DOC 53 **3296/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

17 janvier 2014

PROPOSITION DE LOI

réglant le signalement d'une atteinte à la sécurité ou d'une perte d'intégrité de systèmes d'information électroniques d'une importance vitale pour la société

(déposée par Mme Karolien Grosemans et MM. Theo Francken, Jan Jambon et Bert Maertens)

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

17 januari 2014

WETSVOORSTEL

houdende regels over het melden van een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de samenleving

(ingediend door mevrouw Karolien Grosemans en de heren Theo Francken, Jan Jambon en Bert Maertens)

RÉSUMÉ

Les auteurs visent à instaurer une obligation de signalement en cas d'atteinte à la sécurité ou de perte d'intégrité de systèmes d'information électroniques.

L'obligation de signalement s'applique uniquement aux organisations qui présentent une importance vitale pour notre société. Toutes les autres organisations peuvent y apporter leur concours.

SAMENVATTING

De indieners beogen een meldplicht voor inbreuken op de veiligheid of bij een verlies van integriteit van elektronische informatiesystemen.

De meldplicht geldt alleen voor organisaties die van vitaal belang zijn voor onze samenleving. Alle andere organisaties krijgen de mogelijkheid hiertoe.

N-VA	:	*Nieuw-Vlaamse Alliantie*
PS	:	*Parti Socialiste*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
sp.a	:	*socialistische partij anders*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
Open Vld	:	*Open Vlaamse liberalen en democraten*
VB	:	*Vlaams Belang*
cdH	:	*centre démocrate Humaniste*
FDF	:	*Fédéralistes Démocrates Francophones*
LDD	:	*Lijst Dedecker*
MLD	:	*Mouvement pour la Liberté et la Démocratie*
INDEP-ONAFH	:	*Indépendant-Onafhankelijk*

Abréviations dans la numérotation des publications:

DOC 53 0000/000:	*Document parlementaire de la 53e législature, suivi du n° de base et du n° consécutif*
QRVA:	*Questions et Réponses écrites*
CRIV:	*Version Provisoire du Compte Rendu intégral*
CRABV:	*Compte Rendu Analytique*
CRIV:	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN:	*Séance plénière*
COM:	*Réunion de commission*
MOT:	*Motions déposées en conclusion d'interpellations (papier beige)*

Afkortingen bij de nummering van de publicaties:

DOC 53 0000/000:	*Parlementair document van de 53e zittingsperiode + basisnummer en volgnummer*
QRVA:	*Schriftelijke Vragen en Antwoorden*
CRIV:	*Voorlopige versie van het Integraal Verslag*
CRABV:	*Beknopt Verslag*
CRIV:	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN:	*Plenum*
COM:	*Commissievergadering*
MOT:	*Moties tot besluit van interpellaties (beigekleurig papier)*

Publications officielles éditées par la Chambre des représentants

Commandes:
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.lachambre.be
courriel : publications@lachambre.be

Les publications sont imprimées exclusivement sur du papier cerifié FSC

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

Bestellingen:
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.dekamer.be
e-mail : publicaties@dekamer.be

De publicaties worden uitsluitend gedrukt op FSC gecertifieerd papier

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

1. **Introduction**

La présente proposition de loi introduit une obligation de signalement en cas d'atteinte à la sécurité ou de perte d'intégrité de systèmes d'information électroniques, ci-après dénommées "atteintes TIC". L'obligation de signalement s'applique uniquement aux organisations qui proposent des biens ou des services dont la disponibilité ou la fiabilité présentent une importance vitale pour notre société, et uniquement si l'atteinte a ou peut avoir pour conséquence que leur disponibilité ou leur fiabilité sont, largement, interrompues. Les organisations qui seront soumises à cette obligation de signalement seront désignées par le Comité ministériel du renseignement et de la sécurité. Les entreprises auxquelles cette obligation n'est pas applicable ont la possibilité de signaler volontairement les atteintes TIC.

Les atteintes à la sécurité ou les pertes d'intégrité doivent être signalées au Comité ministériel du renseignement et de la sécurité, ci-après dénommé "Comité ministériel". Le signalement permet à ce Comité de venir en aide à l'organisation touchée et de prévenir d'autres organisations vitales, dans le but ultime d'évaluer le risque de désagrégation sociale et de prévenir cette désagrégation ou, en tout cas, de la limiter le plus possible.

L'aide proposée en vue d'empêcher une désagrégation sociale et la responsabilité des organisations vitales mêmes sont au cœur de la concrétisation de l'obligation de signalement. Cette obligation vise en outre à instaurer une culture de la sécurité, parfois appelée "*just culture*", dans le cadre de laquelle il importe avant tout de tirer les leçons des incidents survenus.

