BEK nr 325 af 28/03/2025 (Gældende)

Bekendtgørelse om generel og udifferentieret registrering af trafikdata fra og med den 30. marts 2025 til og med den 29. marts 2026 og opbevaring til og med den 29. marts 2027

Ministerium: Justitsministeriet

Journalnummer: Justitsmin., j.nr. 2024-16305

Bekendtgørelse om generel og udifferentieret registrering af trafikdata fra og med den 30. marts 2025 til og med den 29. marts 2026 og opbevaring til og med den 29. marts 2027

I medfør af § 786 e og § 786 j, stk. 3, i lov om rettens pleje, jf. lovbekendtgørelse nr. 1160 af 5. november 2024, og efter forhandling med digitaliseringsministeren fastsættes:

Kapitel 1

Formål og anvendelsesområde

§ 1. Bekendtgørelsen har til formål at fastsætte regler om generel og udifferentieret registrering og opbevaring af trafikdata (logning), 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. Bekendtgørelsen finder anvendelse på udbydere som defineret i § 2, 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 2025 til og med den 29. marts 2026 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.

Stk. 2. De oplysninger, der er registreret i medfør af stk. 1, skal opbevares i 1 år fra registreringstidspunktet.

§ 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 2025 til og med den 29. marts 2026 registrere følgende oplysninger om egne e-mail-tjenester:

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

Stk. 2. De oplysninger, der er registreret i medfør af stk. 1, skal opbevares i 1 år fra registreringstidspunktet.

§ 7. En udbyder skal i perioden fra og med den 30. marts 2025 til og med den 29. marts 2026 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.

Stk. 2. De oplysninger, der er registreret i medfør af stk. 1, skal opbevares i 1 år fra registreringstidspunktet.

§ 8. Kan de oplysninger, der er nævnt i §§ 5-7, 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 §§ 5-7, kan efter aftale med udbyderen på dennes vegne foretages af en anden udbyder eller af en tredjemand.

Kapitel 3

Straf

§ 10. Overtrædelse af §§ 5-7 straffes med bøde.

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

Kapitel 4

Ikrafttrædelse

§ 11. Bekendtgørelsen træder i kraft den 30. marts 2025.

Stk. 2. Bekendtgørelsen ophæves den 30. marts 2027.

Justitsministeriet, den 28. marts 2025

PETER HUMMELGAARD

/ Morten Holland Heide

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 digitaliseringsministeren 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 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), herunder Center for Terroranalyse (CTA), Forsvarets Efterretningstjeneste (FE) og Styrelsen for Samfundssikkerhed (SAMSIK) om oplysninger om relevante forhold af betydning for vurderingen, jf. pkt. 2.

Herudover har Justitsministeriet ved sin vurdering lagt vægt på indholdet af følgende offentlige analyseprodukter: CTA's Vurdering af terrortruslen mod Danmark fra marts 2024 (VTD 2024), PET's Vurdering af Spionagetruslen mod Danmark, Færøerne og Grønland fra maj 2023 (VSD 2023), FE's Udsyn: Efterretningsmæssig Risikovurdering 2024 fra december 2024 samt SAMSIK's Vurdering af Cybertruslen mod Danmark 2024 fra september 2024 (oprindeligt udgivet af Center for Cybersikkerhed).

2. Bidrag til trusselsvurderingen fra Rigsadvokaten, PET, CTA, FE og SAMSIK

Rigsadvokaten har over for Justitsministeriet oplyst følgende:

> "Rigsadvokaten har til brug for udtalelsen i lighed med 2021, 2022 og 2023 gennemført datatræk fra politiets sagsstyringssystem (POLSAS) om igangværende og afsluttede sager om overtrædelse af straffelovens kapitel 12 og 13. Rigsadvokaten har derudover foretaget en manuel gennemgang af dataene for 2024 ud fra Rigsadvokatens kendskab til sager vedrørende overtrædelse af straffelovens § 101 a, samt §§ 114-114 j.
>
> Rigsadvokaten kan i den forbindelse oplyse, at tabellen nedenfor indeholder oplysninger om antallet af personer, der i perioden fra og med den 1. januar 2014 til og med den 31. december 2024 er registeret med en sigtelse, tiltale eller dom for overtrædelse af en eller flere bestemmelser i straffelovens kapitel 12 og 13. En person vil alene fremgå det år, hvor sigtelsen, tiltalen eller dommen er registreret i POLSAS. Det bemærkes i den forbindelse, at der kan være en periodevis forskydning af data, da eksempelvis antallet af afgørelser i 2024 også kan vedrøre tiltaler rejst i 2023, ligesom der ikke nødvendigvis

vil være indbyrdes sammenhæng mellem antallet af sigtelser, tiltaler og afgørelser.

Opgørelsen er fordelt på henholdsvis spionagesager, terrorsager og øvrige sager. Det bemærkes, at spionagesager omfatter sager vedrørende overtrædelse af straffelovens § 107 og/eller § 108, at terrorsager omfatter sager vedrørende overtrædelse af straffelovens §§ 114-114 j, og at 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 et offentligt retsmøde, som udgangspunkt ikke indgår i opgørelsen. Dette kan eksempelvis være tilfældet, hvis der – ofte på et tidligt tidspunkt i efterforskningen – er afgørende hensyn til fremmede magter eller til sagens opklaring, der kræver, at sigtelsen ikke må komme til offentlighedens kundskab.

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 18. januar 2025.

