13. januar 2022, FE's Udsyn: Efterretningsmæssig Risikovurdering 2021 af 21. december 2021, CFCS' Vurdering af Cybertruslen mod Danmark 2021 af 7. juni 2021 samt CFCS' Vurdering af Cybertruslen mod Danmark i lyset af Ruslands invasion af Ukraine af 15. marts 2022.

2. Bidrag til trusselsvurderingen fra Rigsadvokaten, Politiets Efterretningstjeneste, Center for Terroranalyse, Forsvarets Efterretningstjeneste og Center for Cybersikkerhed

Rigsadvokaten har over for Justitsministeriet oplyst, at Rigsadvokaten til brug for vurderingen har gennemført datatræk fra politiets sagsstyringssystem (POLSAS) om igangværende og afsluttede sager om overtrædelse af straffelovens kapitel 12 og 13.

Rigsadvokaten har på den baggrund oplyst følgende:

”Af tabel 1-3 nedenfor fremgår oplysninger om antallet af personer, der i perioden fra og med 1. januar 2010 til og med 31. december 2021 er registeret med en sigtelse, tiltale eller dom for overtrædelse af en eller flere bestemmelser i straffelovens kapitel 12 og 13. Opgørelsen af personer er fordelt på år, og en person vil alene fremgå det år, hvor sigtelsen, tiltalen eller dommen er registreret i POLSAS. Derudover er opgørelsen fordelt på henholdsvis spionagesager, terrorsager og øvrige sager. Det bemærkes, at spionagesager omfatter sager vedrørende overtrædelse af straffelovens § 107 og/eller § 108, terrorsager omfatter sager vedrørende overtrædelse af straffelovens §§ 114-114 j, og øvrige sager omfatter sager vedrørende overtrædelse af øvrige bestemmelser i straffelovens kapitel 12 og 13. Det bemærkes, at eventuelle sigtelser i verserende sager, hvor sigtelsen ikke har været oplæst i offentligt retsmøde, som udgangspunkt ikke indgår i opgørelsen. Dette kan f.eks. være tilfældet, hvis der på et tidligt tidspunkt i efterforskningen er afgørende hensyn til fremmede magter eller til sagens opklaring.

Opgørelserne er behæftet med en vis usikkerhed, da POLSAS er et journaliserings- og sagsstyringssystem og ikke et egentligt statistiksystem. Det skal bemærkes, at opgørelserne er baseret på dynamiske data, hvilket betyder, at opgørelserne ikke er endelige. Således vil der kunne ske ændringer afhængigt af tidspunktet for udtrækket af oplysningerne i opgørelserne, idet der f.eks. kan forekomme efterregistreringer. Afgørelser er opgjort efter seneste afgørelse, hvortil afgørelsen kan være anket i mellemtiden. Derfor er afgørelserne ikke nødvendigvis endelige.

Data er opdateret den 12. februar 2022.

Tabel 1 – Antal personer sigtet for overtrædelse af straffelovens kapitel 12 og 13 i perioden fra og med 1. januar 2010 til og med 31. december 2021

	2010	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
Spionagesager	1	-	-	-	-	-	-	-	4	-	5	3
Terrorsager	10	7	13	5	6	8	23	18	5	27	11	42
Øvrige sager	3	4	2	3	4	2	-	1	2	3	2	9
Antal personer sigtet i alt	**14**	**11**	**15**	**8**	**10**	**10**	**23**	**19**	**11**	**30**	**15**[1]	**53**[2]

[1] Tre personer er sigtet for såvel spionage som terrorisme. De tre fremgår derfor både under spionage og terrorisme, men er kun talt med en gang i totalen.

[2] En person er sigtet for terrorisme og for øvrige sager. Den pågældende fremgår derfor både under terrorisme og øvrige sager, men er kun talt med en gang i totalen.

Tabel 2 – Antal personer tiltalt for overtrædelse af straffelovens kapitel 12 og 13 i perioden fra og med 1. januar 2010 til og med 31. december 2021

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Spionagesager	-	-	1	-	-	-	-	-	-	-	2	3
Terrorsager	3	7	2	12	3	2	5	9	6	6	1	11
Øvrige sager	2	1	-	-	1	-	-	-	2	-	2	-
Antal personer tiltalt i alt	**5**	**8**	**3**	**12**	**4**	**2**	**5**	**9**	**8**	**6**	**5**	**11**[3]

[3] Tre personer er sigtet for såvel spionage som terrorisme. De tre fremgår derfor både under spionage og terrorisme, men er kun talt med en gang i totalen.

