UDENRIGSMINISTERIET
Center for Europa og Nordamerika

EKN, sagsnr.: 2019-511
Den 14. maj 2019

SAMLENOTAT

Horisontalt EU-sanktionsregime vedrørende cyberangreb

KOM-dokument foreligger ikke

Nyt notat

1. Resumé

På rådsmødet den 17. maj 2019 ventes en vedtagelse af et horisontalt EU-sanktionsregime vedrørende cyberangreb imod EU og dens allierede mhp. at styrke EU's mulighed for at forebygge, modstå og reagere på ondsindet cyberaktivitet. Det foreslåede sanktionsregime indebærer, at der kan iværksættes målrettede restriktive foranstaltninger i form af indefrysning af midler og indrejseforbud over for personer, grupper, virksomheder og enheder, der er ansvarlige for cyberangreb.

2. Baggrund

Rådet har fremlagt forslag om en afgørelse samt en forordning vedrørende sanktioner ifm. cyberangreb (herefter "forslaget").

Etableringen af et sanktionsregime ifm. cyberangreb sker som led i udmøntning af den omfattende cyberpakke, som EU-kommissionen fremlagde i september 2017. Pakken indeholder en lang række tiltag, der til sammen skal styrke EU's mulighed for at forebygge, modstå og reagere på cyberangreb. Bl.a. i form af en "cyberdiplomatisk værktøjskasse" for EU-svar på cyberangreb i regi af den fælles udenrigs- og sikkerhedspolitik. Redskaberne strækker sig fra dialog i den ene ende af spektret til mulige sanktioner i den anden. Den cyberdiplomatiske værktøjskasse blev udarbejdet pba. FAC-konklusioner fra juni 2017, som specifikt nævner, at muligheden for sanktioner ("restrictive measures") skal inkluderes heri.

Konklusionerne fra GAC den 20. november 2017 hilser tillige den cyberdiplomatiske værktøjskasse velkommen, og nævner også muligheden for brug af sanktioner som EU-respons på cyberangreb. Udenrigsministeren orienterede i den forbindelse den 15. november 2017 Folketingets Europaudvalg om regeringens støtte til rådskonklusionerne og understregede i den forbindelse, at EU's modsvar på cyberangreb ville spænde fra "diplomatisk dialog i den bløde ende til sanktioner i den hårdere ende". Udenrigsrådet vedtog den 16. april 2018 konklusioner, som fordømte de konkrete cyberangreb WannaCry og NotPetya (der bl.a. ramte Mærsk hårdt og kostede virksomheden op mod 2 mia. kr.). Heri refereredes igen til muligheden for sanktioner. DER den 28. juni 2018 opfordrede i sine konklusioner alle medlemslande, Kommissionen og Den Fælles Udenrigstjeneste til at udmønte cyberpakkens elementer (herunder anvendelsen af den cyberdiplomatiske værktøjskasse).

Rådets forslag sker herudover i overensstemmelse med DER-konklusionerne fra 18. oktober 2018 hvori Kommissionen og Den Fælles Udenrigstjeneste blev instrueret om at tage arbejdet med etablering af et cyber-sanktionsregime fremad.

Diskussioner i EU om konsekvenser i forbindelse med cyberangreb blev påbegyndt helt tilbage i februar 2015 med rådskonklusionerne på cyberdiplomati, men der har indtil nu ikke været nævneværdig fremgang mht. etableringen af et sanktionsregime på cyberområdet. Det er derfor glædeligt set fra et dansk synspunkt, at der nu opnås enighed om etableringen af et cybersanktionsregime.

3. Formål og indhold
Det foreslåede sanktionsregime indebærer, at der kan iværksættes målrettede restriktive foranstaltninger i form af indefrysning af midler og indrejseforbud over for personer, grupper, virksomheder og enheder i tredjelande, der er ansvarlige for eller yder økonomisk, teknisk eller materiel støtte ifm. cyberangreb imod EU, tredjelande eller internationale organisationer, hvor det er nødvendigt for at opnå de fælles udenrigs- og sikkerhedsmålsætninger efter EU-Traktatens art. 21. De restriktive foranstaltninger kan endvidere iværksættes over for personer, grupper, virksomheder og enheder, der tilskynder eller opfordrer andre personer, grupper, virksomheder og enheder til handlinger, som resulterer i eller bidrager til cyberangreb. Forslaget er det tredje tematiske EU-sanktionsregime i tillæg til de eksisterende sanktionsregimer mod spredning og brug af kemiske våben og terrorbekæmpelse. Virkefeltet er således ikke på forhånd afgrænset ift. personers, gruppers, virksomheders og enheders geografiske eller organisatoriske tilhørsforhold. Der er ved forslagets fremsættelse endnu ikke optaget nogen personer, grupper, virksomheder og enheder på den til forslaget tilhørende sanktionsliste. Nye personer grupper, virksomheder og enheder kan tilføjes ved enstemmighed.

4. Europa-Parlamentets udtalelser
Europa-Parlamentet skal ikke høres

5. Nærhedsprincippet
Spørgsmålet om nærhedsprincippet er ikke relevant

6. Gældende dansk ret
Ikke relevant

7. Konsekvenser
Forslaget forventes ikke at have lovgivningsmæssige konsekvenser eller væsentlige konsekvenser for statsfinanserne, samfundsøkonomien, miljøet eller beskyttelsesniveauet.

8. Høring
Forslaget har været i høring i myndighedsinteressentkreds vedr. EU-sanktioner (Specialudvalget for EU-sanktioner). Kredsen har ikke bemærkninger til forordningsudkastet.

9. Generelle forventninger til andre landes holdninger
Der er bred enighed iblandt medlemsstaterne om vigtigheden af hurtigst muligt at implementere EU's cyberpakke. Samtlige medlemsstater bakker derfor op om forslaget.

10. Regeringens generelle holdning

Danmark støtter et stadigt tættere internationalt samarbejde om at imødegå cybertrusler, ikke mindst i EU, med fastholdelse af, at operativ cybersikkerhed er national kompetence. Regeringen hilser derfor det store fokus på cybersikkerhed i EU velkomment, og finder, at en fælles EU-indsats øger muligheden for at imødegå cyber-truslen. I den forbindelse ses det fra dansk side vigtigt at give mulighed for at sanktionere de aktører, der står bag cyberangrebene. Derfor har man fra dansk side aktivt arbejdet for at få etableret cybersanktionsregimet, der forventes at styrke EU's mulighed for i fællesskab at kunne imødegå cyberangreb.

11. Tidligere forelæggelse for Folketingets Europaudvalg.
Forslaget har ikke tidligere været forelagt for Folketingets Europaudvalg. Jf. ovenfor orienterede udenrigsministeren den 15. november 2017 Europaudvalget om, at sanktioner ville være en del af EU's cyberdiplomatiske værktøjskasse.