Tabel 1. Antal personer sigtet for overtrædelse af straffelovens kapitel 12 og 13 i perioden 2014 – 2024

Sagstrin	Gerningskode	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Sigtelser	Spionagesager	-	-	-	-	5	-	5	7	1	2	1
Sigtelser	Terrorsager	6	8	24	19	5	27	12	42	9	13	7
Sigtelser	Øvrige sager	4	2	1	-	2	3	1	8	4	11	14
Total		**10**	**10**	**25**	**19**	**12**	**30**	**15**	**57**	**14**	**26**	**22**

Tabel 2. Antal personer tiltalt for overtrædelse af straffelovens kapitel 12 og 13 i perioden 2014 – 2024

Sagstrin	Gerningskode	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Tiltaler	Spionagesager	-	-	-	-	-	-	2	4	-	-	1
Tiltaler	Terrorsager	3	2	5	9	6	6	1	12	14	5	3

Tiltaler	Øvrige sager	1	-	-	-	2	-	2	-	3	-	-
Total		**4**	**2**	**5**	**9**	**8**	**6**	**5**	**13**	**17**	**5**	**4**

Tabel 3. Antal personer dømt for overtrædelse af straffelovens kapitel 12 og 13 i perioden 2014 – 2024

Sagstrin	Fældende/ikke fældende	Gerningskode	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Afgørelser	Ikke fældende	Spionagesager	-	-	-	-	-	-	3	1	3	3	2
		Terrorsager	2	-	24	3	4	1	-	32	14	4	4
		Øvrige sager	1	3	5	1	-	1	-	6	-	2	1
		Total	**3**	**3**	**29**	**4**	**4**	**2**	**3**	**39**	**17**	**9**	**7**
	Fældende	Spionagesager	-	-	-	-	-	-	-	2	-	-	5
		Terrorsager	3	-	5	4	6	6	1	6	9	4	13
		Øvrige sager	-	-	-	-	-	-	2	1	-	-	1
		Total	**3**	**-**	**5**	**4**	**6**	**6**	**3**	**9**	**9**	**4**	**16**
Total			**4**	**3**	**34**	**8**	**10**	**8**	**6**	**46**	**24**	**12**	**19**

I 2025 har Højesteret afsagt dom i en ankesag (U. 2024.3644 – endnu ikke opdateret i UfR), hvor en på gerningstidspunktet 15-årig tiltalt blev dømt for at have ladet sig hverve til at begå eller medvirke til, at andre skulle begå terrorhandlinger for en højreekstremistisk terrororganisation (Feuerkrieg Division). Den tiltalte blev endvidere dømt for at have fremmet denne terrororganisations virksomhed og for forsøg på at hverve en person til at begå eller fremme terrorhandlinger for samme terrororganisation. Den tiltalte blev i byretten frifundet for overtrædelse af straffelovens § 114 c, stk. 3, men dømt for overtrædelse af straffelovens § 114 c, stk. 1, og § 114 e, 1. pkt., og idømt 5 år og 6 måneders fængsel samt kontaktforbud i 6 år. Straffen blev i 2024 skærpet af Østre Landsret til 7 års fængsel samt kontaktforbud i 7 år, idet den tiltalte ligeledes blev dømt for overtrædelse af straffelovens § 114 c, stk. 3. Højesteret stadfæstede den 14. marts 2025 landsrettens dom i forhold til skyldsspørgsmålet, men nedsatte straffen. Højesteret lagde ved strafudmålingen vægt på en række skærpende omstændigheder, herunder at den dømte indtog en ledende rolle i Feuerkrieg Division og var med til at udarbejde deres håndbog, men lagde i formildende retning også navnlig vægt på den dømtes unge alder (15½ år ved anholdelsen) og hans relativt kortvarige medlemskabsperiode forud for anholdelsen (4 måneder). Højesteret fandt på den baggrund samlet set, at straffen skulle fastsættes til 5 års fængsel samt kontaktforbuddet til 5 år. Sagen byggede navnlig på en række fund på telefoner og it-udstyr, der bl.a. kunne belyse, hvem den tiltalte havde haft kontakt til, og hvad han havde sendt til andre.

Højesteret har endvidere afsagt dom i en ankesag (U. 2025.721), hvor tre iranske statsborgere blev idømt fængsel i henholdsvis 8, 7 og 6 år samt udvist, ligesom den ene tiltalte blev frakendt sin danske indfødsret for navnlig bistand til en saudiarabisk efterretningstjeneste, terrorfinansiering og anden fremme af terrorvirksomhed, jf. straffelovens § 108, stk. 1 og 2, § 114 b og § 114 e, 1. pkt. For Højesteret var hovedspørgsmålet, om de handlinger, som var begået af ASMLA, Martyr Muhyiddin Al-Nasser Brigaden og Jaish al-Adl i Iran, skulle anses som terror eller som lovlig frihedskamp mod det iranske styre. Højesteret udtalte, at selve det forhold, at en handling har været rettet mod et land, som ikke er et demokratisk samfund, men regeres af et totalitært regime, der ikke respekterer retsstatsprincippet, ikke indebærer, at handlingen falder uden for terrorbestemmelsernes anvendelsesområde. Ud fra en samlet vurdering af alle sagens elementer fandt Højesteret, at de tiltalte var skyldige i fremme af terrorvirksomhed og terrorfinansiering.

Der er yderligere faldet endelig dom i en ankesag i Østre Landsret (U. 2024.5352), hvor den tiltalte blev idømt fængsel i 8 måneder, jf. straffelovens § 108, stk. 1, ved at have forsøgt at yde bistand til en tyrkisk efterretningstjeneste. I sagen var det relevant at undersøge, om tiltalte havde rettet telefonisk eller anden henvendelse til en tyrkisk efterretningstjeneste.

Endelig har Højesteret afsagt dom i sagen U. 2024.3404, hvor den tiltalte blev idømt fængsel i 4 år samt frakendt dansk indfødsret for at fremme IS's virksomhed, jf. straffelovens § 114 e, 1. pkt., og § 114 j, stk. 1, jf. stk. 3, ved bl.a. at have virket som husmor og hustru til personer, der var aktive i IS, og for at have opholdt sig i et konfliktområde omfattet af indrejse- og opholdsforbud. I nærværende sag fandtes det også relevant bl.a. at kunne undersøge, hvem hun havde haft kontakt med under sit ophold i Syrien. "

CTA har over for Justitsministeriet oplyst følgende:

"CTA vurderer, at terrortruslen mod Danmark fortsat er i niveauet *alvorlig* (niveau 4 ud af 5).

Mere end et år efter at konflikten i Mellemøsten eskalerede med Hamas' terrorangreb mod Israel den 7. oktober 2023, har konflikten fortsat afledt betydning for trusselsbilledet i Danmark.