La présente proposition de loi est conforme à l'ambition de la Commission européenne de parvenir à une obligation de signalement au niveau de toute l'UE pour les autorités et les acteurs clés du marché de manière à accroître la sécurité numérique.

2. **Contenu et signification**

Obligation de signalement

L'objectif de l'obligation de signalement est double. Le fait, pour les secteurs vitaux, de signaler au Comité ministériel toute atteinte sérieuse à la sécurité des

TOELICHTING

DAMES EN HEREN,

1. **Inleiding**

Dit wetsvoorstel introduceert een meldplicht voor inbreuken op de veiligheid of een verlies van integriteit van elektronische informatiesystemen, hierna te noemen 'ICT-inbreuken'. De meldplicht geldt alleen voor organisaties die goederen of diensten aanbieden waarvan de beschikbaarheid of betrouwbaarheid van vitaal belang is voor onze samenleving en alleen als de inbreuk tot gevolg heeft of kan hebben dat de beschikbaarheid of betrouwbaarheid in belangrijke mate wordt onderbroken. De organisaties waarvoor de meldplicht gaat gelden, zullen worden aangewezen door het Ministerieel Comité voor inlichtingen en veiligheid. Bedrijven waarvoor de meldplicht niet geldt, wordt de mogelijkheid geboden om ICT-inbreuken vrijwillig te melden.

De melding moet worden gedaan aan het Ministerieel Comité voor inlichtingen en veiligheid, hierna te noemen 'Ministerieel Comité'. De melding stelt het Comité in staat om hulp te verlenen aan de getroffen organisatie en om andere vitale organisaties te waarschuwen met als uiteindelijk doel om het risico van maatschappelijke ontwrichting in te schatten en die ontwrichting te voorkomen of in elk geval zo veel mogelijk te beperken.

Het bieden van hulp ter voorkoming van maatschappelijke ontwrichting en eigen verantwoordelijkheid van vitale organisaties staat centraal bij de invulling van de meldplicht. Verder beoogt de meldplicht bij te dragen aan het creëren van een veiligheidscultuur, de zogeheten "*just culture*", waarin het leren van incidenten vooropstaat.

Dit wetsvoorstel sluit ook aan bij de ambitie van de Europese Commissie om EU-breed te komen tot een meldplicht voor overheden en vitale marktpartijen die bijdraagt tot het verhogen van de digitale veiligheid.

2. **Inhoud en betekenis**

Meldplicht

Het doel van de meldplicht is tweeledig. Een melding van een ernstige ICT-inbreuk vanuit de vitale sectoren aan het Ministerieel Comité is enerzijds bedoeld om

systèmes TIC vise premièrement à permettre une évaluation de l'impact de cette atteinte et, partant, de la désagrégation sociale qu'elle pourrait entraîner.

Deuxièmement, le signalement donne la possibilité au Comité ministériel de venir en aide à l'organisation touchée et d'anticiper les effets potentiellement plus importants d'une telle atteinte en prévenant et en conseillant d'autres organisations vitales. À cette fin, le Comité ministériel peut faire appel à d'autres organismes (publics) et les coordonner.

Un aspect important de cette obligation de signalement est qu'elle tend vers une culture accordant une place centrale à la contribution conjointe à la sécurité. Le secteur aérien, par exemple, a déjà acquis une grande expérience de cette pratique dans le cadre de l'élaboration d'une "*just culture*".

Il est important que les signalements soient faits en toute confiance afin de limiter les vulnérabilités ou de les prévenir dans le futur. Afin de permettre au Comité ministériel de jouer un rôle d'appui dans la prévention et la limitation des ruptures de disponibilité et de fiabilité des services et biens vitaux pour notre société et d'assurer une culture de la sécurité dans laquelle des signalements sont faits pour en tirer des enseignements, il est important d'abaisser au maximum le seuil des signalements. À cet égard, l'obligation de signalement proposée n'est pas assortie d'une possibilité de sanction et elle est vise en premier lieu à offrir une aide. Le Comité ministériel peut à cet égard servir de point d'information, ou être l'araignée au milieu de sa toile, en vue d'informer les parties et de les conseiller sur les actions à entreprendre. Le Comité peut notamment s'inspirer d'un important réseau national et international de *Computer Emergency Response Teams* publics et privés, qui ont emmagasiné de nombreuses connaissances sur la manière de traiter et de réagir aux atteintes ICT.

Mission du Comité ministériel

Le Comité ministériel est un organe politique qui définit la politique du renseignement. Il donne des avis sur les initiatives politiques et législatives en matière de renseignements et de sécurité. À l'heure actuelle, le Premier ministre, le ministre des Affaires étrangères, le ministre de la Justice, le ministre de la Défense, le ministre de l'Intérieur et le ministre de l'Économie font partie de ce Comité.

