



COM(2010)517(F).

Jansoone

Cellule d'analyse européenne

Proposition de DIRECTIVE relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil

COM(2010) 517

Résumé: Par suite d'attaques simultanées perpétrées récemment sur des systèmes d'information et de l'utilisation de *botnets*, la Commission européenne a élaboré un projet de directive permettant de sanctionner plus sévèrement les auteurs de cyberattaques et d'améliorer la collaboration policière européenne. Ce projet de directive s'inscrit dans le cadre de la stratégie numérique pour l'Europe et du programme de Stockholm. Pour l'heure, le Conseil des ministres et le Parlement européen examinent ce document, qui serait finalisé dans le courant de 2011.

1. Contexte:

La décision-cadre 2005/222/JAI du Conseil de 2005 relative aux attaques visant les systèmes d'information visait à renforcer la coopération entre les autorités des États membres, grâce à un rapprochement des règles pénales des États membres dans le domaine des attaques contre les systèmes d'information.

Elle créait ainsi une législation européenne en matière d'accès illicite à des systèmes d'information, d'atteinte à l'intégrité d'un système et d'atteinte à l'intégrité des données. La décision-cadre contenait également des dispositions spécifiques relatives à la responsabilité des personnes morales, la compétence juridictionnelle et les échanges d'informations.

En juillet 2008, le rapport de la Commission européenne sur la transposition de la décision-cadre précisait que: '*Les récentes attaques perpétrées en Europe depuis l'adoption de la décision-cadre ont souligné l'émergence de plusieurs menaces, que constituent notamment les attaques massives commises simultanément contre plusieurs systèmes d'information et l'utilisation accrue des «botnets» à des fins criminelles.(= robots internet permettant de perpétrer des cyberattaques sur des systèmes IT)*'.

Dès lors que la décision-cadre ne permettait pas de faire face aux risques de cyberattaques de grande envergure, il est aujourd'hui proposé de la remplacer en tenant compte de ces évolutions.

Selon la stratégie numérique pour l'Europe et le programme de Stockholm, cette initiative doit accroître la confiance et la sécurité.

2. Teneur de la Proposition de DIRECTIVE relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI

Ce document est actuellement examiné au niveau du Conseil des ministres et au Parlement européen, et devrait être finalisé dans le courant de l'année 2011.

La Commission européenne a opté pour une nouvelle directive qui remplace la décision-cadre, en reprend les dispositions existantes et introduit une législation spécifique ciblée (c'est-à-dire limitée) pour prévenir les attaques à grande échelle contre des systèmes d'information. Elle prévoit notamment :

- des poursuites plus effectives et des sanctions plus lourdes : Les auteurs de cyberattaques et de maliciels peuvent être poursuivis et sanctionnés plus lourdement.
- une meilleure coopération transfrontière : Les États membres doivent réagir aux demandes d'aide urgentes en cas de cyberattaques.

3. Fondement juridique (européen) + incidence sur la législation interne

- art. 83, paragraphe 1^{er}, TFUE, procédure législative ordinaire
- Législation interne :

La Belgique a ratifié la Convention du Conseil de l'Europe sur la cybercriminalité signée le 23 novembre 2001 couvrant la diversité des aspects de la cybercriminalité.

La loi du 15 mai 2006 modifiant les articles 259bis, 314bis, 504quater, 550bis et 550ter du Code pénal a mis le droit interne en conformité avec ladite convention. Comme cette convention, la décision-cadre impose l'incrimination de la tentative de violation de systèmes informatiques.

Cette décision-cadre a permis une exécution plus uniforme de la convention au sein de l'UE.

Selon l'article 10 de la proposition de directive, la mise en place d'un réseau zombie ou d'un dispositif similaire constituerait un facteur aggravant lors de la commission des infractions énumérées dans la décision-cadre existante (une peine d'emprisonnement maximale d'au moins cinq ans).

Dans la législation belge, le sabotage informatique y est défini sensu lato. Les infractions en cas de violation de systèmes informatiques sont, selon l'article 550ter du Code pénal, passibles d'une peine d'emprisonnement de cinq ans. Il y a également l'article 147 de la loi sur les communications électroniques du 13 juin 2005, mais cet article ne vise pas fondamentalement les attaques d'une telle gravité.