CTA vurderer fortsat, at konflikten i Mellemøsten rummer et væsentligt mobiliseringspotentiale, som kan aktivere en række kendte og ikke-kendte trusselsaktører til spontane eller planlagte reaktioner, herunder terrorangreb. CTA vurderer, at konflikten også i det kommende år vil fungere som en væsentlig drivkraft for terrortruslen mod Danmark og danske interesser, ligesom den vil medvirke til en fortsat øget trussel mod jødiske og israelske interesser i Danmark. I Danmark er der i 2024 rejst sigtelse efter terrorparagrafferne i straffeloven mod flere personer i to separate sager, hvor målet i begge sager var jødiske og/eller israelske interesser i Danmark. CTA vurderer, at personer og netværk, som har forbindelser til eller er tilhængere af militant islamistiske grupper, som er involveret i konflikten i Mellemøsten, aktuelt påvirker trusselsbilledet i dele af Europa, herunder Danmark.

CTA vurderer, at terrortruslen fra militante islamister mod Danmark fortsat er i niveauet *alvorlig* (niveau 4 ud af 5). Siden 2023 har Islamisk Stat udvist øget intention om angreb i Vesten, og konflikten i Mellemøsten har radikaliseret og mobiliseret militante islamister. Det gælder både velkendte trusselsaktører som Islamisk Stat og al-Qaida, der har søgt at udnytte konflikten i deres propaganda og bl.a. opfordret til angreb i Vesten som hævn, og aktører, der ikke tidligere har haft betydning for trusselsbilledet i Danmark. En række af de militant islamistiske angreb i Vesten, som er gennemført og afværget i 2024, har taget afsæt i konflikten.

CTA vurderer, at terrortruslen fra højreekstremister mod Danmark fortsat er i niveauet *generel* (niveau 3 ud af 5). Det skyldes bl.a., at danske højreekstremistiske miljøer både fysisk og online har styrket deres transnationale forbindelser det seneste år, samt tendenser til øget voldsparathed, som forstærkes af målrettet rekruttering i voldsparate miljøer. De senere års stigning i antallet af danske unge og mindreårige, der radikaliseres i højreekstremistiske onlinefora, fortsætter. Samtidig ses en styrket tendens til dannelse af hybride onlinenetværk med elementer af højreekstremisme, men uden formel ledelse, medlemskab og organisationskultur, hvilket gør truslen fra højreekstremister mere fragmenteret og omskiftelig end tidligere.

CTA hæver niveauet for terrortruslen fra venstreekstremister mod Danmark fra niveauet *minimal* (niveau 1 ud af 5) til *begrænset* (niveau 2 ud af 5). Dette skyldes især reaktualiseringen af den pro-palæstinensiske dagsorden som samlende sag som følge af konflikten i Mellemøsten, hvilket på tværs af interne modsætninger har skabt en platform for konkret handling og radikalisering blandt danske venstreekstremister.

CTA vurderer, at terrortruslen fra antimyndighedsekstremister mod Danmark fortsat er i niveauet *begrænset* (niveau 2 ud af 5).

Historisk har terrortruslen mod Danmark primært været drevet af aktører motiveret af militant islamisme, højreekstremisme, venstreekstremisme eller antimyndighedsekstremisme. Ovennævnte er fortsat de væsentligste trusselsaktører, men gennem de senere år har aktører, som ikke umiddelbart passer ind i disse kategorier, spillet en stadig større rolle i trusselsbilledet. I samspil med globale udviklinger og dynamikker bidrager disse aktører til et mere fragmenteret og uforudsigeligt trusselsbillede, hvor sammenhængen mellem motiv og aktør i et stigende antal tilfælde kan være uklar.

Flere af disse aktører har ikke et tydeligt ideologisk tilhørsforhold. Når aktører i mindre grad er begrænset af ideologisk forankrede normer og fjendebilleder, bliver deres måludpegning og fremgangsmåder mere uforudsigelige. Samtidig kan deres forsæt være utydeligt, hvilket kan vanskeliggøre myndighedernes vurdering af, hvorvidt en handling udgør terror. ”

PET har herudover oplyst følgende:

”Fremmede staters efterretningsvirksomhed udgør fortsat en markant, bredspektret og vedvarende trussel mod Danmark. Truslen udgår særligt fra Rusland og Kina, men stater som Iran og Tyrkiet udfører også efterretningsaktiviteter i Danmark i modstrid med nationale sikkerhedsinteresser. Truslen fra fremmede staters efterretningsvirksomhed udspiller sig på baggrund af et stadig mere dynamisk og komplekst trusselsbillede, der er præget af øget stormagtsrivalisering, krige og konflikter, et intensiveret teknologikapløb samt et stadigt stærkere pres fra autoritære stater for at omdefinere internationale regler og normer.

Truslen omfatter først og fremmest spionage, sabotage samt forsøg på ulovligt eller uønsket vis at anskaffe produkter, viden og teknologi for bl.a. at udvikle de fremmede staters militære kapacitet. Der udgår også en trussel fra fremmede efterretningstjenesters påvirkningsvirksomhed og fra fremmede stater, der chikanerer eller udøver pression mod egne statsborgere – primært dissidenter – der opholder sig i Danmark.

Det er PET’s vurdering, at Ruslands risikovillighed vedrørende brug af hybride virkemidler mod Europa er højere end tidligere, og der er derfor aktuelt en skærpet trussel fra fysisk sabotage i Danmark. For-

målet med de russiske aktiviteter er, ifølge PET's vurdering, bl.a. at hindre forsyninger til Ukraine og at skabe usikkerhed og frygt for eskalation i de vestlige samfund for derved at svække opbakningen til den fortsatte politiske, økonomiske og militære støtte til Ukraine blandt befolkninger og politikere i Europa.

I 2024 har der været flere eksempler på, at personer relateret til Rusland har stået bag forskellige former for fysisk sabotage – eksempelvis ildspåsættelse og groft hærværk – i flere europæiske lande. De europæiske lande, der har været mål for sabotageoperationer, er alle væsentlige civile og militære bidragsydere til Ukraines forsvarskamp mod Rusland. Det bemærkes i den forbindelse, at Danmark tilhører kredsen af europæiske lande, der yder væsentlig materiel, politisk og økonomisk støtte til Ukraine.