Tabel 3 – Antal personer dømt for overtrædelse af straffelovens kapitel 12 og 13 i perioden fra og med 1. januar 2010 til og med 31. december 2021

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Spionagesager	-	-	1	-	-	-	-	-	-	-	-	2
Terrorsager	2	4	5	3	3	-	5	4	6	6	1	10
Øvrige sager	3	1	1	2	-	-	-	-	-	-	2	1
Antal personer dømt i alt	**5**	**5**	**7**	**5**	**3**	**-**	**5**	**4**	**6**	**6**	**3**	**13**

Der er i 2021 bl.a. rejst sigtelse mod 13 personer i en sag om planlægning af et eller flere terrorangreb. Flere personer i sagen er sigtet for at have anskaffet sig ingredienser og komponenter til fremstilling af sprængstof og våben. Desuden er flere personer i perioden bl.a. sigtet for at have tilsluttet sig Islamisk Stat (IS) i forbindelse med konflikten i Syrien.

Der er også i 2021 bl.a. rejst tiltale mod tre personer for at have samarbejdet med en udenlandsk efterretningstjeneste, for at have fremmet virksomheden for to terrorbevægelser i Iran og for direkte eller indirekte at have tilvejebragt eller indsamlet midler til en terrorbevægelse. De tiltalte er desuden tiltalt for yderligere forhold vedrørende terrorfinansiering og billigelse af terrorhandlinger. Endelig er en af de tre personer tiltalt for at have trænet, instrueret eller på anden måde oplært en fjerde person til at begå terrorhandlinger.

Derudover er der i perioden bl.a. rejst tiltale mod to personer for forsøg på terrorisme ved i forening at have forsøgt at købe to skydevåben med ammunition mv. til brug for en eller flere terrorhandlinger.

De 13 domfældelser i 2021 omhandler bl.a. flere sager vedrørende fremme af IS' virksomhed. Derudover er der i perioden afsagt dom i en sag, hvor den tiltalte blev fundet skyldig i forsøg på terrorisme ved i forening med to andre at have planlagt at fremstille i hvert fald én bombe, som skulle anvendes under et angreb i København på et ukendt sted, ligesom den tiltalte i forening med en anden forud for detoneringen af bomben skulle stikke flere tilfældige personer ned med kniv. Retten

lagde til grund, at tiltalte sympatiserede med IS, og at han var parat til at begå jihad og indstillet på at blive martyr. ”

Center for Terroranalyse (CTA) har over for Justitsministeriet oplyst følgende:

”Vurdering af Terrortruslen mod Danmark (VTD) udgør Center for Terroranalyses (CTA's) samlede vurdering af terrortruslen mod Danmark og danske interesser i udlandet.

CTA vurderer, at terrortruslen mod Danmark fortsat er i niveauet **alvorlig**. Terrortrusselsniveauet afspejler sager og udviklinger i Danmark og udlandet, som samlet har betydning for vurderingen.

Militante islamister stadig udgør den største terrortrussel mod Danmark. Truslen udgår særligt fra personer og netværk, der inspireres af de militant islamistiske terrorgrupper Islamisk Stat (IS) og al-Qaida (AQ). CTA vurderer endvidere, at Talibans magtovertagelse i Afghanistan i sommeren 2021 har givet terrorgrupper, herunder IS og AQ, større mulighed for at opbygge kapacitet lokalt i regionen.

Truslen fra højreekstremister mod Danmark vurderes af CTA desuden til at være i niveauet *generel*, mens truslen fra venstreekstremister vurderes at være *minimal*.

CTA introducerer som noget nyt i VTD 2022 truslen fra antimyndighedsekstremisme, der accepterer og italesætter nødvendigheden af at anvende vold mod eksempelvis folkevalgte, som et selvstændigt fænomen. CTA vurderer, at truslen fra antimyndighedsekstremister er i niveauet *begrænset*.

