

Modtaget via elektronisk post. Der tages forbehold for evt. fejl

Europaudvalget  
(Alm. del - bilag 186)  
retlige og indre anliggender ministerråd  
(Offentligt)

Medlemmerne af Folketingets Europaudvalg  
og deres stedfortrædere

Bilag	Journalnummer	Kontor	
1	400.C.2-0	EU-sekr.	7. november 2002

Til underretning for Folketingets Europaudvalg vedlægges Justitsministeriets grundnotat om forslag til rammeafgørelse om angreb på informationssystemer.

Kære<DOCUMENT\_START> udenrigsminister.

Vedlagt sender jeg et forslag til rammeafgørelse om angreb på informationssystemer tillige med et grundnotat om forslaget, idet jeg skal anmode om, at materialet oversendes til Folketingets Europaudvalg.

Det bemærkes, at materialet ligeledes vil blive oversendt til Folketingets Retsudvalg.

Med venlig hilsen

## **GRUNDNOTAT**

**om**

### **forslag til rammeafgørelse om angreb på informationssystemer**

#### **1. Baggrund**

I en meddelelse af 19. april 2002 til Rådet og Europa-Parlamentet (KOM(2002)173 endelig) har Kommissionen fremsat et forslag til rammeafgørelse om angreb på informationssystemer.

Formålet med forslaget til rammeafgørelse er bl.a. på baggrund af konklusionerne fra Det Europæiske Råd i Tampere den 15. – 16. oktober 1999 at sikre, at der sker en tilnærmelse af medlemslandenes lovgivning for så vidt angår bekæmpelse af højteknologikriminalitet.

Formålet med forslaget til rammeafgørelse er endvidere at supplere en række tiltag i EU-regi vedrørende IT-kriminalitet.

Kommissionen har ved udarbejdelsen af forslaget til rammeafgørelse taget højde for de resultater, der er opnået i Europarådet i forbindelse med udarbejdelsen af konventionen af 23. november 2001 om IT-kriminalitet. Europarådets konvention om IT-kriminalitet blev åbnet for undertegnelse i november 2001.

## 2. Indhold

Retsgrundlaget for forslaget til rammeafgørelse er artikel 29, artikel 30, stk. 1, litra a), artikel 31 og artikel 34, stk. 2, litra b), i Traktaten om Den Europæiske Union.

Artikel 1 indeholder en beskrivelse af rammeafgørelsens anvendelsesområde og formål. Formålet med rammeafgørelsen er at foretage en indbyrdes tilnærmelse af medlemsstaternes strafferetlige regler vedrørende angreb på informationssystemer med henblik på at forbedre samarbejdet mellem medlemsstaternes myndigheder, herunder de retshåndhævende myndigheder.

Artikel 2 indeholder definitioner af visse udtryk i rammeafgørelsen.

Ved "elektronisk kommunikationsnet" forstås transmissionssystemer og, hvor det er relevant, koblings- og dirigeringsudstyr og andre hjælpemidler, som giver mulighed for at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnetværk, faste (kredsløbs- eller pakkekoblede net, herunder Internettet) og mobile jordbaserede netværk, elkabelsystemer, der anvendes til fremføring af signaler, netværk til radio- og tv-spredning og kabel-tv-net, uanset hvilken type information der overføres. Definitionen svarer til definitionen i direktivet af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet- og tjenester (EFT2002/L108/33).

Ved "computer" forstås enhver anordning eller gruppe af indbyrdes forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af computerdata.

Ved "computerdata" forstås enhver form for gengivelse af faktuelle oplysninger, information eller begreber, som er redigeret i eller omdannet til et format, der egner sig til behandling i et informationssystem, herunder et program, som kan anvendes til at få et informationssystem til at udføre en funktion.

Ved "informationssystem" forstås computere og elektroniske kommunikationsnet samt computerdata, som lagres, behandles, kaldes frem eller overføres i forbindelse med et informationssystems drift, brug, beskyttelse og vedligeholdelse.

For så vidt angår "juridiske personer" henvises til national ret, således at der ved begrebet forstås enhver enhed, der i national ret har status af juridisk person, dog ikke stater, offentlige organer under udøvelsen af offentlig myndighed og offentlige internationale organisationer.