Det er PET's vurdering, at Rusland også fremadrettet vil forsøge at planlægge eller gennemføre sabotageaktioner eksempelvis mod vestlige lande, herunder Danmark, der yder betydelig støtte til Ukraine i krigen mod Rusland, og at de russiske efterretningstjenester har kapacitet til at intensivere brugen af hybride virkemidler over for Vesten yderligere.

De russiske efterretningstjenester indhenter desuden løbende oplysninger om kritisk infrastruktur i vestlige lande, herunder Danmark, og det er meget sandsynligt, at Rusland også planlægger sabotage af kritisk infrastruktur i bl.a. Danmark, som kan aktiveres i tilfælde af en eskalerende konflikt. Ruslands øgede risikovillighed til at udøve sabotage betyder, at dansk kritisk infrastruktur i enkeltstående tilfælde kan blive mål for sabotage. PET vurderer, at Danmarks medlemskab af NATO samt dansk støtte til Ukraine er med til at skærpe fremmede efterretningstjenesters interesse for dansk kritisk infrastruktur. PET vurderer, at kritisk infrastruktur vil være et mål for fjendtlige stater i tilfælde af en eskalerende konflikt eller krig mod NATO.

På baggrund af udvisningen af 15 russiske efterretningsofficerer i april 2022 og den danske regerings indførelse af paritet i september 2023 vurderer PET, at Rusland forsøger at anvende andre måder at spionere i Danmark på, herunder ved at udstationere efterretningsofficerer i Danmark uden for de diplomatiske repræsentationer, ved brug af tilrejsende efterretningsofficerer eller ved, at de russiske efterretningsofficerer i højere grad rekrutterer eventuelle danske kilder i Rusland eller i tredjelande. PET vurderer endvidere, at Rusland vedholdende og kontinuerligt forsøger at genopbygge tilstedeværelsen af

efterretningsofficerer på de såkaldte residenturer, på Ruslands diplomatiske repræsentationer rundt om i Europa, herunder i Danmark.

Kina og det kinesiske kommunistpartis globale ambitioner og vilje til at udfordre Vesten afspejles også i trusselsbilledet i Danmark. Kina har ambitioner om at blive førende indenfor visse forsknings- og teknologiområder, hvor også Danmark er langt fremme, og Kinas efterretningsmæssige fokus er især på forskning og teknologi, som kan fremme landets militære kapacitet. Kina anvender en bred vifte af virkemidler til at understøtte landets strategiske og teknologiske interesser, og PET kan konstatere, at de kinesiske efterretningstjenester har meget vide beføjelser til at indsamle oplysninger i udlandet. Den kinesiske efterretningslovgivning bevirker bl.a., at de kinesiske efterretningstjenester om nødvendigt kan pålægge kinesiske statsborgere, virksomheder, organisationer og myndigheder i Kina, men også i udlandet, at videregive oplysninger, de måtte komme i besiddelse af. Ulovlig eller uønsket overførsel af viden til Kina kan efter PET's vurdering bl.a. ske i forbindelse med forskellige former for kinesisk forskningssamarbejde med danske forskningsinstitutioner, hvor de kinesiske efterretningstjenester kan være involveret.

Truslen fra iransk efterretningsvirksomhed i Danmark er primært rettet mod herboende iranske dissidenter, oppositionsgrupper og toneangivende kritikere af det iranske styre. Truslen mod disse personer udgår ikke kun fra de iranske efterretningstjenester, men også fra andre aktører, heriblandt kriminelle stedfortrædere, der på den ene eller anden måde har forbindelse til efterretningstjenesterne. Sådanne aktører er bl.a. involveret i ulovlig indsamling af oplysninger om eksiliranere i Europa, herunder i Danmark, og de forsøger også aktivt at påvirke iranere bosiddende i Europa til at afstå fra at udøve kritik af og oppositionsvirksomhed mod det iranske styre.

PET vurderer, at Tyrkiet i Danmark udøver forskellige former for efterretningsaktiviteter mod personer og grupper, som den tyrkiske regeringsmagt opfatter som en trussel. PET kan konstatere, at der er personer i Danmark med tyrkisk baggrund, der enten af egen drift eller på vegne af en af de tyrkiske efterretningstjenester, indsamler og videregiver oplysninger til de tyrkiske myndigheder om påståede eller reelle kritikere af den tyrkiske regering.

Danmark er generelt fortsat et attraktivt mål for fremmede efterretningstjenester, bl.a. på grund af Danmarks medlemskab af NATO, EU og FN, den generelle åbenhed i samfundet, digitaliseringen samt et højt teknologisk vidensniveau. Fremmede efterretningstjenester retter

deres aktiviteter mod et bredt spektrum af mål i Danmark, som bl.a. omfatter politikere, embedsfolk, ansatte i sikkerhedsmyndighederne og Forsvaret, danske virksomheder og forskningsinstitutioner, kritisk dansk infrastruktur og dissidenter. Fremmede efterretningstjenester er opportunistiske i deres måludvælgelse, så nye mål kan komme til i et dynamisk trusselsbillede.

Hvis fremmede stater uretmæssigt 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, vil informationerne potentielt kunne bruges både mod Danmark og mod Danmarks samarbejdslande. Yderligere kan dansk teknologi, produkter og viden ende i de forkerte hænder og styrke Danmarks modstanderes militære kapacitetsopbygning. ”

FE har over for Justitsministeriet oplyst følgende:

”Terrortruslen

Terrortruslen i Europa er steget siden 2022. Antallet af gennemførte og afværgede islamistiske terrorangreb i Vesteuropa har brudt en generelt faldende tendens siden 2017. Alene i de to første måneder i 2025 har militante islamister udført seks terrorangreb i Europa. Det er samme antal angreb som i hele 2024. Mindst seks terrorangreb er i samme periode blevet forhindret.