La présente proposition de loi confie les missions supplémentaires suivantes au Comité: la réception de signalements d'atteintes ICT, l'aide aux organisations

tijdig te kunnen inschatten hoe groot de impact en daarmee de potentiële maatschappelijke ontwrichting is.

Anderzijds stelt de melding het Ministerieel Comité in staat om hulp aan de getroffen organisatie te verlenen en om te anticiperen op de mogelijk bredere effecten van een dergelijke inbreuk door andere vitale organisaties te waarschuwen en te adviseren. Het Ministerieel Comité kan daarbij andere (overheids)organisaties inzetten en coördineren.

Belangrijk bij de meldplicht is ook dat deze een cultuur beoogt waarin het gezamenlijk bijdragen aan veiligheid centraal staat. In de luchtvaartsector bestaat bijvoorbeeld ruime ervaring met deze praktijk onder de noemer van het werken aan een "*just culture*".

Het is van belang dat de meldingen in vertrouwen gedaan worden om kwetsbaarheden te beperken dan wel in de toekomst te vermijden. Om het Ministerieel Comité een ondersteunende rol te laten vervullen bij het voorkomen en beperken van onderbrekingen van de beschikbaarheid en betrouwbaarheid van voor de samenleving vitale diensten en goederen én te zorgen voor een veiligheidscultuur waarbij meldingen gedaan worden om daar lering uit te trekken, is het van belang om de drempel om meldingen te doen zo laag mogelijk te maken. In verband hiermee is de voorgestelde meldplicht niet voorzien van de mogelijkheid tot bestraffing en is de meldplicht primair gericht op het bieden van hulp. Het Ministerieel Comité kan daarbij functioneren als informatieknooppunt, ofwel de spin in het web, om partijen te informeren en te adviseren over de te ondernemen acties. Het Comité kan daarbij putten uit een omvangrijk nationaal en internationaal netwerk van o.a. publieke en private Computer Emergency Response Teams waarbinnen veel kennis beschikbaar is over de wijze van omgaan met en het leveren van response bij ICT-inbreuken.

Taak van het Ministerieel Comité

Het Ministerieel Comité is een politiek orgaan dat het inlichtingenbeleid bepaalt. Het geeft advies over politieke en legislatieve initiatieven op het vlak van inlichtingen en veiligheid. Momenteel maken de eerste minister, de minister van Buitenlandse Zaken, de minister van Justitie, de minister van Landsverdediging, de minister van Binnenlandse Zaken en de minister van Economie deel uit van dit Comité.

Dit wetsvoorstel voegt als bijkomende taak van het Comité toe: het ontvangen van meldingen van ICT-inbreuken, het verlenen van hulp aan getroffen vitale

vitales touchées et la mise en garde des autres organisations vitales contre les vulnérabilité avérées dans le but de prévenir, ou en tout cas de limiter au maximum, toute désagrégation sociale.

Signalement

En vue de la nouvelle mission précitée du Comité ministériel, il importe que le signalement au Comité contienne suffisamment d'informations pour concrétiser cette mission et pouvoir estimer les risques d'une atteinte et les mesures nécessaires à prendre à cet égard. A cet égard, il importe que le signalement se compose dans tous les cas d'un certain nombre d'éléments, même s'il change de nature en fonction du secteur vital.

Tout d'abord, le signalement doit donner une idée de la nature et de l'ampleur de l'atteinte ICT. Sur la base de ces informations, on peut chercher de manière ciblée sur le réseau national et international, entre autres, des informations pertinentes et des connaissances importantes pour la partie touchée. Une spécification du type de système touché est par exemple importante à cet égard. Ensuite, lors du signalement, il faut indiquer le moment auquel l'atteinte ICT concernée a commencé. Enfin, le signalement doit évoquer les mesures déjà prises, afin qu'il soit également possible de prodiguer des conseils sur cette base quant aux éventuelles mesures supplémentaires à prendre. Il importe également que le signalement indique le temps de réparation prévu ainsi que les coordonnées de la partie concernée afin qu'elle puisse être contactée au besoin dans le cadre de l'assistance.

Parties soumises à l'obligation de signalement

La présente proposition de loi contient une obligation de signalement pour les organisations qui fournissent des biens ou des services vitaux au sein de divers secteurs. Il s'agit en l'occurrence de parties de l'infrastructure vitale où une atteinte directe ou indirecte (effet de cascade) peut entraîner une déstabilisation sociale. Les fournisseurs auxquels s'applique l'obligation de signalement seront désignés par le Comité ministériel, après avis des régions. Seront au moins reprises dans la liste des parties soumises à l'obligation de signalement:

— les organisations actives dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Comité ministériel du renseignement et de la sécurité (d'après la loi du 30 novembre 1998 organique des services de renseignement et de sécurité);

organisaties en het waarschuwen van andere vitale organisaties voor gebleken kwetsbaarheden met als doel om maatschappelijke ontwrichting te voorkomen of in elk geval zo veel mogelijk te beperken.