Ved "autoriseret person" forstås enhver fysisk eller juridisk person, som ved kontrakt, lov eller tilladelse f.eks. har ret til at bruge, forvalte, kontrollere, teste eller udføre videnskabelig forskning ved hjælp af et informationssystem.

For så vidt angår definitionen af "uretmæssig" henvises til national ret, således at der ved begrebet forstås, at en handling i henhold til national ret ligger uden for rammerne af en autoriseret persons adfærd eller anden lovlig adfærd.

Artikel 3 forpligter medlemsstaterne til at kriminalisere forsætlig uretmæssig adgang til et informationssystem ("hacking"), eller en del heraf, når den pågældende handling:

- a. er rettet mod en del af et informationssystem, som er udstyret med specifikke beskyttelsesforanstaltninger,
- a. begås for at forvolde en fysisk eller juridisk person skade, eller
- a. begås for at opnå en økonomisk gevinst.

Artikel 4 vedrører ulovlig forstyrrelse af informationssystemer.

Efter artikel 4, litra a), forpligtes medlemsstaterne til at kriminalisere forsætlig uretmæssig adfærd, som udgør et alvorligt indgreb, der består i at udføre alvorlige hindringer eller afbrydelser af et informationssystems drift, når dette sker ved at tilføre eller sende et informationssystem computerdata. Medlemsstaterne forpligtes endvidere til at kriminalisere alvorlige hindringer eller afbrydelser af et informationssystems drift, når dette sker ved at beskadige, slette, forvanske, ændre, tilsløre eller hindre adgang til et informationssystem computerdata. Den første del af bestemmelsen retter sig mod den situation, hvor et informationssystem udsættes for et såkaldt "Denial-of-Service" angreb. Et "Denial-of-Service" indebærer, at almindelig brug af systemet hindres eksempelvis ved gentagne fremsendelser af så store mængder e-mails, at systemet overbelastes. Den anden del af bestemmelsen retter sig bl.a. mod udbredelse af virus.

Efter artikel 4, litra b), forpligtes medlemsstaterne til at kriminalisere forsætlig uretmæssig adfærd, som udgør et alvorligt indgreb, der består i at slette, forvanske, ændre, tilsløre eller hindre adgang til computerdata i et informationssystem med henblik på at forvolde en fysisk eller juridisk person skade. Denne adfærd dækker virusangreb på et informationssystems indhold (computerdata).

Det følger af artikel 5, at medlemsstaterne skal kriminalisere medvirken til og forsøg på de i artikel 3 og 4 omhandlede lovovertrædelser.

Artikel 6 forpligter medlemsstaterne til at sikre, at de i artikel 3, 4 og 5 opregnede lovovertrædelser straffes med effektive, proportionale og afskrækkende sanktioner, der i alvorlige tilfælde som minimum har en strafferamme på fængsel indtil 1 år. Alvorlige tilfælde omfatter ikke handlinger, hvor den udviste adfærd ikke har forvoldt skade eller medført økonomisk gevinst. Endvidere følger det af bestemmelsen, at der skal være mulighed for at idømme bøder i tillæg til eller som alternativ til frihedsstraf.

I artikel 7 pålægges medlemsstaterne at sikre, at strafferammen for de i artikel 3, 4 og 5 nævnte lovovertrædelser som minimum er fængsel indtil 4 år, når en række skærpende omstændigheder foreligger. Det drejer sig om tilfælde, hvor lovovertrædelser:

- a. er begået inden for rammerne af en kriminel organisation,
- a. skaber eller fører til betydelige direkte eller indirekte økonomiske tab, tilføjer en fysisk person skade eller tilføjer en del af medlemsstatens kritiske infrastruktur betydelig skade, eller
- a. fører til betydelig gevinst.

Endvidere forpligtes medlemsstaterne til at sikre, at de i artikel 3 og 4 nævnte lovovertrædelser i gentagelsestilfælde straffes med strengere straffe end straffen i henhold til artikel 6.

Efter artikel 8 skal medlemslandene sikre, at den kompetente myndighed kan nedsætte straffen, hvis lovovertrædelserne alene har medført mindre skade.