Antallet af dræbte i 2024 og foreløbigt i 2025 er dog væsentligt lavere end tidligere år. Det skyldes sandsynligvis, at de fleste angreb de seneste år er blevet udført med simple midler, herunder knive.

FE kan desuden konstatere, at konflikten i Gaza fortsat spiller en markant rolle ift. at inspirere til terrorangreb i Europa. Terrorgrupper som Islamisk Stat og al-Qaida har som følge af krigen i Gaza intensiveret opfordringer til terror i Vesten, herunder især mod jødiske og israelske mål. Det er sandsynligt, at terrorister vil forsøge at angribe mindre beskyttede mål, såsom store forsamlinger af civile, og bruge helt simple midler såsom biler og knive.

Flere Islamisk Stat-undergrupper – herunder Islamisk Stat i Khorasan-provinsen (ISKP) i Afghanistan og Islamisk Stat i Somalia – har gentagne gange siden 2023 mobiliseret, opfordret og vejledt enkeltpersoner til at udføre terrorangreb i Europa.

Terrorgrupper som Islamisk Stat er i stand til at udføre koordinerede angreb med mange ofre tæt på Vesteuropa. Terrorgrupper vil dog stadig have svært ved at gennemføre større koordinerede angreb i Vesteuropa, hvor der f.eks. ikke er samme adgang til skydevåben og materialer til at fremstille sprængstoffer. Myndigheder i Vesteuropa er generelt også effektive til at optrevle og modvirke angrebsplaner, som involverer større personkredse og netværk.

Højreekstremister udgør også en terrortrussel, og de vil fortsat dyrke digitale fællesskaber, hvor der bliver spredt ekstremistiske budskaber, manifester og angrebsvideoer. Det er sandsynligt, at højreekstremister i Vesten i de kommende år vil bruge enkeltstående begivenheder til at anspore til vold og muligvis terror mod forskellige minoritetsgrupper.

Rusland

Det er Ruslands strategiske ambition at svække USA's ledende globale rolle, de vestlige landes sammenhold og den regelbaserede verdensorden. Rusland vil i stedet have en verdensorden, hvor stormagter og regionale magter kan forfølge deres egne interesser uden om USA og de øvrige vestlige lande, og hvor det er stormagternes evne og vilje til at bruge militær magt, der i sidste ende definerer spillereglerne i internationale forhold.

Det er sandsynligt, at Rusland vil forsøge at fremkalde en frygt og ubeslutsomhed i NATO-lande, der skal skabe usikkerhed om det samlede NATO's evne til at reagere hurtigt og effektivt mod Rusland.

Det er meget sandsynligt, at Rusland fortsat vil være opmærksom på at undgå, at dets militære aktiviteter kommer til at udløse NATO's artikel 5 om alliancens kollektive forsvarsforpligtelse. Det er samtidigt sandsynligt, at Rusland de kommende år gradvist vil blive mere villig til at bruge militære magtmidler til at lægge pres på eller udfordre NATO eller enkelte NATO-lande, også i Østersøregionen.

Ruslands øgede risikovillighed over for NATO-lande vil stige yderligere, i takt med at Ruslands konventionelle militære styrke vokser. Det betyder også, at den militære trussel fra Rusland vil stige over de kommende år.

Putin-styret har iværksat en ambitiøs oprustning af Ruslands konventionelle væbnede styrker. Det sker parallelt med en militarisering af samfundet. Samtidigt gennemfører Rusland en militærreform, der

skal effektivisere planlægning, indsættelse og føring af de militære styrker. Det er Ruslands målsætning, at landets konventionelle styrker med kort forberedelsestid skal kunne vinde en krig mod NATO i Ruslands vestlige grænseområder og skal kunne indsættes mod militært underlegne nabolande.

Rusland er blevet mere villig til at bruge hybride virkemidler i Vesten. Rusland har i løbet af Ukraine-krigen udvist en stigende risikovillighed og parathed til at anvende offensive hybride virkemidler i vestlige lande. Dette er f.eks. kommet til udtryk i forbindelse med russisk sabotage mod mål i Vesten. Det er sandsynligt, at Rusland løbende planlægger og forbereder sabotageaktioner mod udvalgte mål i Danmark og i andre europæiske lande.

Rusland forbereder også at kunne udføre sabotage, som kan iværksættes forud for en militær konflikt med NATO. Formålet med krigsforberedende sabotage er at sætte styrker, materiel og infrastruktur, der understøtter bl.a. Danmarks evne til at forsvare sig, ud af spil umiddelbart før en militær konflikt mellem NATO og Rusland.

Det er meget sandsynligt, at Rusland løbende opdaterer sine planer for at sabotere kritisk undersøisk infrastruktur i tilfælde af en eskalerende konflikt eller krig mod NATO. I kystnære farvande, som de indre danske farvande, vil Rusland kunne angribe undersøisk infrastruktur fra alle typer fartøjer. Det er også muligt at ødelægge kabler og rørledninger ved at trække anker, trawl og lignende henover dem. I Nordatlanten kræver det specialiserede fartøjer at angribe undersøisk infrastruktur. Rusland råder over forskningsskibe og ubåde, der kan kortlægge infrastrukturen, og specialiserede ubåde og droner, der vil kunne angribe dem.

Ruslands krig mod Ukraine har vist, hvordan Rusland anvender hybride virkemidler både som forberedelse til og under en direkte militær konflikt. Allerede før invasionen brugte Rusland hybride virkemidler mod Ukraine, især påvirkningskampagner og cyberangreb med henblik på at destabilisere landet.

Ruslands påvirkningskampagner har i mange år spillet en central rolle i landets forsøg på at udøve indflydelse på de vestlige samfund, og det er sandsynligt, at truslen fra Ruslands påvirkningskampagner mod vestlige lande vil stige yderligere.

Rusland forsøger bl.a. at påvirke politiske processer og den offentlige opinion i vestlige lande ved hjælp af vestlige politikere og offentlige meningsdannere, der ser positivt på Rusland. Rusland forsøger at opbygge kontakter til vestlige politikere fra begge sider af det politiske spektrum, særligt på yderfløjene. Rusland spreder også fortællinger på sociale medier, der skal svække befolkningens tillid til politiske processer og etablerede medier.