Melding

Met het oog op de bovenstaande nieuwe taak van het Ministerieel Comité is het van belang dat de melding aan het Comité bestaat uit voldoende informatie om daadwerkelijk invulling te geven aan deze taak en een inschatting te kunnen maken van de risico's van een inbreuk en de in verband daarmee benodigde maatregelen. Daarbij is het van belang dat de melding, hoewel deze qua aard per vitale sector verschilt, in elk geval bestaat uit een aantal elementen.

Ten eerste dient de melding inzicht te geven in de aard en omvang van de ICT-inbreuk. Op basis van deze informatie kan onder meer gericht in het nationale en internationale netwerk gezocht worden naar relevante informatie en kennis die voor de getroffen partij van belang is. Een specificatie van het soort getroffen systemen is in dit verband bijvoorbeeld van belang. Ten tweede dient bij de melding aangegeven te worden wat het tijdstip van aanvang van de betrokken ICT-inbreuk is. Ten derde dient de melding in te gaan op de reeds getroffen maatregelen, zodat mede op basis daarvan geadviseerd kan worden over de eventuele nog te treffen aanvullende maatregelen. Ook is het van belang dat de melding ingaat op de te verwachten hersteltijd, én dat de melding contactgegevens van de betrokken partij bevat, zodat desgewenst in nader contact kan worden getreden in het kader van de hulpverlening.

Meldplichtige partijen

Dit wetsvoorstel bevat een meldplicht voor organisaties die vitale goederen of diensten aanbieden binnen diverse sectoren. Het gaat daarbij om onderdelen van de vitale infrastructuur waarbij een inbreuk direct of indirect (cascade-effect) tot maatschappelijke ontwrichting kan leiden. De aanbieders waarvoor de meldplicht gaat gelden, zullen worden aangewezen door het Ministerieel Comité, na advies van de gewesten. Minstens opgenomen in de lijst van meldplichtige partijen worden:

— organisaties die actief zijn in de economische en industriële sectoren die verbonden zijn met Defensie en die opgenomen zijn in een door het Ministerieel Comité voor inlichting en veiligheid goedgekeurde lijst (volgens de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst);

— les organisations qui entrent dans le champ d'application du Décret flamand du 15 juin 2012 sur le commerce des armes ainsi que du décret wallon et de l'ordonnance bruxelloise en la matière;

— les organisations qui entrent dans le champ d'application de la loi du 22 mai 2001 portant assentiment à l'accord de coopération du 21 juin 1999 entre l'État fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses.

Les organisations qui ne sont pas soumises à l'obligation de signalement peuvent, sur une base volontaire, signaler des atteintes TIC au Comité ministériel. Le traitement d'un signalement volontaire se déroule comme celui d'un signalement par une partie soumise à l'obligation de signalement. Une organisation non soumise à l'obligation de signalement qui signale une atteinte TIC bénéficie de la même confidentialité qu'une partie soumise à l'obligation de signalement.

Atteintes TIC à signaler

L'obligation de signalement prévue par la présente proposition de loi concerne uniquement les véritables atteintes à la sécurité et les véritables pertes d'intégrité d'un système d'information électronique. La proposition de loi ne s'applique pas aux dérangements qui n'ont rien à voir avec ce type d'atteinte TIC, comme les attaques DDoS (*Distributed Denial of Service*). Lors d'une attaque DDoS, il est porté atteinte à l'accessibilité d'un service en ligne sans que les systèmes utilisés à cet égard soient affectés.

En outre, lors de ce type d'attaques, l'indisponibilité ne sera généralement que temporaire. Dans ces cas, l'effet de désagrégation sociale est dès lors généralement beaucoup plus réduit que dans le cas de véritables atteintes TIC. Il n'empêche, cependant, que les organisations ont toujours la possibilité de signaler volontairement au Comité ministériel les problèmes sérieux d'accessibilité.

Les organisations à désigner dans les secteurs vitaux ne sont pas obligées de signaler chaque atteinte TIC au Comité ministériel. L'obligation de signalement s'applique uniquement lorsque l'atteinte entraîne ou peut entraîner une importante rupture de disponibilité ou de fiabilité du bien ou du service désigné. Il conviendra de préciser notamment en concertation avec les secteurs et départements concernés ce qu'il faut entendre par "important" pour les différents biens et services concernés. À cet égard, la question de savoir dans

— organisaties die vallen onder de toepassing van het Vlaamse Wapenhandeldecreet van 15 juni 2012, evenals het Waalse decreet en de Brusselse ordonnantie ter zake;

— organisaties die vallen onder de toepassing van de wet van 22 mei 2001 houdende instemming met het Samenwerkingsakkoord van 21 juni 1999 tussen de Federale Staat, het Vlaams, het Waals en het Brussels Hoofdstedelijk Gewest betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken.