Artikel 9 indeholder nærmere regler for juridiske personers strafansvar. Bestemmelsen forpligter medlemsstaterne til at sikre, at juridiske personer kan gøres strafferetligt ansvarlige med hensyn til de handlinger, der er omfattet af forslaget, i det omfang handlingerne er begået for at skaffe den juridiske person vinding og er begået af en person, der handler enten individuelt eller som medlem af et organ, der handler på vegne af den juridiske person.

Endvidere forpligtes medlemsstaterne til at sikre, at juridiske personer også kan straffes i tilfælde, hvor f.eks. utilstrækkelig kontrol eller tilsyn fra den juridiske persons side har gjort det muligt for en person, der er underlagt den juridiske persons myndighed, at begå de nævnte lovovertrædelser.

Efter forslaget artikel 10 er medlemsstaterne forpligtede til at sikre, at der overfor juridiske personer kan iværksættes sanktioner, der er effektive, proportionale og virker afskrækkende, herunder bødestraf eller andre sanktioner, som f.eks. fratagelsen af retten til at modtage offentlige ydelser og tilskud samt forbud mod at udøve erhvervsaktivitet.

Artikel 11 indeholder bestemmelser om straffekompetence og forpligter bl.a. medlemsstaterne til at etablere straffemyndighed, når lovovertrædelserne er begået helt eller delvist på medlemslandets territorium. Medlemsstaterne forpligtes i den forbindelse til at etablere straffekompetence i det tilfælde, hvor gerningsmanden begår lovovertrædelserne, mens han fysisk befinder sig på landets område, uanset om lovovertrædelserne er rettet mod et informationssystem på dette område. Herudover forpligtes medlemsstaterne til at etablere straffekompetence i det tilfælde, hvor lovovertrædelserne begås mod et informationssystem på landets område, uanset om gerningsmanden på gerningstidspunktet fysisk befandt sig på landets område. Endvidere forpligter bestemmelsen medlemsstaterne til at samarbejde i sager, hvor flere medlemsstater har straffekompetence.

Artikel 12 indeholder bestemmelser om udveksling af oplysninger om de lovovertrædelser, der er omfattet af rammeafgørelsen. Bestemmelsen forpligter medlemsstaterne til at oprette operationelle kontaktpunkter, der fungerer 24 timer i døgnet.

I artikel 13 fastslås det, at medlemsstaterne senest den 31. december 2003 skal have truffet de nødvendige foranstaltninger for at gennemføre rammeafgørelsen i national ret, mens det af artikel 14 fremgår, at rammeafgørelsen træder i kraft 20 dage efter offentliggørelsen i EF-Tidende.

### 3. Dansk ret

#### 3.1. Straffelovens bestemmelser, der finder anvendelse i relation til IT-kriminalitet

Straffelovrådet afgav i 1985 betænkning nr. 1032/1985 om datakriminalitet. På grundlag af betænkningen gennemførtes i 1985 en række straffelovsændringer, herunder ændring af straffelovens § 193 samt indsættelse af straffelovens §§ 263, stk. 2 og 3, samt 279 a.

Efter straffelovens § 193, stk. 1, straffes den, som på retsstridig måde fremkalder omfattende forstyrrelse i driften af almindelige samfærdselsmidler, offentlig postbesørgelse, telegraf- eller telefonanlæg, radio- eller fjernsynsanlæg, databehandlingsanlæg, eller anlæg, der tjener til almindelig forsyning med vand, gas, elektrisk strøm eller varme, med fængsel indtil 4 år eller under formildende omstændigheder med bøde.

"Databehandlingsanlæg" blev tilføjet bestemmelsen ved ovennævnte lovændringer i 1985. Det fremgår af bemærkningerne til bestemmelsen, at udtrykkene "omfattende forstyrrelse i driften" og "almenskadelig karakter" angiver, at der må anlægges en kvantitativ vurdering af angrebets omfang, og at man formentlig herved må lægge afgørende vægt på størrelsen af den personkreds, der berøres af angrebet. Som eksempel nævnes, at en af storbanks centrale dataanlæg helt sættes ud af funktion. Derimod vil en betydelig driftsforstyrrelse af en bankfilials dataterminal ikke være omfattet af bestemmelsen.

