JUSTITSMINISTERIET
Politi- og Strafferetsafdelingen

Folketinget
Kommunaludvalget
Christiansborg
1240 København K

Dato: 25. juni 2013
Kontor: Strafferetskontoret
Sagsbeh: Jean Elisabeth Hørdum
Sagsnr.: 2013-0032-0719
Dok.: 754185

Hermed sendes endelig besvarelse af spørgsmål nr. 95 (Alm. del), som Folketingets Kommunaludvalg har stillet til justitsministeren den 22. april 2013. Spørgsmålet er stillet efter ønske fra Michael Aastrup Jensen (V).

Morten Bødskov

/

Lise Bitsch

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 95 (Alm. del) fra Folketingets Kommunaludvalg:

> ”Vil ministeren oplyse strafferammen for at begå DDoS-angreb og tilsvarende angreb på den digitale infrastruktur, og i hvilket omfang der rejses sigtelser og fældes dom i denne type sager, samt niveauet for de straffe der udmåles ved domfældelse?”

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Rigsadvokaten og fra Rigspolitiet. Rigspolitiets udtalelse er sendt via Rigsadvokaten.

Rigsadvokaten har oplyst følgende:

> ”**1.** Jeg kan i den forbindelse oplyse, at Rigspolitiet til brug for mit bidrag til besvarelsen af spørgsmålet har oplyst, at DDoS står for ”Distributed Denial of Service” og er betegnelsen for et it-angreb, hvor der fra et større antal computere på samme tid iværksættes en stor mængde forespørgsler til den samme internetadresse. Herved belastes den pågældende server i en sådan grad, at reelle forespørgsler til serveren kun i begrænset omfang kan besvares, eller at serveren på grund af overbelastning helt ophører med at fungere.
>
> Et angreb af den beskrevne karakter kan iværksættes ved, at gerningsmanden ved hjælp af et frit tilgængeligt stykke software udøver kontrol over en større mængde (ofte tusindvis) inficerede computere.
>
> **2.** It-angreb af denne karakter kan som udgangspunkt straffes efter reglen i straffelovens § 293, stk. 2. Efter denne bestemmelse straffes således den, der uberettiget hindrer en anden i helt eller delvis at råde over ting med bøde eller fængsel indtil 1 år. Bestemmelsen omfatter efter forarbejderne bl.a. elektroniske rådighedshindringer, som lægger beslag på den angrebnes it-system og derved hindrer vedkommende helt eller delvist i at bruge systemet. I betænkning nr. 1417/2002 om it-kriminalitet, der ligger til grund for bestemmelsen, nævnes som et andet eksempel blokering af et anlæg gennem uafbrudt transmission eller ved, at serveren uafbrudt bliver bedt om at sende sin IP-adresse.
>
> Straffen for overtrædelse af straffelovens § 293, stk. 2, kan stige til fængsel i 2 år, hvor der er tale om overtrædelser af mere systematisk eller organiseret karakter, eller der i øvrigt foreligger særligt skærpende omstændigheder. Ved vurderingen heraf

kan der navnlig lægges vægt på rådighedshindringens omfang og varighed.

Hvis der ved et it-angreb fremkaldes omfattende forstyrrelse i driften af centrale it-systemer, vil forholdet også kunne straffes efter reglen i straffelovens § 193, stk. 1. Efter denne bestemmelse straffes således bl.a. den, der på retsstridig måde fremkalder omfattende forstyrrelse i driften af informationssystemer, med bøde eller fængsel indtil 6 år.

Hvis der ved angrebet sker beskadigelse af det angrebne it-system, f.eks. således at den hidtidige adgang til systemet umuliggøres eller besværliggøres, vil forholdet tillige kunne straffes som hærværk efter straffelovens § 291. Efter denne bestemmelse straffes således bl.a. den, der ødelægger eller beskadiger ting, der tilhører en anden, med bøde eller fængsel indtil 1 år og 6 måneder.

Efter bestemmelsens stk. 2 kan straffen stige til fængsel i 6 år, hvis der øves hærværk af betydeligt omfang eller af mere systematisk eller organiseret karakter, eller hvis gerningsmanden tidligere er fundet skyldig i hærværk mv. Hærværk i betydeligt omfang foreligger ikke alene, hvor den skete ødelæggelse har et betydeligt fysisk omfang, men også hvor der er ødelagt betydelige værdier. Der kan endvidere lægges vægt på, om handlingen har medført betydelige efterfølgende skadevirkninger for de ramte.

I helt særlige tilfælde vil et it-angreb af den karakter, der er nævnt i spørgsmålet, kunne anses som en terrorhandling omfattet af straffelovens § 114, stk. 1, nr. 4, såfremt overtrædelsen begås på en måde, der kan bringe menneskeliv i fare eller forårsage betydelige økonomiske tab. Forbrydelsen skal endvidere være begået med terrorismeforsæt (f.eks. forsæt til at skræmme befolkningen i alvorlig grad) og skal kunne tilføje et land mv. alvorlig skade. Overtrædelse af § 114, stk. 1, nr. 4, straffes med fængsel indtil på livstid.

3. Sager om it-angreb af den karakter, der er nævnt i spørgsmålet, er ikke registreret under en selvstændig journalkode i politiets sagsstyringssystem (POLSAS), og det er derfor ikke umiddelbart muligt at give præcise oplysninger om antallet af sigtelser og domfældelser og om strafniveauet i eventuelle sager. Dette vil forudsætte en ressourcekrævende manuel gennemgang af sager i politikredsene. En sådan gennemgang har jeg på det foreliggende grundlag ikke fundet anledning til at iværksætte.

Jeg kan dog til orientering oplyse, at antallet af sigtelser for overtrædelse af straffelovens § 293, stk. 2, inden for de seneste fem år fordeler sig således:

2008	2009	2010	2011	2012
15	3	2	10	20

I samme periode ser antallet af fældende afgørelser (domme, bødeforelæg mv.) for overtrædelse af straffelovens § 293, stk. 2, således ud:

2008	2009	2010	2011	2012
7	9	3	5	9

Opmærksomheden henledes på, at straffelovens § 293, stk. 2, ikke alene omfatter it-angreb, men også andre former for rådighedshindringer, og at de anførte tal derfor ikke nødvendigvis kun omfatter it-angreb."