Organisaties die niet onder de meldplicht vallen, kunnen op basis van vrijwilligheid ICT-inbreuken melden bij het Ministerieel Comité. De afhandeling van een vrijwillige melding gebeurt op dezelfde wijze als een melding door een meldplichtige partij. Een niet-meldplichtige organisatie die een ICT-inbreuk meldt, geniet dezelfde vertrouwelijkheid als een meldplichtige partij.

Te melden ICT-inbreuken

De meldplicht in dit wetsvoorstel heeft alleen betrekking op een daadwerkelijke inbreuk op de veiligheid en op een daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem. Het wetsvoorstel heeft geen betrekking op verstoringen waarbij geen sprake is van een dergelijke ICT-inbreuk, zoals DDoS-aanvallen (*Distributed Denial of Service*). Bij een DDoS-aanval wordt de bereikbaarheid van een onlinedienst aangetast zonder aantasting van de systemen die in dat verband worden gebruikt.

Veelal zal het bij deze aanvallen bovendien om een tijdelijke beperking van de bereikbaarheid gaan. Hierdoor is de maatschappelijk ontwrichtende werking in deze gevallen in het algemeen veel beperkter dan in geval van daadwerkelijke ICT-inbreuken. Dat neemt overigens niet weg dat organisaties steeds de mogelijkheid hebben om ernstige verstoringen van de bereikbaarheid op basis van vrijwilligheid aan het Ministerieel Comité te melden.

De aan te wijzen organisaties in de vitale sectoren zijn niet verplicht om elke ICT-inbreuk aan het Ministerieel Comité te melden. De verplichting tot melden geldt alleen als de inbreuk tot gevolg heeft of kan hebben dat de beschikbaarheid of betrouwbaarheid van het aangewezen goed of de aangewezen dienst in belangrijke mate wordt of kan worden onderbroken. Mede op basis van overleg met de betrokken sectoren en departementen moet nader worden uitgewerkt wat voor de verschillende betrokken goederen en diensten moet worden verstaan

quelles circonstances il est ou peut être question d'une désagrégation sociale sera notamment déterminante.

Confidentialité

Afin de pouvoir aider l'organisation touchée et d'aider à prévenir ou à limiter les conséquences dommageables d'une atteinte TIC, le Comité ministériel devra souvent disposer de données confidentielles pour les entreprises concernées, qui ne peuvent tomber en de mauvaises mains. C'est ainsi que les données techniques concernant l'organisation de systèmes d'information électroniques pourraient être détournées par ceux qui souhaitent attaquer les systèmes. Il importe que les organisations qui seront soumises à l'obligation de signalement ne soient pas réticentes à communiquer des informations. C'est dans ce but qu'il convient de régler dûment l'utilisation confidentielle des informations. À cet effet, l'article 6 proposé prévoit à quelle fin et à qui des informations ou des conseils peuvent être donnés, sur la base des données communiquées au comité en vertu de l'obligation de signalement prévue dans la loi proposée. Les informations fournies dans le cadre du signalement concernent généralement les informations d'entreprise et de fabrication, visées à l'article 6, § 1er, 7°, de la loi du 11 avril 1994 relative à la publicité de l'administration.

Respect

Ainsi qu'il a été indiqué, l'obligation de signalement prévue dans la présente proposition de loi n'est pas assortie d'une possibilité de sanction. Le Comité ministériel ne contrôlera pas le respect de l'obligation de signalement et ne se verra pas conférer de pouvoir de sanction.

Le groupe cible se limite à l'autorité fédérale et aux acteurs vitaux dans les secteurs essentiels. L'utilité et la nécessité de partager des données confidentielles relatives aux atteintes TIC, qui sont ou peuvent être lourdes de conséquences, font l'object d'un large consensus en l'occurrence. Les parties précitées ont conscience de leurs responsabilités. L'instauration proposée de l'obligation de signalement, qui sera concrétisée en concertation avec les organisations concernées, créera les conditions favorables à un respect spontané.

Face au coût modeste que représente le signalement pour les organisations concernées, il y a d'importants bénéfices en termes de limitation des dommages et de résolution de problèmes. Les données fournies en application de l'obligation de signalement étant traitées de manière confidentielle, il n'y pas lieu de craindre une atteinte à la réputation ou à la compétitivité. Afin de

onder "in belangrijke mate". Daarbij zal mede bepalend zijn onder welke omstandigheden sprake is of kan zijn van maatschappelijke ontwrichting.