Efter straffelovens § 263, stk. 2, straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling, med fængsel indtil 6 måneder. Begås forholdet med fortsat til at skaffe sig eller gøre sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder eller under andre særlig skærpende omstændigheder, kan straffen efter straffelovens § 263, stk. 3, stige til fængsel indtil 4 år.

For databedrageri straffes efter straffelovens § 279 a den, som for derigennem at skaffe sig eller andre uberettiget vinding retsstridigt ændrer, tilføjer eller sletter oplysninger eller programmer til elektronisk databehandling eller i øvrigt retsstridigt forsøger at påvirke resultatet af sådan databehandling. Efter straffelovens § 285 straffes databedrageri med fængsel indtil 1 og 6 måneder. Det følger af straffelovens § 286, stk. 2, at straffen for databedrageri kan stige til fængsel i 8 år, når forbrydelsen er af særlig grov beskaffenhed, eller når der er begået et større antal forbrydelser.

Efter straffeloven § 291, stk. 1, straffes den, som ødelægger, beskadiger eller bortskaffer ting, der tilhører en anden, med bøde eller fængsel indtil 1 år. Hvis der øves hærværk af betydeligt omfang, eller hvis gerningsmanden tidligere er fundet skyldig i hærværk eller overtrædelse af straffelovens §§ 180, 181, 183, stk. 1 og 2, 184, stk. 1, 193 eller 194, kan straffen efter straffelovens § 291, stk. 2, stige til fængsel i 4 år.

Herudover straffes efter straffelovens § 293, stk. 2, den, som lægger hindringer i vejen for, at nogen udøver sin ret til at råde over eller tilbageholde en ting, med bøde eller under skærpende omstændigheder med fængsel indtil 6 måneder.

#### 3.2. Forsøg og medvirken

Efter straffelovens § 21, stk. 1, straffes handlinger, som sigter til at fremme eller bevirke udførelsen af en forbrydelse, når den ikke fuldbyrdes som forsøg. Efter bestemmelsens stk. 3 straffes forsøg kun, når der for lovovertrædelsen kan idømmes en straf, der overstiger fængsel i 4 måneder.

Efter straffelovens § 23, stk. 1, 1. pkt., omfatter den for en lovovertrædelse givne straffebestemmelse alle, der ved tilskyndelse, råd eller dåd har medvirket til handlingen.

#### 3.3. Bestemmelser om straffastsættelse

Straffelovens kapitel 10 indeholder bestemmelser om straffastsættelse.

Efter straffelovens § 80, stk. 1, skal der ved straffens udmåling tages hensyn til lovovertrædelsens grovhed og til oplysninger om gerningsmandens person, herunder om hans almindelige personlige og sociale forhold, hans forhold før og efter gerningen samt hans bevæggrunde til denne. Efter straffelovens § 80, stk. 2, vil det forhold, at gerningen er begået af flere i forening, i reglen være at anse som en skærpende omstændighed.

Efter straffelovens § 81 er det en betingelse for anvendelsen af bestemmelser om forhøjet straf eller andre retsfølger i gentagelsestilfælde, at gerningsmanden, inden han på ny forbrød sig, i den danske stat er fundet skyldig i en efter det fyldte 18. år begået strafbar handling, som loven tillægger gentagelsesvirkning på den nu begåede, eller i forsøg på eller medvirken til en sådan. Efter straffelovens § 81, stk. 2, kan retten tillægge straffedomme afsagte uden for den danske stat samme gentagelsesvirkning som de her i landet afsagte. Gentagelsesvirkningen ophører efter straffelovens § 81, stk. 3, når der førend den nye strafbare handling blev begået, er forløbet 5 år, efter at den tidligere straf er udstået, endeligt eftergivet eller bortfaldet.

I retspraksis tillægges forstraffe endvidere betydning for strafudmålingen uafhængigt af, om der foreligger særskilte bestemmelser om forhøjet straf eller strengere retsfølger i gentagelsestilfælde. Domstolene kan således tage straffe for lovovertrædelser begået før det fyldte 18. år i betragtning, ligesom domstolene ved strafudmålingen kan lægge vægt på forstraffe, der ligger mere end 5 år tilbage. Udenlandske domme kan også tillægges betydning i disse gentagelsessituationer.

