Cellule d'analyse européenne

« PAQUET CYBER »

COMMUNICATION CONJOINTE « Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide » (JOIN(2017)450)

RAPPORT DE LA COMMISSION évaluant dans quelle mesure les États membres ont pris les dispositions nécessaires pour se conformer à la directive 2013/40/UE relative aux attaques contre les systèmes d'information (COM(2017)474)

COMMUNICATION DE LA COMMISSION relative à la mise en œuvre effective de la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (COM(2017)476)

Proposition de RÈGLEMENT relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité) (COM(2017)477)

Proposition de DIRECTIVE concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces (COM(2017)489)

1. Contexte

Le monde numérique présente de nombreux avantages, mais il est également vulnérable. Le nombre croissant de cyber-incidents en est la preuve. La cybersécurité est d'une importance primordiale pour renforcer la confiance du consommateur et des entreprises dans le marché numérique.

Dans une communication de 2013, la Commission européenne et la Haute Représentante pour les Affaires étrangères et la Politique de Sécurité ont plaidé en faveur d'un renforcement de la sécurité de l'environnement numérique, de la réduction de la cybercriminalité et du développement d'une politique européenne de cybersécurité.

Le « paquet cyber » 2017, présenté ici, complète la Stratégie de la cybersécurité de 2013, comble plusieurs lacunes et développe plus avant certains points forts.

2. Contenu

Les lignes de force du paquet cyber peuvent être résumées comme suit :

	Contenu	Commentaire
1	Objectif	La cybersécurité est d'une importance capitale pour renforcer la confiance du consommateur et des entreprises dans le marché numérique. Ce Paquet cyber 2017 vise à compléter et à renforcer la Stratégie de cybersécurité de 2013.
2	Meilleure résilience contre les cyberattaques JOIN(2017)450 et COM(2017)474	L'UE réagira mieux aux cyberattaques en prévoyant des mesures concrètes d'aide à la détection, à l'instruction et aux poursuites judiciaires pour tous les types de cyberincidents. Un réseau européen de centres d'expertise en cybersécurité serait créé. Ce réseau devra coopérer avec les États membres en vue de garantir que les moyens de défense nationaux soient aussi avancés que les armes des cybercriminels. Il y aura une réponse coordonnée en cas d'incidents et de crises de grande ampleur. L'option d'un Fonds d'intervention pour les urgences de cybersécurité est examinée (aide d'urgence aux États membres en cas de cyberattaque).
3	Réforme de l'ENISA COM(2017)477	L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) voit son mandat renforcé, à savoir : - qu'elle pourra soutenir la politique de l'UE en matière de cybersécurité ainsi que les États membres dans leur lutte contre les cyberattaques ; - qu'elle jouera un rôle central dans la certification paneuropéenne de cybersécurité (qui garantira que les biens et services numériques peuvent être utilisés en toute sécurité). Les mesures de certification proposées visent à lutter contre le morcellement entraîné par les systèmes nationaux de certification existants et à contribuer à l'élaboration du marché unique numérique ; - qu'elle organisera des exercices paneuropéens annuels de cybersécurité (en collaboration avec l'OTAN).
4	Mise en œuvre de la directive SRI COM(2017)476	La Commission européenne donne quelques lignes directrices en vue d'une mise en œuvre rapide de la directive SRI de 2016, qui vise à réaliser un niveau commun de sécurité des réseaux et de l'information dans l'UE.
5	La lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces COM(2017)489	La proposition vise à éliminer les obstacles qui entravent les enquêtes pour fraude et contrefaçon de moyens de paiement autres que les espèces. Le champ d'application est élargi afin de pouvoir sanctionner plus facilement les infractions commises avec certains instruments de paiement (en particulier non matériels). Des sanctions communes sont prévues et l'accès transfrontière aux preuves électroniques est facilité. La directive tient compte des comportements frauduleux actuels auxquels les services bancaires sur internet sont confrontés (*skimming*, *carding*, *phishing, pharming*).

3. Cadre juridique européen

- L'art. 114 du Traité sur le fonctionnement de l'Union européenne (TFUE) relatif au marché intérieur et art. 83, paragraphe 1, du TFUE (lutte contre la criminalité grave revêtant une dimension transfrontière) ;
- L'art. 222 du TFUE, qui prévoit qu'un incident ou une attaque informatique présentant un caractère particulier de gravité peut être, pour un État membre, une raison suffisante pour invoquer la clause de solidarité de l'UE ;
- La législation européenne en ce qui concerne les attaques visant les systèmes d'information ;
- La convention du Conseil de l'Europe sur la cybercriminalité.