Vertrouwelijkheid

Om de getroffen organisatie te kunnen helpen en de schadelijke gevolgen van de ICT-inbreuk te helpen voorkomen of beperken, zal het Ministerieel Comité vaak moeten beschikken over bedrijfsvertrouwelijke gegevens die niet in verkeerde handen mogen vallen. Technische gegevens over de inrichting van elektronische informatiesystemen kunnen bijvoorbeeld misbruikt worden door degenen die de systemen willen aanvallen. Van belang is dat organisaties waarvoor de meldplicht gaat gelden, niet terughoudend zijn met het verschaffen van informatie. Met het oog hierop dient de vertrouwelijke omgang met informatie goed te worden geregeld. Daartoe regelt het voorgestelde artikel 6 met welk doel en aan wie informatie en advies mag worden verstrekt die gebaseerd is op de aan het Comité op grond van de in dit wetsvoorstel vervatte meldplicht verstrekte gegevens. De met betrekking tot de melding verstrekte informatie betreft in het algemeen de ondernemings- en fabricagegegevens als bedoeld in artikel 6, § 1, 7°, van de wet van 11 april 1994 betreffende de openbaarheid van bestuur.

Naleving

Zoals gezegd is de in dit wetsvoorstel vervatte meldplicht niet voorzien in de mogelijkheid van bestraffing. Het Ministerieel Comité gaat geen toezicht houden op de naleving van de meldplicht en krijgt ook geen handhavingsbevoegdheden.

De doelgroep is beperkt tot de federale overheid en de vitale actoren in de randvoorwaardelijke sectoren. Het nut en de noodzaak van het delen van vertrouwelijke gegevens met betrekking tot ICT-inbreuken die ernstige gevolgen hebben of kunnen krijgen, wordt hier breed gedragen. Voornoemde partijen zijn zich bewust van hun verantwoordelijkheid. Met de voorgestelde inrichting van de meldplicht die in samenwerking met de betrokken organisaties nader gestalte wordt gegeven, worden gunstige voorwaarden geschapen voor spontane naleving.

Tegenover de bescheiden kosten van melding voor de betrokken organisaties staan hoge baten in de vorm van schadebeperking en probleemoplossing. Gegevens die ter uitvoering van de meldplicht worden verstrekt, worden vertrouwelijk behandeld zodat voor schade aan reputatie of concurrentiepositie niet gevreesd hoeft te worden. Om deze vertrouwelijkheid mee te garanderen,

garantir cette confidentialité, la présente proposition de loi impose un devoir de discrétion aux autorités, assorti d'une disposition pénale.

Charges administratives

L'obligation de signalement prévue par la présente proposition de loi n'a aucune incidence sur les charges administratives qui pèsent sur les citoyens. Elle entraînera en revanche une légère hausse de celles incombant aux organisations qui relèvent de son champ d'application. Cet impact ne pourra faire l'objet d'une évaluation définitive que lorsque les acteurs soumis à l'obligation de signalement auront été identifiés. L'interprétation des termes "importante rupture" (article 4, § 1er) influencera également en partie l'étendue des charges administratives. Il s'indiquera de déterminer plus avant, en concertation avec les secteurs et départements concernés (si possible par secteur), quelles atteintes doivent être considérées comme suffisamment graves pour être soumises à l'obligation de signalement. Ces règles pourront par exemple être inscrites dans un arrêté royal pris sur proposition du Comité ministériel, ou traduites dans des lignes de conduite.

COMMENTAIRE DES ARTICLES

Art. 2

L'acteur peut être une personne morale ou une personne physique.

Système d'information: il s'agira souvent — mais pas nécessairement — de systèmes dépendant de l'internet.

Art. 3

Cet article règle la portée de la loi et confère un fondement légal pour la désignation, par arrêté royal pris sur proposition du Comité ministériel, des acteurs et des biens et services soumis à l'obligation de signalement inscrite dans l'article 4. Il doit s'agir de biens ou de services présentant une importance vitale pour notre société. L'acteur ne doit pas obligatoirement être établi en Belgique; l'essentiel est qu'il offre des biens ou des services présentant une importance vitale pour notre société.

legt dit wetsvoorstel de overheid een discretieverplichting met bijbehorende strafbepaling op.