### 3.4. Bøde

Det fremgår af straffelovens § 50, at bøder tilfalder statskassen, og at bøde kan idømmes som tillægsstraf til en anden strafart, når tiltalte ved lovovertrædelsen har opnået eller tilsigtet at opnå økonomisk vinding for sig selv eller andre. Den bødefældte kan ikke kræve bøden betalt eller erstattet af andre.

### 3.5. Juridiske personers strafansvar

Efter straffelovens § 25 kan en juridisk person straffes med bøde, når dette er bestemt ved lov eller i medfør af lov.

I forlængelse heraf følger det af straffelovens § 306, at selskaber (juridiske personer m.v.) kan pålægges strafansvar for overtrædelse af straffeloven.

### 3.6. Straffemyndighed

Under dansk straffemyndighed hører efter straffelovens § 6 handlinger, som foretages i den danske stat, på dansk fartøj, som befinder sig uden for nogen stats folkeretligt anerkendt område, samt på dansk fartøj, som befinder sig på fremmed folkeretligt anerkendt område, af personer, der hører til fartøjet eller som rejsende følger med dette.

Efter straffelovens § 7, stk. 1, hører endvidere under dansk straffemyndighed handlinger, som en person, der har dansk indfødsret eller er bosat i en den danske stat, har foretaget uden for denne, for så vidt handlingen er foretaget uden for folkeretligt anerkendt statsområde, hvis handlinger af den pågældende art kan medføre højere straf end fængsel i 4 måneder, eller for så vidt handlingen er foretaget inden for s&ari ng;dant område, hvis den er strafbar også efter den dér gældende lovgivning.

Endvidere hører handlinger foretagne uden for den danske stat, uanset hvor gerningsmanden hører hjemme, under dansk straffemyndighed efter straffelovens § 8, nr. 6, når udlevering af sigtede til retsforfølgning i et andet land afslås, og handlingen, for så vidt den er foretaget inden for folkeretligt anerkendt statsområde, er strafbar efter den dér gældende lovgivning, og den efter dansk ret kan medføre højere straf end fængsel i 1 år.

Herudover følger det af straffelovens § 9, at i de tilfælde, i hvilke en handlingens strafbarhed afhænger af eller påvirkes af en indtrådt eller tilsigtet følge, betragtes handlingen tillige som foretaget dér, hvor virkningen er indtrådt eller tilsigtet at skulle indtræde.

### 3.7. Informationsudveksling

Danmark er tilsluttet G8-landenes 24-timers/7 dages informationsnet til bekæmpelse af højteknologikriminalitet. Rigspolitichefens Kommunikationscenter er i den forbindelse udpeget som kontaktpunkt, og centeret har døgnet rundt en specialist i højteknologikriminalitet fra Nationalt Efterforskningsstøttecenter (NEC) tilknyttet. Denne specialist kan formidle kontakt til den relevante politikreds, der vil kunne træffe operative foranstaltninger.

## 4. Lovgivningsmæssige og statsfinansielle konsekvenser

Pligten til at kriminalisere den adfærd, der er nævnt i artikel 3 i udkastet til rammeafgørelse, må anses som opfyldt ved straffelovens § 263, stk. 2. Bestemmelsens anvendelsesområde dækker bl.a. den indtrængen, der begås af udenforstående ("hacking"), samt den indtrængen, der begås af personer, der i kraft af ansættelsesforhold eller lignende har lovlige opgaver med hensyn til betjening af et anlæg, men som går ud over det, den pågældende er bemyndiget til at foretage sig.

Straffelovens § 263, stk. 2, indeholder ikke et krav om, at den pågældende adfærd skal være udført i forhold til et informationssystem, hvortil der er etableret særlige sikkerhedsforanstaltninger, ligesom bestemmelsen ikke stiller krav om, at adfærden udøves med henblik på at forvolde en fysisk eller juridisk person skade eller for opnå en økonomisk gevinst.

Derimod lægger domstolene ved strafudmålingen bl.a. vægt på, om der har været en rimelig sikkerhed eller kontrol, eller om en eventuel mangel på sikkerhed har muliggjort, at kriminaliteten har fået et særligt stort omfang.