4. Développements européens

La présidence estonienne accorde une grande importance aux mesures stratégiques visant à établir un marché numérique européen unique. Cela implique en outre une plus grande collaboration européenne en matière de cybersécurité et une actualisation de la stratégie européenne relative à la cybersécurité. En 2025, l'Europe doit être devenue un leader mondial dans ce domaine.

5. Cadre belge :

La loi du 28 novembre 2000 relative à la criminalité informatique et la loi du 1er juillet 2011 relative à la sécurité et protection des infrastructures critiques, qui prévoient un cadre permettant de lutter contre les attaques informatiques, ainsi que l'arrêté royal du 9 mai 2012 « portant création d'un *computer emergency response team,* le CERT ».

À l'issue du super Conseil des ministres de mai 2017, plusieurs mesures nouvelles en matière de cybersécurité ont été annoncées : un point de contact national opérationnel qui sera accessible 24 heures sur 24 et 7 jours sur 7, la mise en place d'une campagne de sensibilisation nationale et l'élargissement du *computer emergency response team*.

6. Suivi au sein de la (des) commission(s) compétente(s) de la Chambre :

- la commission de la Justice ;
- la commission de l'Intérieur ;
- pour information : le comité d'avis fédéral pour les questions européennes.

7. Suivi auprès des instances fédérales :

- le Centre pour la cybersécurité Belgique, qui est l'autorité centrale en matière de cybersécurité en Belgique[1].
- la *Federal Computer Crime Unit* (FCCU), qui est l'instance spécialisée dans la lutte contre la cybercriminalité ;
- le SPF Justice.

[1] Dès 2018, le Centre pour la cybersécurité Belgique effectuera par exemple un contrôle important afin de garantir l'imperméabilité des logiciels électoraux contre des cyber-attaques externes (voir la note de politique générale « Sécurité et Intérieur » de 2018 http://www.lachambre.be/flwb/pdf/54/2708/54K2708008.pdf, p. 37).

8. Subsidiarité et proportionnalité

Le délai imparti pour formuler un avis de subsidiarité au sujet des propositions législatives expire le 7 décembre 2017 (COM(2017)477) et le 21 novembre 2017 (COM(2017)489).

Dans le cadre du « dialogue politique » (initiative Barroso), les parlements nationaux peuvent transmettre leurs remarques à la Commission européenne. Cette procédure n'est pas assortie d'un délai.

Projet d'avis de subsidiarité et de proportionnalité:

La cybersécurité est essentielle pour renforcer la confiance du consommateur et des sociétés dans le marché unique numérique. Le « paquet cyber » annonce des initiatives visant à compléter et à renforcer la stratégie de cybersécurité de 2013. Il aborde des défis transfrontaliers par excellence qu'il convient d'appréhender dans un cadre politique et législatif européen.

À première vue, le « paquet cyber » ne va pas au-delà des mesures nécessaires pour atteindre les objectifs fixés en la matière, d'autant que la Belgique aligne ses actions sur le calendrier numérique européen.

La réforme de l'Agence de cybersécurité de l'Union européenne (ENISA) permettra à l'Union européenne de réagir de façon adéquate aux cyberattaques, qui sont de plus en plus fréquentes. Les certificats européens de cybersécurité garantiront la sécurité des appareils qui commandent les infrastructures critiques. La reconnaissance mutuelle de ces certificats par les États membres renforcera le marché numérique intérieur.

La proposition de directive concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces remplace la réglementation européenne existante et la modernise. Cette proposition contribue à la lutte proactive contre la fraude liée aux opérations bancaires en ligne. Elle encourage par ailleurs la collaboration entre les États membres et entre les pouvoirs publics et le secteur privé.

Pour en savoir plus :

Document afférents au « paquet cyber »

JOIN(2017)450: http://www.ipex.eu/IPEXL-WEB/dossier/document/JOIN20170450.do

COM(2017)474: http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20170474.do

COM(2017)476: http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20170476.do

COM(2017)477: http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20170477.do

COM (2017)489: http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20170489.do

Descripteurs Eurovoc:	UNION EUROPÉENNE – SÉCURITÉ INFORMATIQUE – CRIMINALITÉ INFORMATIQUE – INFORMATIQUE – SÉCURITÉ PUBLIQUE – INTERNET – TELECOMMUNICATION

Rédaction: Roeland Jansoone, premier conseiller, tél. 02/549.80.93, roeland.jansoone@dekamer.be

Europese analysecel

CYBERPAKKET

GEZAMENLIJKE MEDEDELING “Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU” (JOIN(2017)450)