Endvidere vurderer CTA vedrørende konflikten i Ukraine, at det fortsat er for tidligt at vurdere konsekvenserne heraf for terrortruslen mod Danmark. CTA vurderer dog på nuværende tidspunkt, at konflikten ikke i sig selv har direkte indflydelse på terrortruslen. Konflikten kan dog have afledte effekter, der kan påvirke terrortrusselsbilledet. På kort sigt kan større migrationsstrømme fra Ukraine betyde, at personer, der også kan udgøre en trussel for Danmark, indrejser skjult i strømmene. På længere sigt kan bl.a. tilstedeværelsen af et konfliktområde i Europa, hvor tilgængeligheden af våben må formodes at være høj, eventuelt kunne tiltrække tilrejsende ekstremister, som på sigt også kan udgøre en trussel mod Danmark.

CTA vurderer samlet set, at terrortruslen mod Danmark og danske interesser i udlandet de næste 12 måneder er i niveauet *alvorlig*."

Politiets Efterretningstjeneste (PET) har over for Justitsministeriet oplyst følgende:

> ”Det er PET’s vurdering, at der er en specifik og vedvarende trussel fra fremmede staters efterretningsvirksomhed i Danmark. PET har i de seneste år afdækket flere sager, der vidner om, at en række fremmede stater aktivt udfører efterretningsvirksomhed mod Danmark. Myndighederne i andre vestlige lande har på tilsvarende vis afdækket sager, der viser, at der er en trussel mod deres samfund.
>
> Danmark står over for en bredspektret og kompleks trussel fra fremmede staters efterretningsvirksomhed. Truslen udgår primært fra Rusland, Kina og Iran, men der er også eksempler på, at andre stater udfører efterretningsaktiviteter i Danmark. Den fremmede efterretningsvirksomhed omfatter spionage, herunder cyberspionage, påvirkning, chikane, forsøg på ulovligt at anskaffe produkter, teknologi og viden samt i helt særlige tilfælde likvideringsforsøg.
>
> Danmark er i kraft af sin ofte aktive rolle på den internationale scene og medlemskab af internationale samarbejdsfora som EU, NATO og FN et attraktivt mål for fremmed efterretningsvirksomhed. Hertil kommer, at dansk teknologi og forskning på en række områder er verdensførende og dermed attraktivt at få adgang til.
>
> PET kan konstatere, at politikere, embedsfolk, offentlige myndigheder, dansk forsvar, virksomheder, forskningsinstitutioner, forskere, studerende og dissidenter løbende indgår som mål og/eller midler i fremmede staters efterretningsvirksomhed mod Danmark.
>
> Fremmede staters efterretningstjenester er kendetegnet ved at være professionelle modstandere med en høj kapacitet, der i nogle tilfælde planlægger og gennemfører aktiviteter med en lang tidshorisont. Fremmede efterretningstjenester har ofte mange ressourcer til rådighed, og de udnytter løbende teknologiske fremskridt til at udvikle nye måder at operere både hjemme og i udlandet.
>
> Hvis fremmede stater via spionage får adgang til klassificerede og beskyttelsesværdige informationer, kan det skade Danmarks sikkerhed og handlefrihed. Hvis det drejer sig om informationer, der omhandler Danmarks forhold til andre lande, kan informationerne undertiden bruges både mod Danmark og mod de lande, som vi samarbejder med. Spionage mod virksomheder og forskningsinstitutioner i Danmark kan endvidere skade Dan-

marks konkurrenceevne og føre til tab af indtægter, arbejdspladser og prestige.

PET vurderer endvidere, at truslen fra russiske efterretnings- og påvirkningsaktiviteter mod Danmark aktuelt er uændret i lyset af krigen i Ukraine."

Forsvarets Efterretningstjeneste (FE) og Center for Cybersikkerhed (CFCS) har over for Justitsministeriet oplyst følgende:

"Terrortruslen

Terrortruslen er fortsat alvorlig og kommer især fra militante islamister, men også fra højreekstremister. Al-Qaida og Islamisk Stat inspirerer stadig individer og netværk til angreb i og uden for Europa. Vestlige fremmedkrigere vil fortsat udgøre en trussel. Både al-Qaida og Islamisk Stat har en vedblivende intention om at angribe Vesten, og deres regionale undergrupper udgør en trussel mod vestlige interesser i store dele af verden.