Det må endvidere antages, at den adfærd, der er omfattet af forslaget artikel 3, litra ii), og som består i at skaffe sig adgang til en informationssystem for at forvolde en fysisk eller juridisk person skade, i visse tilfælde vil kunne omfattes af straffelovens § 263, stk. 3. Det kan eksempelvis være forbundet med betydelige skadevirkninger for en virksomhed, at der skaffes oplysninger om dennes erhvervshemmeligheder.

Herudover må det antages, at den adfærd, der er omfattet af forslaget artikel 3, litra iii), og som består i at skaffe sig uretmæssig adgang til informationssystem for at opnå en økonomisk gevinst, i visse tilfælde vil kunne være omfattet af straffelovens § 279 a om databedrageri. Det vil f.eks. være tilfældet i den situation, hvor en person trænger ind i en banks computersystem med henblik på retsstridigt at overføre beløb til sin egen konto.

Den adfærd, der er nævnt i artikel 4, litra a), i udkastet til rammeafgørelse indeholder dels en pligt til at kriminalisere adfærd, der består i at hindre eller afbryde et informationssystems drift ved at tilføre eller sende det computerdata, dels en pligt til at kriminalisere adfærd, der hindrer eller afbryder et informationssystems drift ved beskadigelse, sletning, ændring m.v. af informationssystemets computerdata.

Den første situation retter sig bl.a. mod det tilfælde, hvor et informationssystem udsættes for et såkaldt "Denial-of-Service" angreb, der hindrer almindelig brug af systemet ved at udvirke overbelastning eller nedbrud. Den øvrige adfærd, der er beskrevet i artikel 4, litra a), retter sig bl.a. mod udspredelse af virus, der har til formål at hindre eller afbryde driften af selve informationssystemet typisk ved at ændre eller slette computerdata i informationssystemet

Pligten til at kriminalisere den adfærd, der består i at hindre eller afbryde et informationssystems drift ved at beskadige, slette, forvanske, ændre eller tilsløre informationssystemets computerdata må anses for opfyldt ved hærværksbestemmelsen i straffelovens § 291, stk. 1.

Anderledes forholder det sig med den del af gerningsindholdet, der består i at hindre eller afbryde et informationssystems drift ved at tilføre eller sende informationssystemet computerdata eller ved at hindre adgang til informationssystemets computerdata, idet der i disse tilfælde ikke forekommer ødelæggelse eller beskadigelse af ting.

Adfærden vil imidlertid efter omstændighederne kunne anses for omfattet af straffelovens § 293, stk. 2, der bl.a. vedrører tilfælde, hvor man lægger hindringer i vejen for, at nogen udøver sin ret til at råde over en ting.

Det er tilsvarende vurderingen, at pligten til at kriminalisere den adfærd, der er nævnt i artikel 4, litra b), i udkastet til rammeafgørelse, vil kunne anses for opfyldt ved straffelovens §§ 291 og 293, stk. 2. Det bemærkes, at straffelovens § 291 alene stiller krav om, at adfærden har medført ødelæggelse, beskadigelse m.v. Derimod indeholder § 291 ikke betingelse om, at adfærden er foretaget med henblik på at forvolde en fysisk eller juridisk person skade. Tilsvarende gør sig gældende i relation til straffelovens § 293, stk. 2.

Det bemærkes, at straffelovens §§ 291 og 293, stk. 2, ikke oprindeligt er udformet med henblik på IT-kriminalitet. Det kan således ikke afvises, at en uændret vedtagelse af denne del af rammeafgørelsen vil kræve lovændringer, idet bestemmelserne eventuelt bør tilpasses adfærd, der vedrører IT-kriminalitet. Det tilføjes, at betænkning nr. 1417/2002 om IT-kriminalitet bl.a. behandler spørgsmålet om, hvorvidt der er klar strafferetlig dækning inden for alle hærværksområder i relation til elektronisk databehandling. Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet (Brydsholt-udvalget) påpeger i betænkningen, at den strafferetlige dækning af området ikke er helt klar og foreslår på den baggrund, at straffelovens § 293, stk. 2, ændres, således at det klart fremgår, at bestemmelsen også omfatter rådighedshindring ad elektronisk vej.