VERSLAG VAN DE COMMISSIE betreffende de maatregelen om te voldoen aan Richtlijn 2013/40/EU over aanvallen op informatiesystemen (COM(2017)474)

MEDEDELING VAN DE COMMISSIE betreffende de doeltreffende uitvoering van Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (COM(2017)476)

Voorstel voor een VERORDENING inzake Enisa, het agentschap van de Europese Unie voor cyberbeveiliging, en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie ("de cyberbeveiligingsverordening") (COM(2017)477)

Voorstel voor een RICHTLIJN betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten (COM(2017)489)

1. Context

De digitale wereld biedt veel voordelen, maar is ook kwetsbaar. Dit blijkt uit het stijgend aantal cyberincidenten. Cyberveiligheid is van essentieel belang om het vertrouwen van de consument en de bedrijven in de digitale markt te versterken.

In een mededeling van 2013 hebben de Europese Commissie en de hoge vertegenwoordiger voor buitenlandse zaken en veiligheidsbeleid gepleit voor meer beveiliging van de digitale omgeving, het terugdringen van de cybercriminaliteit en het ontwikkelen van een Europees cyberbeveiligingsbeleid.

Het Cyberpakket 2017, dat hier voorligt, is een aanvulling op de Cyberveiligheidstrategie van 2013, pakt enkele lacunes aan en werkt een aantal sterke punten verder uit.

2. Inhoud

De krachtlijnen van het cyberpakket kunnen als volgt worden samengevat:

	Inhoud	Toelichting
1	Doel	Cyberveiligheid is van essentieel belang om het vertrouwen van de consument en de bedrijven in de digitale markt te versterken. Dit Cyberpakket 2017 beoogt de Cyberveiligheidstrategie van 2013 aan te vullen en te versterken.
2	Meer weerbaarheid tegen cyberaanvallen JOIN(2017)450 en COM(2017)474	Er komt een betere EU-respons op cyberaanvallen met concrete stappen om elke cyberaanval op te sporen en te onderzoeken, en om de cybercriminelen te vervolgen. Er zou een Europees Netwerk van kenniscentra voor cyberbeveiliging worden opgericht. Dat centrum moet samenwerken met de lidstaten om te waarborgen dat de nationale verdedigingsmiddelen even geavanceerd zijn als de wapens van cybercriminelen. Er komt een gecoördineerd antwoord in geval van grote incidenten en crisissen. De optie van een cyberbeveiligingsnoodfonds wordt onderzocht (noodsteun aan lidstaten ingeval van cyberaanval).
3	Hervorming van ENISA COM(2017)477	Het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) krijgt een versterking van haar mandaat, d.w.z. - ondersteuning van het EU-cyberveiligheidsbeleid, bijstand van de lidstaten in hun strijd tegen cyberaanvallen; - een centrale rol in de EU-brede cyberbeveiligingscertificering (die garandeert dat digitale goederen en diensten veilig kunnen worden gebruikt). De voorgestelde certificeringmaatregelen dienen de versnippering ingevolge nationale certificeringregelingen aan te pakken en bij te dragen tot de digitale eengemaakte markt; - jaarlijkse organisatie van Europabrede cyberbeveiligingsoefeningen (i.s.m. NAVO).
4	Implementatie van de NIS-richtlijn COM(2017)476	De Europese Commissie geeft enkele richtsnoeren met het oog op de vlotte implementatie van de NIS-richtlijn van 2016, die een gemeenschappelijk niveau van netwerk- en informatiebeveiliging binnen de EU wenst op te zetten.
5	De bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten COM(2017)489	Het voorstel wil obstakels wegnemen die het onderzoek belemmeren naar fraude en vervalsing van niet-chartaal geldverkeer. Er komt een verruiming van het toepassingsgebied om strafbare feiten die met bepaalde betaalinstrumenten (met name onlichamelijke) worden gepleegd beter te bestraffen. Er komen gemeenschappelijke sancties en een gemakkelijkere grensoverschrijdende toegang tot elektronisch bewijsmateriaal. De richtlijn houdt rekening met de actuele frauduleuze gedragingen waarmee het internetbankieren wordt geconfronteerd (“skimming”, “carding”, “phishing” en “pharming”).

3. Europees juridisch kader:

- Art 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU) m.b.t. de interne markt en art artikel 83, lid 1, VWEU (bestrijding zware criminaliteit met een grensoverschrijdende dimensie);
- Art. 222 VWEU dat stelt dat een cyberincident of -aanval van bijzonder ernstige aard voldoende reden kan zijn voor een lidstaat om een beroep te doen op de solidariteitsclausule van de EU;
- De Europese wetgeving m.b.t. aanvallen tegen informatiesystemen;
- Verdrag van de Raad van Europa inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken.

