FORSVARSMINISTERIET

UDENRIGSMINISTERIET

21. december 2023

UDLEVERINGSNOTAT: INTERNATIONALE SAMARBEJDER OM ATTRIBUERING OG MODSVAR PÅ CYBERANGREB

Internationale samarbejder vedr. muligheder for attribuering og modsvar på cyberangreb

Danmark spiller en aktiv rolle i det internationale samarbejde for en styrket afskrækkelse i cyberspace og for at understøtte implementeringen af international lov, normer og regler i cyberspace.

Danmark ønsker via offentlige attribueringer og sanktioner at udskamme og straffe ondsindede cyberaktører for at dæmme op for cyberangreb mod Danmark, partnere og allierede.

Det er en national beslutning, om Danmark offentligt skal attribuere et cyberangreb, samt evt. sanktionere aktørerne bag. Danmark vil dog altid i videst muligt omfang indgå i et tæt internationalt samarbejde med partnere og allierede i sager som vedrører modsvar på cyberangreb, bl.a. i rammen af EU og NATO. Dertil kommer, at Danmark indgår i en række internationale samarbejder blandt ligesindede lande, hvor modsvar på cyberangreb udvikles og koordineres.

Danmark har også mulighed for at udvise solidaritet gennem nationale støtte- og solidaritetserklæringer til offentlige attribueringer fra partnere og allierede. Dette skete senest baseret på en fælles EU-erklæring som følge af Storbritanniens offentlige attribuering af cyberangreb mod højtstående parlamentarikere og demokratiske institutioner til russiske trusselsaktører i december 2023.

EU's tilgang til svar på cyberangreb
Der er i EU et ønske om en fælleseuropæisk tilgang til svar på eksterne cyberangreb mod EU, EU's medlemslande og mod partnerlande. Rammen for EU's fælles reaktion på ondsindede cyberaktiviteter er nedfældet i den cyberdiplomatiske værktøjskasse. Værktøjskassen blev etableret i 2017 i regi af den fælles udenrigs- og sikkerhedspolitik, og den revideres løbende i takt med den sikkerhedspolitiske udvikling.

De mulige modsvar i den cyberdiplomatiske værktøjskasse strækker sig fra dialog i den ene ende af spektret til sanktioner i den anden ende. Formålet med værktøjskassen er at forhindre, afskrække eller modsvare cyberangreb. Brugen af værktøjskassen følger bl.a. hovedprincippet om, at EU's fælles reaktion på ondsindede cyberaktiviteter skal stå i rimeligt

forhold til cyberaktivitetens omfang, størrelse, varighed, intensitet, kompleksitet, karakter og virkninger, samt overholde gældende international ret og ikke krænke grundlæggende rettigheder og friheder.

Offentlig attribuering er en beslutning, som EU's medlemsstater kan foretage individuelt eller koordineret. Sanktionering kræver dog enighed blandt medlemsstaterne. Her vil det være en forudsætning, at tilstrækkelige beviser, der peger på en aktør som værende ansvarlig for cyberangrebet, deles med de øvrige EU-medlemsstater, med henblik på at kunne få deres opbakning.

Den cyberdiplomatiske værktøjskasse har siden etableringen været brugt aktivt til at koordinere fælleseuropæiske attribueringer af cyberangreb mod medlemsstater eller partnerlande, til solidaritetserklæringer i relation til partneres attribueringer af cyberangreb og til at nedlægge sanktioner mod aktører bag cyberangreb mod medlemsstater.

NATO's strategiske svarmuligheder på ondsindet cyberaktivitet
Der er i NATO ligeledes et ønske om en stærk fælles tilgang til effektive og passende svar på ondsindet cyberaktivitet rettet mod Alliancen, dens interesser og dens allierede samt mod partnere. NATO er ligesom EU en værdifuld platform for politisk konsultation og koordination, hvor allierede kan skabe fælles situationsbevidsthed, styrke informationsdeling samt koordinere eventuelle modsvar mod ondsindet cyberaktivitet.

Rammen for samarbejdet om offentlig attribuering og eventuelle modsvar på ondsindet cyberaktivitet i regi af NATO er nedfældet i NATO's guide til strategiske svarmuligheder til ondsindet cyberaktivitet fra 2019.

Offentlig attribuering af, samt modsvar på, et cyberangreb, er en beslutning, som NATO-allierede kan foretage individuelt, bilateralt eller multilateralt efter et ad hoc princip. Allierede kan ligeledes vælge at koordinere en samlet NATO-attribuering samt undersøge muligheden for kollektive svar på ondsindet cyberaktivitet. En kollektiv attribuering af ondsindet cyberaktivitet kræver forudgående godkendelse i Det Nordatlantiske Råd (NAC), som er NATO's politiske beslutningsorgan.

Individuelle eller koordinerede NATO-modsvar på ondsindet cyberaktivitet kan være skærpet dialog i den ene ende af spektret til proportionelle modsvar som følge af brud på international lovgivning i den anden ende.