Administratieve lasten

De in dit wetsvoorstel geregelde meldplicht heeft geen gevolgen voor de administratieve lasten van burgers maar zal wel leiden tot een bescheiden stijging van de administratieve lasten voor de organisaties die onder het toepassingsbereik vallen. Een definitieve raming kan pas worden gemaakt als vaststaat voor welke actoren de meldplicht zal gelden. Bovendien bepaalt ook de nadere uitwerking van "in belangrijke mate" (artikel 4, § 1) voor een deel de omvang van de administratieve lasten. Er moet samen met de betrokken sectoren en departementen — zo mogelijk per sector _ nader worden uitgewerkt welke inbreuken ernstig genoeg zijn om onder de meldplicht te vallen. Dit kan bijvoorbeeld door een koninklijk besluit genomen op voorstel van het Ministerieel Comité of door middel van beleidsregels.

ARTIKELSGEWIJZE TOELICHTING

Art. 2

Een actor kan zowel een rechtspersoon als een natuurlijke persoon zijn.

Informatiesysteem: Het zal vaak gaan om systemen die van het internet afhankelijk zijn maar dat is geen vereiste.

Art. 3

Dit artikel regelt de reikwijdte van de wet en geeft een grondslag voor aanwijzing bij koninklijk besluit genomen op voorstel van het Ministerieel Comité van de actoren en de goederen en diensten waarvoor de in artikel 4 opgenomen meldplicht geldt. Het moet gaan om voor onze samenleving vitale goederen of diensten. Een actor kan ook buiten België gevestigd zijn; het gaat erom dat hij goederen of diensten aanbiedt die vitaal zijn voor onze samenleving.

Art. 4

Ainsi qu'il a été précisé dans les développements, l'obligation de signalement s'applique uniquement en cas d'atteinte effective à la sécurité ou de perte effective d'intégrité d'un système d'information électronique, et non lorsqu'une (autre) perturbation, telle qu'une attaque DDOS se produit.

Par ailleurs, l'obligation de signalement ne s'applique que si l'atteinte TIC entraîne ou peut entraîner une importante rupture de disponibilité ou de fiabilité du bien ou service désigné. Il conviendra de préciser (par exemple dans l'arrêté royal pris sur proposition du Comité ministériel dont il est question au § 3, ou encore au moyen de lignes de conduite), en concertation notamment avec les secteurs et départements concernés, ce qu'il y a lieu d'entendre par "importante rupture de disponibilité ou de fiabilité" des différents biens et services visés. Il sera essentiel de définir à cet effet dans quelles circonstances il est ou peut être question de désagrégation sociale. Les critères à prendre en considération en l'espèce sont, par exemple, la longue durée de l'interruption d'un processus ou d'un service vital dont les effets sont ressentis tant par l'acteur que par d'autres parties. Il convient aussi de tenir compte de la gravité de l'atteinte, lorsque cette dernière se révèle aussi potentiellement nuisible pour d'autres parties au sein des pouvoirs publics et des secteurs vitaux.

L'obligation de signalement s'applique donc également lorsque l'atteinte TIC n'a pas encore effectivement entraîné une importante rupture de disponibilité ou de fiabilité d'un bien ou d'un service vital, mais que ce risque est bien présent. Il s'agit en effet également d'une information capitale pour la prévention de conséquences négatives pour la société. De précieux enseignements peuvent en outre être tirés de telles atteintes.

Il est important que le signalement d'une atteinte TIC soumise à l'obligation de signalement ait lieu dans les meilleurs délais, afin que le Comité ministériel soit en mesure d'évaluer aussi vite que possible les risques en termes de disponibilité ou de fiabilité d'un bien ou d'un service vital et d'apporter son aide en prenant des mesures visant à garantir ou à rétablir la disponibilité ou la fiabilité. Il convient à cet égard de tenir compte du fait qu'un certain délai s'écoulera parfois entre l'atteinte effective et le constat par l'acteur (de la gravité) de cette atteinte.

Les modalités d'application visées au § 3 servent notamment à concrétiser quelles données doivent être fournies en vertu de l'obligation de signalement en ce qui concerne les différents biens et services désignés, et la manière dont ces données doivent être fournies.

Art. 4

De meldplicht geldt alleen in geval van een daadwerkelijke inbreuk op de veiligheid of een daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem, en dus, zoals in het algemeen deel is toegelicht, niet tevens bij (andere) verstoringen, zoals DDoS-aanvallen.

De meldplicht geldt daarnaast alleen als door de ICT-inbreuk de beschikbaarheid of betrouwbaarheid van het aangewezen goed of de aangewezen dienst in belangrijke mate wordt of kan worden onderbroken. Mede op basis van overleg met de betrokken sectoren en departementen moet nader worden uitgewerkt (bijvoorbeeld bij het in § 3 bedoelde koninklijk besluit genomen op voorstel van het Ministerieel Comité of door middel van beleidsregels) wat voor de verschillende betrokken goederen en diensten moet worden verstaan onder "in belangrijke mate". Daarbij zal mede bepalend zijn onder welke omstandigheden sprake is of kan zijn van maatschappelijke ontwrichting. Hierbij gaat het bijvoorbeeld om criteria zoals langdurige uitval van een vitaal proces of vitale dienst waardoor zowel de actor als andere partijen geconfronteerd worden met de gevolgen van de uitval. Tevens valt daarbij te denken aan de ernst van de inbreuk, waardoor deze mogelijk ook voor andere partijen binnen de overheid en de vitale sectoren schadelijk is.