Selon l'article 14 de la proposition de directive, il faut donner suite à une demande d'assistance émise par les points de contact opérationnels dans un certain délai. La Federal Computer Crime Unit est le point de contact national pour la problématique des cyberattaques.

- Délai de mise en œuvre proposé: au plus tard 2 ans après l'adoption

4. Commission(s) compétente(s)

- Commission de la Justice
- Commission de l'Infrastructure
- Comité d'avis des Questions scientifiques et technologiques

5. Avis de subsidiarité et de proportionnalité

- Avis de la Commission européenne: l'approche européenne est motivée par :
 - la dimension transfrontalière de la cybercriminalité

- la nécessité d'un rapprochement du droit pénal matériel et des règles de procédure des États membres. Cela permet d'éviter que les auteurs se rendent dans les États membres ayant une législation plus souple. Les États membres peuvent échanger des informations et comparer les données pertinentes. Renforcement de la coopération internationale.
- Cette directive se limite au minimum requis pour la réalisation de ces objectifs et sa portée ne va pas au-delà de ce qui est nécessaire, compte tenu de la précision requise de la législation pénale.
- Les Parlements d'Italie et de Suède ont examiné ce projet de directive et n'ont émis aucune observation concernant la subsidiarité et la proportionnalité de la mesure.
- Le gouvernement néerlandais a fourni une réponse à la Première Chambre à une série de questions de la commission de la Justice.
- Situation en Belgique:
 - En réponse à une question parlementaire du député Bracke du 21 décembre 2010 (voir: CRIV 53 COM 076, pp. 17-18), le ministre de la Justice a indiqué que le projet de directive était une initiative importante, en particulier en ce qui concerne l'harmonisation du taux de la peine et l'amélioration de l'efficacité de la coopération entre les États membres. Le ministre estime que chaque pays devrait mettre sur pied un partenariat public-privé plus large dans un centre national spécialisé en vue de mieux suivre la situation, indépendamment de la police et de la Sûreté de l'État. Outre le secteur public, le secteur bancaire peut également y siéger. De tels centres existent déjà en France et en Irlande. Ils permettent de réagir plus rapidement et de manière plus adéquate aux cyberattaques, en réseau avec d'autres pays.
 - En ce qui concerne la mise en œuvre, les infractions sont – à première vue – déjà punissables en vertu de la Convention sur la cybercriminalité. Sur le terrain, la recherche de la criminalité informatique est plus complexe, en raison du contexte technologique et transfrontalier. Le cas échéant, on peut vérifier quelle est l'opinion du monde de l'entreprise concernant le projet de directive.

6. Pour en savoir plus:

- Texte de la proposition de Directive:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:FR:PDF>
- Réponse du 30 novembre 2010 du ministre néerlandais de la Justice aux membres de la Première Chambre à des questions relatives au projet de directive :
http://www.eerstekamer.nl/eu/behandeling/20101130/brief_van_de_minister_van_2/f=/viktk3c0aaq4.pdf
- Rapport 2008 de la Commission relatif aux attaques visant les systèmes d'information :
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0448:FIN:FR:PDF>
- Rapport sur la sécurité TIC du 28 février 2008 fait au nom de la commission de l'Infrastructure par M. Roel Deseyn:
<http://www.lachambre.be/FLWB/PDF/52/0898/52K0898001.pdf>

Descripteurs Eurovoc:	Criminalité informatique - protection des données - rapprochement des législations - système informatique - lutte contre le crime - droit pénal - élaboration du droit communautaire
----------------------------------	--

Rédaction:

Roeland Jansoone, conseiller, tél. 02/549.80.93, roeland.jansoone@lachambre.be



Europese analysecel

Voorstel voor een **RICHTLIJN over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/JBZ**

COM(2010) 517

Samenvatting: Als gevolg van recente gelijktijdige aanvallen op informatiesystemen en het gebruik van *botnets*, heeft de Europese commissie een ontwerprichtlijn opgesteld met een kader om daders van cyberaanvallen zwaarder te bestraffen en de Europese politie samenwerking te verbeteren. Deze ontwerprichtlijn past binnen de Digitale Agenda voor Europa en het programma van Stockholm. Momenteel bespreken de Raad van Ministers en het Europees Parlement dit document, dat in de loop van 2011 zou worden afgerond.