Forslagets bestemmelser om forsøg og medvirken må anses som opfyldt i kraft af bestemmelserne i straffelovens §§ 21 og 23.

Efter forslaget artikel 6 forpligtes medlemsstaterne til at sikre, at lovovertrædelser omfattet af rammeafgørelsen i alvorlige tilfælde kan straffes med fængsel i ikke under 1 år, idet alvorlige tilfælde ikke omfatter forhold, hvor lovovertrædelserne ikke forvoldte skade eller medførte økonomisk gevinst.

Det fremgår ikke klart af forslaget artikel 6, stk. 1, om formuleringen "forvoldte skade eller medførte økonomisk gevinst" henviser til rammeafgørelsens enkelte bestemmelser, der vedrører adfærd med henblik på skadeforvoldelse og økonomisk vinding, eller om bestemmelsen generelt henviser til adfærd, der har forvoldt skade eller medført økonomisk gevinst.

I det omfang der er tale om en generel henvisning til handlinger, der har forvoldt skade eller medført økonomisk gevinst bemærkes, at dansk ret som udgangspunkt alene straffer forsætlig adfærd. Det vil som udgangspunkt sige, at gerningsmanden skal have haft til hensigt eller have anset det som overvejende sandsynligt, at handlingen indebærer skade eller medfører økonomisk vinding.

Strafferammen for overtrædelse af straffelovens § 263, stk. 2, er 6 måneder, idet straffen efter straffelovens § 263, stk. 3, kan stige til fængsel indtil 4 år, hvis forholdet begås med fortsæt til at skaffe sig eller gøre sig bekendt med oplysninger om erhvervshemmeligheder eller under andre særlig skærpende omstændigheder.

Bemærkningerne til straffelovens § 263, stk. 3, præciserer ikke nærmere, hvad der ligger i ordene "eller under andre særlig skærpende omstændigheder". I Straffelovrådets betænkning nr. 1032/1985 om datakriminalitet nævnes, at det kan være vanskeligt præcist at angive, hvad der bør kunne medføre strafskærpende, samt at rådet bl.a. har haft tilfælde for øje, hvor en

udnyttelse eller videregivelse af oplysningerne kan være forbundet med betydelige skadevirkninger. Som eksempel nævnes adgang til offentlige edb-registre.

Det må imidlertid anses for tvivlsomt, om det økonomiske tab i form af udgifter til kontrol og lignende – og dermed den skade, der er forbundet med, at en person skaffer sig adgang til et informationssystem – er omfattet af "andre skærpene omstændigheder", idet et sådant indgreb sædvanligvis er forbundet med betydelige genoprettelsesomkostninger.

På den baggrund er det vurderingen, at forslaget vil nødvendiggøre en ændring af strafferammen i straffelovens § 263, stk. 2, i relation til den adfærd, der er omfattet af forslagets artikel 3, litra i). Det bemærkes, at Brydesholt-udvalget i betænkning nr. 1417/2002 om IT-kriminalitet foreslår, at strafmaksimum i straffelovens § 263, stk. 2, forhøjes til fængsel i 1 år og 6 måneder. Udvalget anfører i den forbindelse, at strafferammen bør afspejle, at hacking er alvorligt indgreb for de fleste virksomheder

Som nævnt ovenfor vil den adfærd, der er omfattet af forslagets artikel 3, litra ii), og som består i at skaffe sig adgang til en informationssystem for at forvolde en fysisk eller juridisk person skade, kunne anses for omfattet af straffelovens § 263, stk. 3, idet det kan være forbundet med betydelige skadevirkninger for en virksomhed, at der skaffes oplysninger om dennes erhvervshemmeligheder.

Endvidere antages det, at den adfærd, der er omfattet af forslagets artikel 3, litra iii), og som består i at skaffe sig uretmæssig adgang til informationssystem for at opnå en økonomisk gevinst, vil kunne være omfattet af straffelovens § 279 a om databedrageri, der straffes med fængsel indtil 1 år og 6 måneder og i grove tilfælde med fængsel indtil 8 år.

Handlinger, der er omfattet af forslagets artikel 4, må betegnes som alvorlige, i det omfang handlingen medfører systemnedbrud og dermed omfattes af straffelovens bestemmelse om hærværk.