Rusland udgør en aktiv og vedvarende spionagetrussel mod Kongeriget Danmark. Ruslands hensigt med spionagen er bl.a. at få indsigt i dansk udenrigs-, sikkerheds- og forsvarspolitik og beslutningsprocesser, danske militære kapaciteter og dansk kritisk infrastruktur. Rusland spionerer blandt andet med det formål at forberede sabotage. Rusland spionerer ved hjælp af menneskelige kilder og elektronisk indhentning, f.eks. indhentning mod telekommunikation. Desuden udfører Rusland cyberspionage. Rusland har betydelige kapaciteter inden for disse efterretningsmetoder. Udvisningen af russiske efterretningsagenter under diplomatisk dække på Ruslands ambassader har gjort det vanskeligere for landet at spionere i Europa. Rusland forsøger derfor i højere grad at hverve agenter online på sociale medier. Rusland benytter også denne metode til hvervning til sabotage. Agenterne ved ikke nødvendigvis, at de løser opgaver for en russisk efterretningstjeneste. Herudover udnytter Rusland civilsamfundet f.eks. diaspora, den russisk ortodokse kirke og civile skibe og fly til at indhente viden om danske interesser. Metoderne gør det vanskeligt at skelne mellem legitime og illegitime aktiviteter og slører grænsen mellem det militære og civile.

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.

Kinas omfattende og vedvarende spionage mod andre lande er også målrettet danske myndigheder, virksomheder og organisationer. Danmarks medlemskab af FN's sikkerhedsråd og det kommende danske EU-formandskab vil midlertidigt skærpe spionagetruslen mod Danmark. Danmark vil i den periode have adgang til flere oplysninger og være involveret i at træffe beslutninger, som en række fremmede stater vil have interesse i at påvirke til deres fordel.

Kinesiske efterretningstjenester arbejder også målrettet på at kontrollere kinesere i andre lande og bruge dem som middel til spionage og andre formål. Kinas militær og kinesiske efterretningstjenester har bl.a. 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 interesser, såvel som landets 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 overføre teknologi og viden til Kina. Til det formål bruger Kina en lang række midler, herunder videnskabeligt samarbejde, talentprogrammer, investeringer og spionage. Det er meget sandsynligt, at Kina også ønsker at tilegne sig viden og teknologi fra danske forskningsinstitutioner og virksomheder.

Mellemøsten

Konflikter i Mellemøsten vil fortsat kunne udgøre en trussel mod europæisk sikkerhed. Regionen vil også i de kommende år være præget af strukturelle problemer, som forringer befolkningernes levevilkår og skaber øget grobund for terror og migration.

Krigen i Gaza og konflikten mellem Iran og Israel har på flere måder skærpet det trusselsbillede, som Europa står over for.

Irans efterretningstjenester har øget deres fokus på israelske og jødiske mål og interesser i Europa som følge af den skærpede konflikt med Israel. Desuden har iranske efterretningstjenester gennem en årrække forfulgt iranske eksilgrupper og personer i Europa, som det iranske styre anser som en trussel. Det gælder også i Danmark.

I Yemen har den iransk-støttede Houthi-bevægelse brugt krigen i Gaza som begrundelse for at angribe civile handelsskibe. Det har bl.a. tvunget danske rederier til at sejle uden om Det Røde Hav.

I Syrien vil Islamisk Stat og andre terrorgrupper forsøge at udnytte det pludseligt opståede magttomrum efter Assad-styrets fald i slutningen af 2024 til at vokse sig stærkere igen. Det indebærer en risiko for, at Islamisk Stat i Syrien igen kan komme til at udgøre en alvorlig terrortrussel mod Europa. ”

SAMSIK har i koordination med FE over for Justitsministeriet oplyst følgende:

”Cyberangreb fra både stater og ikke-statslige hackere og hackergrupper udgør en vedvarende og alvorlig trussel mod Danmark. Cyberkriminelle, cyberaktivister og statslige aktører arbejder systematisk, vedholdende og målrettet på at ramme mål i Danmark. Truslen hænger ofte sammen med andre sikkerhedspolitiske udfordringer, Danmark står over for.

Trusselsniveaet for cyberspionage og cyberkriminalitet mod Danmark er **MEGET HØJT.** Cyberkriminalitet er blandt de mest synlige cybertrusler og kan have mærkbare konsekvenser for både borgere og organisationer i samfundet.

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. Cyberspionage retter sig også i nogle tilfælde mod virksomheder og myndigheder, som kan blive værdifulde for fremmede stater at have adgang til i fremtiden. Eksempelvis kan adgange opnået via cyberspionage anvendes til fremtidige destruktive cyberangreb.

Truslen fra destruktive cyberangreb er **MIDDEL.** Danmark står overfor et trusselsbillede, hvor destruktive cyberangreb er en reel mulighed. Ruslands risikovillighed over for NATO-lande har øget sandsynligheden for, at Rusland vil udføre denne type cyberangreb mod bl.a. Danmark.

Det er dog fortsat mindre sandsynligt, at Rusland i den nuværende situation vil gennemføre destruktive cyberangreb mod Danmark, hvor hensigten er at skabe alvorlige konsekvenser for samfundsvigtige funktioner. Mindre omfattende destruktive cyberangreb kan dog stadig få betydelige konsekvenser for offeret og samfundet.