1. Context:

Het Kaderbesluit 2005/222/JBZ van 2005 over aanvallen op informatiesystemen beoogde een betere samenwerking tussen de overheden van de lidstaten door onderlinge afstemming van de strafrechtelijke bepalingen van de lidstaten inzake aanvallen op informatiesystemen.

Hierdoor kwam Europese wetgeving tot stand m.b.t. onrechtmatige toegang tot informatiesystemen, onrechtmatige systeemverstoring en onrechtmatige gegevensverstoring. Het Kaderbesluit bevatte tevens specifieke regels betreffende de aansprakelijkheid van rechtspersonen, rechtsmacht en informatie-uitwisseling.

In Juli 2008 stelde het Verslag van de Europese commissie over de tenuitvoerlegging van het kaderbesluit dat: *'Sinds het vaststellen van het kaderbesluit hebben recente aanvallen in heel Europa allerlei nieuwe bedreigingen aan het licht gebracht: omvangrijke gelijktijdige aanvallen op informatiesystemen en een toenemend crimineel gebruik van zogeheten botnets. (= internetrobots waarmee cyberaanvallen kunnen worden uitgevoerd op IT-systemen)'*.

Omdat het Kaderbesluit geen aanpak bood voor de risico's van grote cyberaanvallen wordt thans voorgesteld om het Kaderbesluit te vervangen, rekening houdend met deze ontwikkelingen.

Dit initiatief moet volgens de Digitale agenda voor Europa en het programma van Stockholm voor meer vertrouwen en veiligheid zorgen.

2. Inhoud van het Voorstel voor een RICHTLIJN over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/JBZ

Dit document wordt momenteel besproken op het niveau van de Raad van Ministers en het Europees Parlement en zou in de loop van 2011 worden afgerond.

De Europese commissie heeft geopteerd voor een nieuwe richtlijn die het kaderbesluit vervangt, de bestaande bepalingen ervan overneemt en een specifieke gerichte (d.w.z. beperkte) wetgeving invoert ter voorkoming van grootschalige aanvallen op informatiesystemen, met name:

- Effectievere vervolging en zwaardere sancties: Daders van cyberaanvallen en makers van kwaadaardige software kunnen worden vervolgd en zwaarder bestraft.
- Betere grensoverschrijdende samenwerking: Lidstaten moeten reageren op dringende verzoeken om steun bij cyberaanvallen.

3. Rechtsgrond (Europees) + impact op interne wetgeving

- Artikel 83, lid 1, VWEU, gewone wetgevingsprocedure
- Interne wetgeving:

België heeft het op 23 november 2001 ondertekende Verdrag inzake cybercriminaliteit van de Raad van Europa geratificeerd. Dit verdrag bestrijkt de diverse aspecten van cybercriminaliteit.

De wet van 15 mei 2006 tot wijziging van de artikelen 259bis, 314bis, 504quater, 550bis en 550ter van het Strafwetboek heeft het interne recht in overeenstemming gebracht met voormeld verdrag. Zoals het Verdrag, legt het Kaderbesluit de strafbaarstelling op van de poging tot schending van informaticasystemen.

Dit Kaderbesluit heeft een meer uniforme uitvoering van het verdrag binnen de EU mogelijk gemaakt.

Het opzetten van een botnet of een vergelijkbaar instrument bij het plegen van de in het huidige kaderbesluit opgesomde strafbare feiten zou, overeenkomstig Artikel 10 van de ontwerprichtlijn, als een verzwarende factor zou gelden (maximale gevangenisstraf van minstens 5 jaar).

In de Belgische wetgeving wordt informaticasabotage ruim gedefinieerd. Artikel 550ter van het Strafwetboek voorziet maximale gevangenisstraffen van 5 jaar, terwijl artikel 145 van de wet op de elektronische communicatie van 13 juni 2005, dat eigenlijk niet bedoeld is voor dergelijk ernstige aanvallen, een gevoelig lichtere strafbepaling aangeeft dan het artikel 550ter van het Strafwetboek.