Cybertruslen

Cyberangreb fra både stater og cyberkriminelle er en vedvarende og alvorlig trussel mod Danmark. Truslen hænger ofte sammen med andre sikkerhedspolitiske udfordringer, Danmark står over for. Cyberangreb kan i fremtiden gøre endnu større skade på vores samfund. Det kan eksempelvis ske, hvis det drejer sig om destruktive cyberangreb rettet mod at ødelægge kritisk infrastruktur. Ifølge CFCS er truslen fra cyberkriminalitet og cyberspionage MEGET HØJ. Både cyberkriminelle og medarbejdere hos statslige aktører arbejder systematisk, vedholdende og målrettet på at ramme mål i Danmark.

Truslen fra cyberspionage retter sig især mod danske myndigheder og organisationer, som arbejder med udenrigs- og sikkerhedspolitik i bred forstand. Ved hjælp af cyberspionage kan fremmede stater opnå viden om danske interesser, overvejelser og beslutninger i forbindelse med større internationale sager eller udenrigspolitiske forhandlinger. Den viden kan staterne bl.a. udnytte til at modarbejde danske interesser eller sætte danske forhandlere og beslutningstagere under pres.

Truslen er derudover særligt rettet mod virksomheder, der besidder en viden, som andre stater har interesse i. Cyberspionage retter sig også i nogle tilfælde mod virksomheder og myndigheder, som kan blive værdifulde for fremmede stater at have adgang til i fremtiden. Fremmede stater kan eksempelvis bruge cyberspionage mod virksomheder og myndigheder til at opbygge kapacitet til at kunne gennemføre destruktive cyberangreb

mod dem i forbindelse med en alvorlig konflikt. Det kan f.eks. være i forbindelse med militære konflikter, hvor private virksomheder også spiller en rolle for bl.a. forsyningssikkerheden og militæret. CFCS vurderer dog, at truslen fra destruktive cyberangreb mod danske myndigheder og virksomheder på nuværende tidspunkt er LAV. Det betyder, at det er mindre sandsynligt, at danske virksomheder og myndigheder bliver udsat for forsøg på destruktive cyberangreb inden for de næste to år.

Succesfulde destruktive cyberangreb kan have meget alvorlige konsekvenser, f.eks. i form af afbrudt adgang til samfundsvigtige funktioner, såsom strøm, transport eller internet eller omfattende ødelæggelse af data og enheder. Der er derfor tale om en potentiel trussel, som kan have alvorlige konsekvenser.

Det er mindre sandsynligt, at fremmede stater aktuelt har intentioner om at udføre destruktive cyberangreb mod Danmark. Flere stater har dog kapacitet til at udføre den type angreb. Det betyder, at truslen kan stige, hvis intentionen ændrer sig. Truslen kan ændre sig i forbindelse med en skærpet konflikt eller geopolitiske spændinger mellem Danmark og stater, der har kapacitet til at udføre destruktive cyberangreb.

Påvirkning generelt

Fremmede magter forsøger i stadigt højere grad at udnytte informationsrummet til at påvirke holdninger og adfærd i vestlige demokratier, herunder Danmark. Dette udgør en stigende trussel imod Danmarks offentlige og frie debat. I forsøget på at manipulere den offentlige debat gør statslige aktører brug af en række forskellige påvirkningsmetoder. Kina, Rusland og andre stater bruger falske profiler på sociale medier til at promovere særlige budskaber. Profilerne fremstår ofte som vestlige borgere i forsøg på at skabe en illusion af, at vestlige borger for eksempel støtter russiske og kinesiske mærkesager. Statslige aktører bruger ligeledes vestlige borgere som forstærkere for deres budskaber eller som mellemmænd for påvirkningsoperationer. Endelig kan hack og læk understøtte fremmede staters interesser. Statslige hackere stjæler følsomme oplysninger og lækker dem på strategiske tidspunkter for at påvirke den offentlige mening i Vesten. Lækket kan finde sted op til et valg med henblik på at påvirke udfaldet eller for at skabe splid i en befolkning.