Straffen for hærværk er bøde eller fængsel indtil 1 år. I det omfang, der øves hærværk af betydeligt omfang, kan straffe stige til fængsel i 4 år. Det bemærkes, at Brydesholt-udvalget i betænkning nr. 1417/2002 om IT-kriminalitet foreslår, at strafferammen for straffelovens § 293, stk. 2, om rådhedshindring ændres, således at denne svarer til straffelovens § 293, stk. 1. Det vil sige, at udvalget finder, at strafmaksimum bør forhøjes til fængsel i 1 år og under skærpene omstændigheder til fængsel i 2 år.

På den baggrund må det antages, at forslagets artikel 6, stk. 1, ikke i øvrigt giver anledning til lovændringer.

Forslagets artikel 6, stk. 2, vedrørende bøder som supplement til frihedsstraf må anses for opfyldt ved straffelovens § 50.

Forslagets artikel 7 opregner en række skærpene omstændigheder, hvorefter medlemsstaterne forpligtes til at fastsætte en strafferamme, der som minimum er fængsel indtil 4 år. Det drejer sig om tilfælde, hvor lovovertrædelsen er begået inden for rammerne af en kriminel organisation, hvor lovovertrædelsen har ført til betydeligt økonomisk tab eller har tilføjet en person fysisk skade, samt hvor lovovertrædelsen har ført til betydelig gevinst.

Artikel 7, stk. 1, litra b) og c), er formuleret således, at det er selve lovovertrædelsens virkning, der anses som en skærpene omstændighed. Derimod tillægges det ikke vægt som en skærpene omstændighed, at den pågældende havde til hensigt eller anså det for overvejende sandsynligt, at lovovertrædelsen medførte den omtalte virkning.

Det kan på den baggrund ikke afvises, at denne del af rammeafgørelsen vil kræve lovændringer.

I det omfang det fornødne fortsat er tilstede, vil adfærden imidlertid kunne omfattes af straffelovens §§ 193, 263, stk. 3, 279 a, og 291, stk. 2. Derimod er det ikke i sig selv en skærpene omstændighed, at lovovertrædelsen er begået inden for rammerne af en kriminel organisation.

Artikel 7, stk. 2, forpligter medlemsstaterne til at sikre, at straffen i gentagelsestilfælde er frihedsstraf, der er strengere end normalstraffen for lovovertrædelser omfattet af rammeafgørelsen.

Straffelovens § 291, stk. 1, indeholder bestemmelser om forhøjet straf i gentagelsestilfælde. Desuden kan domstolene i forbindelse med strafudmålingen tillægge såvel udenlandske som danske forstraffe betydning.

På den baggrund må det antages, at artikel 7, stk. 2, ikke vil give anledning til lovændringer.

Efter artikel 8 forpligtes medlemsstaterne til at sikre, at straffen kan nedsættes, i det omfang gerningsmanden alene forvoldte mindre skade.

I det tilfælde hvor gerningsmanden alene havde til hensigt at forvolde mindre skade, må det antages, at henvisningen i straffelovens § 80 til lovovertrædelsens grovhed opfylder denne forpligtelse.



Forslagets bestemmelser om juridiske personer og straffemyndighed skønnes ikke at ville give anledning til lovændringer. Endvidere må forslaget bestemmelser om udveksling af oplysninger antages at være opfyldt gennem Danmarks tilslutning til G8-landenes 24-timers/7 dages informationsnet til bekæmpelse af højteknologikriminalitet.

Forslaget til rammeafgørelse skønnes ikke at have statsfinansielle konsekvenser

## **5. Høring**

Forslaget til rammeafgørelse er sendt i høring hos Advokatrådet, Amnesty International, Det Danske Center for Menneskerettigheder, Datatilsynet, Den Danske Dommerforening, Dommerfuldmægtigforeningen, Landsforeningen af beskikkede advokater, Politiforbundet i Danmark, Politifuldmægtigforeningen, Landsklubben HK Politi, Foreningen af Politimestre i Danmark, Rigsadvokaten, Rigspolitichefen, Ministeriet for Videnskab, Teknologi og Forskning, Politidirektøren i København, præsidenterne for Vestre og Østre Landsret, Københavns Byret og retterne i Århus, Odense og Roskilde.