4. Europese ontwikkelingen

Het Estse voorzitterschap hecht veel belang aan strategische maatregelen voor een digitale eengemaakte markt. Dit omvat eveneens meer Europese samenwerking op het gebied van cyberveiligheid en het actualiseren van de EU-cyberveiligheidsstrategie. Europa moet in 2025 een wereldleider op het gebied van cyberveiligheid zijn.

5. Belgisch intern kader:

De wet van 28 november 2000 betreffende de informaticacriminaliteit en de wet van 1 juli 2011 betreffende de veiligheid en bescherming van kritieke infrastructuur voorzien in een kader dat aanvallen tegen computersystemen bestrijdt. Voorts is er het koninklijk besluit van 9 mei 2012 tot “Oprichting van een *computer emergency response team*, het CERT”.

De superministerraad van mei 2017 heeft een aantal nieuwe maatregelen op het vlak van cyberveiligheid aangekondigd: een operationeel nationaal contactpunt dat 24 uur per dag en zeven dagen per week bereikbaar is, een nationale sensibiliseringscampagne en de uitbreiding van het *computer emergency response team*.

6. Opvolging in de bevoegde Kamercommissie(s):

- Commissie Justitie
- Commissie Binnenlandse zaken.
- Ter informatie: adviescomité voor Europese aangelegenheden.

7. Opvolging bij de federale instanties:

- Het Centrum voor Cybersecurity België zorgt als centrale autoriteit voor de cyberveiligheid in België[1].
- De instantie die gespecialiseerd is in de bestrijding van cybercriminaliteit is de Federal Computer Crime Unit (FCCU).
- FOD Justitie.

[1] Zo zal het “*Center for Cyber Security Belgium”* vanaf 2018 een belangrijke controle uitvoeren om de ondoordringbaarheid van de verkiezingssoftware te garanderen in het geval van een externe cyberaanval. (zie beleidsnota 2018 Binnenlandse Zaken http://www.dekamer.be/flwb/pdf/54/2708/54K2708008.pdf, p. 37)

8. **Subsidiariteit en proportionaliteit:**

De termijn om een subsidiariteitsadvies over de wetgevingsvoorstellen COM(2017)477 en 489 te formuleren, verstrijkt respectievelijk op 7 december 2017 en op 21 november 2017.

De nationale parlementen kunnen in het kader van de "politieke dialoog" (initiatief Barroso) aan de Europese Commissie opmerkingen formuleren. Deze procedure is niet gebonden aan een termijn.

Ontwerpadvies betreffende de subsidiariteit en proportionaliteit:

Cyberveiligheid is van essentieel belang om het vertrouwen van de consument en de bedrijven in de digitale eengemaakte markt te versterken. Het cyberpakket kondigt initiatieven aan die de cyberveiligheidstrategie van 2013 aanvullen en versterken. Het gaat om bij uitstek grensoverschrijdende uitdagingen die het best worden aangepakt binnen een Europees beleids- en wetgevend kader.

De maatregelen gaan op het eerste zicht niet verder dan nodig is om de doelstellingen te bereiken, te meer daar België haar acties afstemt op de Europese digitale agenda.

De hervorming van het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA) zal de EU toelaten om passend te reageren op het stijgend aantal cyberaanvallen. De Europese cyberveiligheidscertificaten betekenen een garantie voor de veiligheid van de apparaten die de kritieke infrastructuur aansturen. De wederzijdse erkenning door de lidstaten van de cyberveiligheidscertificaten versterkt de digitale interne markt.

De ontwerprichtlijn ter bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten vervangt en actualiseert bestaande Europese regelgeving. Het voorstel draagt bij tot een proactief optreden tegen fraude bij internetbankieren. Voorts draagt het voorstel bij tot meer samenwerking onder de lidstaten en tussen de publieke overheden en de private sector.

Om meer te weten:

Documenten van het "cyberpakket"

JOIN(2017)450: http://www.ipex.eu/IPEXL-WEB/dossier/document/JOIN20170450.do

COM(2017)474: http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20170474.do

COM(2017)476: http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20170476.do

COM(2017)477: http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20170477.do

COM (2017)489: http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20170489.do

Eurovoc-descriptoren:	EUROPESE UNIE – COMPUTERVEILIGHEID – COMPUTERCRIMINALITEIT – INFORMATICA – OPENBARE VEILIGHEID – INTERNET – TELECOMMUNICATIE

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