Artikel 14 van de ontwerprichtlijn bepaalt dat, binnen een bepaalde termijn, gehoor moet worden gegeven aan een verzoek om bijstand van de operationele meldpunten. De Federal Computer Crime Unit is het nationale contactpunt voor de problematiek van cyberaanvallen.

- Voorgestelde termijn ter implementatie: uiterlijk 2 jaar na goedkeuring

4. Bevoegde commissie(s)

- Commissie Justitie
- Commissie Infrastructuur
- Adviescomité Wetenschappelijke en Technologische vraagstukken

5. Advies inzake subsidiariteit en proportionaliteit

- Advies van de Europese commissie: Europese aanpak wordt gemotiveerd door de noodzaak tot:
 - grensoverschrijdende dimensie van cybercriminaliteit
 - afstemming van materiële strafrecht en de procedureregels van de lidstaten. Hierdoor wordt voorkomen dat daders naar lidstaten trekken met soepeler wetgeving. Lidstaten kunnen informatie uitwisselen en relevante gegevens vergelijken. Versterking internationale samenwerking.

- Deze richtlijn beperkt zich tot het voor de verwezenlijking van deze doelstellingen tot het vereiste minimum en reikt niet verder dan wat daarvoor nodig is, rekening houdend met de vereiste nauwkeurigheid van de strafwetgeving.
- De Parlementen van Italië en Zweden hebben deze ontwerprichtlijn onderzocht en hadden geen opmerkingen m.b.t. de subsidiariteit en proportionaliteit van de maatregel.
- De Nederlandse regering heeft aan de Eerste Kamer een antwoord verschaft m.b.t. een aantal vragen van de commissie Justitie.
- Belgische situatie:
 - Naar aanleiding van een parlementaire vraag van Kamerlid Bracke dd. 21 december 2010 (zie: CRIV 53 COM 076, pp. 17-18), stelde de minister van Justitie dat de ontwerprichtlijn een belangrijk initiatief was, inzonderheid wat de harmonisering van de strafmaat en de efficiëntere samenwerking tussen de lidstaten betreft. De minister verkondigde de stelling dat elk land een bredere, publiekprivate samenwerking zou moeten uitbouwen in een nationaal, gespecialiseerd centrum om alles beter op te volgen, los van politie en Veiligheid van de Staat. Naast de publieke sector, kan de banksector hierin ook zetelen. Dergelijke centra bestaan reeds in Frankrijk en Ierland. Het laat toe adequater en sneller te reageren, in netwerk met andere landen, om een antwoord te bieden op cyberaanvallen.
 - Wat de implementatie betreft, zijn – op het eerste gezicht – de strafbare feiten ook reeds strafbaar ingevolge het Verdrag inzake Cybercriminaliteit. Op het terrein is de opsporing van de informaticacriminaliteit complexer, gelet op de grensoverschrijdende en technologische context. Desgevallend kan worden nagegaan hoe de bedrijfswereld tegen de ontwerprichtlijn aankijkt.

6. Om meer te weten:

- Tekst van het voorstel van Richtlijn:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:NL:PDF>
- Antwoord dd. 30 november 2010 van de Nederlandse minister van Justitie aan de leden van de Eerste Kamer op vragen m.b.t. de ontwerprichtlijn:
http://www.eerstekamer.nl/eu/behandeling/20101130/brief_van_de_minister_van_2/f=/viktk3c0aaq4.pdf
- Verslag 2008 van de Commissie over aanvallen op informatiesystemen:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0448:FIN:NL:PDF>
- Nota van de minister van Justitie inzake de overeenstemming van de Belgische wetgeving met het Cybercrimeverdrag:
http://stefaandeclerck.be/files/pdf/Cybercrime_nota_conformiteit.pdf
- Verslag over ICT-veiligheid van 28 februari 2008 namens de commissie Infrastructuur uitgebracht door de heer Roel Deseyn:
<http://www.dekamer.be/FLWB/PDF/52/0898/52K0898001.pdf>

Eurovoc-descriptoren:	Computercriminaliteit – gegevensbescherming – harmonisatie van wetgevingen – informatieverwerkend systeem – misdaadbestrijding – strafrecht – uitwerking van het communautaire recht
------------------------------	--

Redactie: Roeland Jansoone, adviseur, tel. 02/549.80.93, roeland.jansoone@dekamer.be