Rusland

Ruslands invasion af Ukraine i februar 2022 understreger Ruslands villighed til offensivt at bruge militære midler til at opnå landets udenrigs- og sikkerhedspolitiske målsætninger. Rusland

skærper derudover konfrontationen med Vesten med offensive efterretningsoperationer, cyberspionage og påvirkning.

Rusland vil fortsat forsøge at udnytte meningsforskelle blandt de europæiske lande til at splitte vestlige alliancer. Rusland vil fortsat forsøge at svække de europæiske landes muligheder for at reagere samlet over for Rusland.

Rusland spionerer målrettet mod Danmark. Rusland bruger et bredt spektrum af metoder, der skal indhente informationer om dansk sikkerhedspolitik og militære forhold. Forskning, råstoffer, søfart, stormagtspolitik og militær tilstedeværelse er blandt de områder, som Rusland interesserer sig for i Arktis. Spionagen sker både gennem brug af cyberangreb, og ved at russiske efterretningstjenester f.eks. hverver kilder og aflytter telefoner. Denne indsats kan udøves af personer eller kilder, der befinder sig fysisk i Danmark.

Ud over at være et mål for den politiske og militære spionage er Danmark som et teknologisk foregangsland også udsat for russisk industrispionage. Industrispionagen bidrager til, at Rusland udvikler sine militære kapaciteter og ville kunne true NATO-alliancens teknologiske overlegenhed i tilfælde af konflikt. Rusland spionerer mod forsvarsindustrien verden over og ses også interesseret i den danske forsvarsindustris viden om militær teknologi og materiel.

Rusland bruger sin efterretningskapacitet i et bredt spektrum af operationer, herunder attentater og sabotageaktioner i vestlige lande. Rusland har kapaciteten til at udføre den type operationer i Danmark. Der er dog ikke en erkendt hensigt om at gennemføre sabotage i Danmark. Rusland har foreløbigt holdt sig til at ramme militær hjælp, mens den er i Ukraine. I tilfælde af at konflikten i Ukraine eskalerer, kan Rusland dog stort set uden varsel ændre tilgang og forsøge at sabotere våbenhjælp i oprindelses- og transitlandene med midler, som gør det vanskeligt at attribuere eventuelle hændelser direkte til Rusland.

Kina

Kinas voksende indflydelse og globale ambitioner skaber spændinger i forholdet til en række vestlige lande, herunder til Danmark. Samtidig søger Kina mere håndfast og offensivt at imødegå kritik af det, landet opfatter som sine indre anliggender. For at understøtte sine strategiske interesser bruger Kina sin økonomiske tyngde til at lægge politisk og økonomisk pres på andre lande, ligesom Kina målrettet anvender cyberspionage til at fremme sine interesser. Danmark rammes også af disse virkemidler.

> Kinas omfattende og vedvarende cyberspionage mod andre lande er også målrettet mod danske myndigheder, virksomheder og organisationer. Kinas militær og kinesiske efterretningstjenester har meget væsentlige kapaciteter og evner til at skaffe sig fuld og vedvarende adgang til organisationers digitale informationer. Der er tale om en konstant og langsigtet aktivitet, der gavner Kinas sikkerheds- og udenrigspolitiske, økonomiske og kommercielle interesser.
>
> Kina arbejder målrettet på at tilegne sig teknologi og viden. Kina ønsker at styrke sin teknologiske udvikling og opnå uafhængighed af udenlandsk teknologi på strategisk vigtige områder. Derfor fokuserer landet på det hjemlige marked og på at udvikle produkter og teknologier, som kinesiske virksomheder lige nu importerer fra udlandet. Kina ønsker på den måde at opnå større kontrol med de vigtigste forsyningskæder, eksempelvis for avancerede computerchips.
>
> Kina har en omfattende indsats, der skal kortlægge og om muligt overføre teknologi og viden til Kina. Til det formål har Kina en række talentprogrammer, som bl.a. skal tiltrække forskere til Kina, og som også har fokus på at øge Kinas forskningsmæssige kompetencer. Det er sandsynligt, at Kina i den forbindelse også ønsker at tilegne sig viden og teknologi fra danske forskningsinstitutioner og virksomheder. ”

3. Vurdering af truslen mod Danmarks nationale sikkerhed fra terror

Justitsministeriet vurderer, at terror udgør en alvorlig, reel og aktuel trussel mod den nationale sikkerhed i Danmark de næste 12 måneder.