> Hvis Rusland i den nuværende situation beslutter at gennemføre et destruktivt cyberangreb mod Danmark, vil formålet sandsynligvis være at skabe frygt og lægge pres på det danske samfund og beslutningstagere. Den konkrete fysiske effekt af angrebene vil sandsynligvis være sekundær, hvilket efterlader en lang række potentielle mål i samfundet. Selvom det er mindre sandsynligt, at Rusland vil gennemføre destruktive cyberangreb med alvorlige og omfattende konsekvenser, er det sandsynligt, at hackergrupper knyttet til Rusland løbende forbereder sig på at kunne udføre den angrebstype mod Danmark. Sandsynligheden for, at disse angreb finder sted, kan derfor stige med kort eller uden varsel – særligt hvis konflikten mellem Rusland og Vesten eskalerer eller ændrer karakter.
>
> Truslen fra cyberaktivisme er **HØJ.** Cyberaktivistiske angreb, der løbende har ramt danske mål, understreger, at truslen fra cyberaktivisme mod danske virksomheder og myndigheder er blevet en del af normalbilledet. Det gælder særligt pro-russiske cyberaktivisters overbelastningsangreb mod hjemmesider og internetvendte tjenester. Angrebene understøtter Ruslands interesser, og det er sandsynligt, at nogle af cyberaktivisterne har forbindelser til den russiske stat. ”

3. Vurdering af truslen mod Danmarks nationale sikkerhed fra terror

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

Justitsministeriet har ved vurderingen bl.a. lagt vægt på CTA's udtalelse ovenfor. Heraf fremgår det bl.a., at CTA vurderer, at terrortruslen er i niveauet *alvorlig*. Ifølge CTA er trusselsbilledet fortsat præget af afledte konsekvenser af konflikten i Mellemøsten, der eskalerede med Hamas' terrorangreb mod Israel den 7. oktober 2023, og det vurderes, at konflikten også i det kommende år vil fungere som en væsentlig drivkraft for terrortruslen mod Danmark og danske interesser samt medvirke til en øget trussel mod jødiske og israelske interesser i Danmark.

Ved vurderingen har Justitsministeriet desuden lagt vægt på, at CTA vurderer, at terrortruslen fra militante islamister fortsat er i niveauet *alvorlig*. Ifølge CTA har Islamisk Stat siden 2023 udvist øget intention om angreb i Vesten, og konflikten i Mellemøsten har radikaliseret og mobiliseret militante islamister. Derudover har en række af de militant islamistiske angreb i Vesten, som er gennemført og afværget i 2024, taget afsæt i konflikten.

Det har endvidere indgået i Justitsministeriets vurdering, at truslen fra højreekstremister vurderes fortsat at være i niveauet *generel*. Ifølge CTA skyldes trusselsniveauet bl.a., at danske højreekstremistiske miljøer både fysisk og online har styrket deres transnationale forbindelser det seneste år, og at der ses tendenser til øget voldsparathed, som forstærkes af målrettet rekruttering i voldsparate miljøer.

Justitsministeriet har derudover lagt vægt på, at CTA vurderer, at terrortruslen fra venstreekstremister mod Danmark er opjusteret til niveauet *begrænset*, idet trusselsniveauet tidligere har været i niveauet *minimal*. Ifølge CTA skyldes opjusteringen især reaktualiseringen af den pro-palæstinensiske dagsorden

som samlende sag, hvilket på tværs af interne modsætninger har skabt en platform for konkret handling og radikalisering blandt danske venstreekstremister.

Herudover har Justitsministeriet ved vurderingen lagt vægt på FE's udtalelse ovenfor, hvor det bl.a. fremgår, at terrortruslen i Europa er steget siden 2022, og at krigen i Gaza har været et vigtigt motiv bag flere terrorangreb og forsøg på terrorangreb i Europa i 2024 og 2025. Terrorgrupper som Islamisk Stat og al-Qaida har intensiveret opfordringer til terror i Vesten, herunder især mod jødiske og israelske mål globalt. Ifølge FE er det sandsynligt, at terrorister vil forsøge at angribe mindre beskyttede mål, såsom store forsamlinger af civile, og bruge helt simple midler såsom biler og knive.

Det har endvidere indgået i Justitsministeriets vurdering, at FE vurderer, at højreekstremister også udgør en terrortrussel, og at det ifølge FE er sandsynligt, at højreekstremister i Vesten i de kommende år vil bruge enkeltstående begivenheder til at anspore til vold og muligvis terror mod forskellige minoritetsgrupper. Derudover har Justitsministeriet lagt vægt på, at FE vurderer, at Islamisk Stat og andre terrorgrupper i Syrien vil forsøge at udnytte det pludseligt opståede magttomrum efter Assad-styrets fald i slutningen af 2024 til at vokse sig stærkere igen, hvilket indebærer en risiko for, at Islamisk Stat i Syrien igen kan komme til at udgøre en alvorlig terrortrussel mod Europa.

I forlængelse heraf bemærker Justitsministeriet, at der ifølge Rigsadvokatens dataudtræk i politiets sagsstyringssystem (POLSAS) i 2024 blev rejst syv sigtelser, tre tiltaler og skete 13 domfældelser for overtrædelse af terrorbestemmelserne i straffelovens kapitel 13 om forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme mv. Det bemærkes i den forbindelse, at sigtelserne ifølge CTA bl.a. vedrører flere personer i to separate sager, hvor målet i begge sager var jødiske og/eller israelske interesser i Danmark.

Justitsministeriet vurderer, at oplysningerne fra CTA, FE samt oplysningerne fra Rigsadvokaten om ovennævnte straffesager og deres karakter understøtter, at der også de næste 12 måneder må forventes at være en alvorlig, reel og aktuel trussel mod Danmarks nationale sikkerhed fra terror.

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

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

Justitsministeriet har ved vurderingen bl.a. lagt vægt på PET's udtalelse ovenfor samt PET's Vurdering af Spionagetruslen mod Danmark af 2. maj 2023. Det fremgår bl.a. heraf, at der er en markant, bredspektret og vedvarende trussel fra fremmede staters efterretningsvirksomhed mod Danmark. Truslen udgår særligt fra Rusland og Kina, men stater som Iran og Tyrkiet udfører også efterretningsaktiviteter i Danmark i modstrid med nationale sikkerhedsinteresser.

Justitsministeriet har i den forbindelse også lagt vægt på, at truslen først og fremmest omfatter spionage, sabotage samt forsøg på ulovligt eller på uønsket vis at anskaffe produkter, viden og teknologi for bl.a. at udvikle de fremmede staters militære kapacitet. Der udgår ifølge PET også en trussel fra fremmede efterretningstjenesters påvirkningsvirksomhed og fra fremmede stater, der chikanerer eller udøver pression mod egne statsborgere – primært dissidenter – der opholder sig i Danmark.

Det har desuden indgået i Justitsministeriets vurdering, at PET vurderer, at Ruslands risikovillighed vedrørende brug af hybride virkemidler mod Europa, er højere end tidligere, og at der derfor aktuelt er en skærpet trussel fra fysisk sabotage i Danmark. Dertil kommer, at PET vurderer, at Rusland også fremadrettet vil forsøge at planlægge eller gennemføre sabotageaktioner eksempelvis mod vestlige lande,

herunder Danmark, der yder betydelig støtte til Ukraine i krigen mod Rusland, og at det er meget sandsynligt, at Rusland også planlægger sabotage af kritisk infrastruktur i bl.a. Danmark, som kan aktiveres i tilfælde af en eskalerende konflikt.

Justitsministeriet har endvidere lagt vægt på, at PET vurderer, at Danmark generelt fortsat er et attraktivt mål for fremmede efterretningstjenester, og at fremmede efterretningstjenester retter deres aktiviteter mod et bredt spektrum af mål i Danmark, som bl.a. omfatter politikere, embedsfolk, ansatte i sikkerhedsmyndighederne og Forsvaret, danske virksomheder og forskningsinstitutioner, kritisk dansk infrastruktur og dissidenter.

Derudover har Justitsministeriet lagt vægt på, at det efter PET's opfattelse kan skade Danmarks sikkerhed og handlefrihed, hvis fremmede stater uretmæssigt får adgang til klassificerede og beskyttelsesværdige informationer. Yderligere kan dansk teknologi, produkter og viden ende i de forkerte hænder og styrke Danmarks modstanderes militære kapacitetsopbygning.

Justitsministeriet har ved vurderingen desuden lagt vægt på FE's udtalelse ovenfor, hvoraf det bl.a. fremgår, at Rusland udgør en aktiv og vedvarende spionagetrussel mod Kongeriget Danmark, og at Rusland bl.a. spionerer med det formål at forberede sabotage. Derudover er det FE's vurdering, at Kinas omfattende og vedvarende spionage mod andre lande også er målrettet danske myndigheder, virksomheder og organisationer, og at det er meget sandsynligt, at Kina også ønsker at tilegne sig viden og teknologi fra danske forskningsinstitutioner og virksomheder. Ifølge FE vil Danmarks medlemskab af FN's sikkerhedsråd og det kommende danske EU-formandskab midlertidigt skærpe spionagetruslen mod Danmark.

Justitsministeriet bemærker herudover, at det ved Rigsadvokatens datatræk i politiets sagsstyringssystem (POLSAS) ses, at der i 2024 blev rejst en sigtelse, en tiltale og skete fem 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.

Justitsministeriet vurderer, at oplysningerne fra PET og PET's Vurdering af Spionagetruslen mod Danmark af 2. maj 2023, oplysningerne fra FE og FE's Udsyn: Efterretningsmæssig Risikovurdering 2024 fra december 2024 samt oplysningerne fra Rigsadvokaten om ovennævnte straffesager og deres karakter understøtter, at der også de næste 12 måneder må forventes at være en alvorlig, reel og aktuel trussel mod Danmarks nationale sikkerhed fra spionage og fremmede staters efterretningsvirksomhed.

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

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

Ved vurderingen har Justitsministeriet bl.a. lagt vægt på SAMSIK's udtalelse ovenfor, hvoraf det bl.a. fremgår, at trusselsniveaet for cyberspionage og cyberkriminalitet mod Danmark er MEGET HØJT. Ifølge SAMSIK retter truslen fra cyberspionage sig især mod danske myndigheder og organisationer, som arbejder med udenrigs- og sikkerhedspolitik i bred forstand.

Justitsministeriet har endvidere lagt vægt på oplysningerne fra SAMSIK om, at truslen fra destruktive cyberangreb er MIDDEL. Ifølge SAMSIK står Danmark overfor et trusselsbillede, hvor destruktive cyberangreb er en reel mulighed, og Ruslands risikovillighed over for NATO-lande har øget sandsynligheden for, at Rusland vil udføre denne type cyberangreb mod bl.a. Danmark. SAMSIK vurderer dog, at det er mindre sandsynligt, at Rusland i den nuværende situation vil gennemføre destruktive cyberangreb mod

Danmark, men mindre omfattende destruktive cyberangreb kan stadig få betydelige konsekvenser for offeret og samfundet.

Det har desuden indgået i Justitsministeriets vurdering, at det er sandsynligt, at hackergrupper knyttet til Rusland løbende forbereder sig på at kunne udføre destruktive cyberangreb mod Danmark, og at sandsynligheden for, at disse angreb finder sted, derfor kan stige med kort eller uden varsel – særligt hvis konflikten mellem Rusland og Vesten eskalerer eller ændrer karakter.

Derudover har Justitsministeriet lagt vægt på, at FE vurderer, at Rusland udfører cyberspionage, og at Rusland har betydelige kapaciteter inden for denne efterretningsmetode.

Endelig noterer Justitsministeriet sig, at der ikke findes særskilte gerningskoder for cyberangreb og cyberspionage omfattet af straffelovens kapitel 12 og 13, og at Rigsadvokaten derfor ikke har kunnet trække tal på sigtelser, tiltaler eller domfældelser vedrørende cyberangreb og cyberspionage.

Det forhold, at der ikke foreligger tal på sigtelser, tiltaler eller domfældelser vedrørende cyberangreb og cyberspionage omfattet af straffelovens kapitel 12 og 13, kan efter Justitsministeriets opfattelse ikke føre til en ændret trusselsvurdering.

Justitsministeriet vurderer, at oplysningerne fra SAMSIK og SAMSIK's Vurdering af Cybertruslen mod Danmark 2024 fra september 2024, FE og FE's Udsyn: Efterretningsmæssig Risikovurdering 2024 fra december 2024 understøtter, at der også de næste 12 måneder må forventes en alvorlig, reel og aktuel trussel mod Danmarks nationale sikkerhed fra cyberangreb og cyberspionage.

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 2025 til og med den 29. marts 2026. Oplysninger registreret i medfør af disse regler vil skulle opbevares et år fra registreringstidspunktet.