Det fremgår således bl.a. af CTA's Vurdering af terrortruslen mod Danmark 2022 af 29. marts 2022, at terrortruslen mod Danmark ligger i niveauet *alvorlig.* Terrortrusselsniveauet afspejler sager og udviklinger i Danmark og udlandet, som samlet har betydning for vurderingen.

Militante islamister udgør stadig den største terrortrussel mod Danmark. Truslen udgår særligt fra personer og netværk, der inspireres af de militant islamistiske terrorgrupper Islamisk Stat (IS) og al-Qaida (AQ).

CTA vurderer endvidere, at Talibans magtovertagelse i Afghanistan i sommeren 2021 har givet terrorgrupper, herunder IS og AQ, større mulighed for at opbygge kapacitet lokalt i regionen.

Truslen fra højreekstremister mod Danmark vurderes af CTA desuden til at være i niveauet *generel*, mens truslen fra venstreekstremister vurderes at være *minimal*.

CTA introducerer som noget nyt i Vurdering af terrortruslen mod Danmark 2022 af 29. marts 2022 truslen fra antimyndighedsekstremisme, der accepterer og italesætter nødvendigheden af at anvende vold mod

eksempelvis folkevalgte, som et selvstændigt fænomen. CTA vurderer, at truslen fra antimyndighedsekstremister er i niveauet *begrænset*.

Endvidere vurderer CTA i forhold til konflikten i Ukraine, at det fortsat er for tidligt at vurdere konsekvenserne heraf for terrortruslen mod Danmark. CTA vurderer dog på nuværende tidspunkt, at konflikten ikke i sig selv har direkte indflydelse på terrortruslen. Konflikten kan dog have afledte effekter, der kan påvirke terrortrusselsbilledet. På kort sigt kan større migrationsstrømme fra Ukraine betyde, at personer, der også kan udgøre en trussel for Danmark, indrejser skjult i strømmene. På længere sigt kan bl.a. tilstedeværelsen af et konfliktområde i Europa, hvor tilgængeligheden af våben må formodes at være høj, eventuelt tiltrække tilrejsende ekstremister, som på sigt også kan udgøre en trussel mod Danmark.

Justitsministeriet bemærker hertil, at det ved datatræk i politiets sagsstyringssystem (POLAS) ses, at der i 2021 er rejst 42 sigtelser, 11 tiltaler og sket 10 domfældelser for overtrædelse af de terrorrelaterede bestemmelser i straffelovens kapitel 13 om forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme mv. Sigtelserne vedrører i alt 42 personer, tiltalerne i alt 11 personer og domfældelserne i alt 10 personer.

Justitsministeriet vurderer, at CTA's Vurdering af terrortruslen mod Danmark 2022 af 29. marts 2022 samt ovennævnte straffesager og deres karakter underbygger, at der også de næste 12 måneder må forventes at være en alvorlig, reel og aktuel trussel mod Danmarks nationale sikkerhed.

4. Vurdering af truslen mod Danmarks nationale sikkerhed fra spionage og fremmede magters efterretningsvirksomhed

Justitsministeriet vurderer endvidere, at truslen mod Danmarks nationale sikkerhed fra spionage og fremmede staters efterretningsvirksomhed er alvorlig, reel og aktuel de næste 12 måneder.

PET har i de seneste år afdækket flere sager, der vidner om, at en række fremmede stater aktivt udfører efterretningsvirksomhed i Danmark. Truslen, der de senere år er blevet mere markant, er kompleks og bredspektret og udgår primært fra Rusland, Kina og Iran, men der er også eksempler på, at andre stater udfører efterretningsaktiviteter i Danmark.

Ifølge PET og FE er der en specifik og vedvarende trussel fra fremmede staters efterretningsvirksomhed i Danmark, bl.a. i kraft af, at dansk teknologi og forskning på en række områder er verdensførende og dermed attraktivt at opnå adgang til.

Politikere, embedsfolk, offentlige myndigheder, Forsvaret, virksomheder, forskningsinstitutioner, forskere, studerende og dissidenter indgår løbende som mål og/eller midler i fremmede staters efterretningsvirksomhed mod Danmark. Fremmede staters efterretningstjenester er kendetegnet ved at være professionelle modstandere med en høj kapacitet, der i nogle tilfælde planlægger og gennemfører aktiviteter med en lang tidshorisont. Fremmede efterretningstjenester har ofte mange ressourcer til rådighed og udnytter løbende teknologiske fremskridt til at udvikle nye måder at operere.

Justitsministeriet bemærker, at der i 2020 og 2021 er rejst flere sigtelser og tiltaler samt sket domfældelser i sager om overtrædelse af de bestemmelser, der omhandler spionage og fremmede staters efterretningsvirksomhed, i straffelovens kapitel 12 om landsforræderi og andre forbrydelser mod statens

selvstændighed og sikkerhed. Det understøtter efter Justitsministeriets opfattelse ministeriets vurdering af den alvorlige, reelle og aktuelle trussel fra spionage og fremmede staters efterretningsvirksomhed.

5. Vurdering af truslen mod Danmarks nationale sikkerhed fra cyberangreb og cyberspionage

Herudover vurderer Justitsministeriet, at truslen mod Danmarks nationale sikkerhed fra cyberangreb og cyberspionage er alvorlig, reel og aktuel de næste 12 måneder.

Ifølge FE/CFCS har Ruslands invasion af Ukraine ikke på nuværende tidspunkt påvirket de aktuelle niveauer for cybertrusler. Det tempo og den spænding, som den nuværende situation foregår i, øger dog risikoen for misforståelser. Det medfører, at de sikkerhedspolitiske forhold – og derved trusselsniveauerne – hurtigt kan ændre sig.

Truslen fra cyberkriminalitet og cyberspionage er ifølge CFCS *meget høj*, idet både cyberkriminelle og medarbejdere hos statslige aktører arbejder systematisk, vedholdende og målrettet på at ramme mål i Danmark. Denne vurdering bygger bl.a. på konkrete cyberangreb og løbende angrebsforsøg.

Truslen fra cyberspionage retter sig især mod danske myndigheder og organisationer, som arbejder med udenrigs- og sikkerhedspolitik i bred forstand. Cyberspionage retter sig også i nogle tilfælde mod virksomheder og myndigheder, herunder Forsvaret, som kan blive værdifulde for fremmede stater at have adgang til i fremtiden. Bl.a. Rusland og Kina udfører cyberspionage målrettet mod Danmark.

CFCS vurderer, at truslen fra destruktive cyberangreb mod danske myndigheder og virksomheder på nuværende tidspunkt er lav, men at dette kan ændres med kort eller ingen varsel. Med destruktive cyberangreb forstås angreb, hvor den forventede effekt er enten død eller personskade, betydelig skade på fysiske objekter, eller ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning. Det betyder ifølge CFCS, at det er mindre sandsynligt, at danske virksomheder og myndigheder bliver udsat for forsøg på sådanne destruktive cyberangreb inden for de næste to år.

Det bemærkes, at der ikke foreligger sigtelser, tiltaler eller domfældelser vedrørende cyberangreb og cyberspionage. Det forhold, at der ikke har været indledt straffesager i relation til cyberangreb og cyberspionage, svækker dog efter Justitsministeriets opfattelse ikke vurderingen af, at truslen mod Danmarks nationale sikkerhed fra cyberangreb og cyberspionage må forventes at være alvorlig, reel og aktuel de næste 12 måneder, hvilket understreges af de konkrete hændelser og angrebsforsøg, som CFCS har kunnet konstatere.

6. Samlet vurdering af truslen mod Danmarks nationale sikkerhed

Justitsministeriet vurderer samlet set, at der er tale om tilstrækkeligt konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig, de næste 12 måneder.

På den baggrund vil der blive fastsat regler, der pålægger udbydere at foretage generel og udifferentieret registrering af trafikdata, som vil gælde fra og med den 30. marts 2022, kl. 12.00, til og med den 29. marts 2023. Oplysninger registreret i medfør af disse regler vil skulle opbevares et år fra registreringstidspunktet.