De meldplicht geldt dus ook als de ICT-inbreuk nog niet daadwerkelijk heeft geleid tot een belangrijke onderbreking van de beschikbaarheid of betrouwbaarheid van een vitaal goed of vitale dienst, maar dat gevolg wel zal kunnen hebben. Dit is immers evenzeer informatie die van groot belang is met het oog op het voorkomen van schadelijke maatschappelijke gevolgen. Bovendien kan ook van dergelijke inbreuken veel worden geleerd.

Van belang is het dat de melding van een ICT-inbreuk waarvoor de meldplicht geldt zo snel als mogelijk wordt gedaan, teneinde het Ministerieel Comité zo snel als mogelijk in de gelegenheid te brengen de risico's voor de beschikbaarheid of betrouwbaarheid van een vitaal goed of vitale dienst te kunnen bepalen en hulp te verlenen bij het treffen van maatregelen om de beschikbaarheid of betrouwbaarheid te waarborgen of herstellen. Daarbij dient in aanmerking genomen te worden dat soms enige tijd zal verstrijken tussen de feitelijke inbreuk en de constatering (van de ernst) daarvan door de actor.

De in § 3 bedoelde nadere regels dienen onder meer om te concretiseren welke gegevens voor de verschillende aangewezen goederen en diensten ingevolge de meldplicht verstrekt moeten worden en de wijze waarop de gegevens verstrekt moeten worden. De nadere

Les modalités d'application peuvent par exemple aussi être utilisées pour préciser ce qu'il convient d'entendre par "important" en ce qui concerne les différents biens et services désignés, pour l'application du § 1er.

Art. 5

Les acteurs qui ne sont pas soumis à l'obligation de signalement peuvent, sur une base volontaire, signaler des atteintes TIC au Comité ministériel. Le traitement d'un signalement volontaire se déroule comme celui d'un signalement par un acteur soumis à l'obligation de signalement. Un acteur non soumis à l'obligation de signalement qui signale une atteinte TIC doit bien sûr bénéficier de la même confidentialité qu'un acteur soumis à l'obligation de signalement.

Art. 6

L'obligation de signalement a pour objectif premier de permettre au Comité ministériel d'évaluer les risques de l'atteinte TIC et de venir en aide à l'acteur touché par cette atteinte.

L'intérêt sous-jacent de cette obligation est d'empêcher ou de limiter la désagrégation sociale dans notre pays. Les données fournies peuvent ensuite aussi servir pour conseiller et informer d'autres acteurs, les CERT désignés par le Comité ministériel et le public. Le signalement peut par exemple permettre, également en vue de limiter ou d'empêcher la désagrégation sociale, de prévenir d'autres parties au sein du secteur vital concerné ou d'autres secteurs vitaux, en leur fournissant des informations sur l'origine des attaques ciblées ou sur les vulnérabilités techniques de systèmes d'information utilisés en plusieurs endroits.

À cet égard, il va de soi que la transmission d'informations à d'autres acteurs dans l'optique précitée ne doit pas dépasser ce qui est strictement nécessaire pour permettre à ces acteurs de déterminer s'ils sont ou risquent d'être confrontés à un même type d'atteinte et de prendre les mesures qui s'imposent en cas d'atteinte (éventuelle) pour garantir la disponibilité et la fiabilité de leurs biens ou de leurs services qui présentent une importance vitale pour la société.

L'expression "Cellule de crise informatique" (§ 1er, 2°) désigne une CERT (*Computer emergency response Team*), c'est-à-dire une équipe d'experts en TIC capables de réagir rapidement et de manière adéquate lorsqu'un incident de sécurité menace des ordinateurs

regels kunnen bijvoorbeeld ook gebruikt worden om te verduidelijken wat voor de verschillende aangewezen goederen en diensten bij de toepassing van § 1 moet worden verstaan onder "in belangrijke mate".

Art. 5

Actoren die niet onder de meldplicht vallen, kunnen op basis van vrijwilligheid ICT-inbreuken melden bij het Ministerieel Comité. De afhandeling van een vrijwillige melding gebeurt op dezelfde wijze als een melding door een meldplichtige actor. Een niet-meldplichtige actor die een ICT-inbreuk meldt, moet uiteraard dezelfde vertrouwelijkheid genieten als een meldplichtige actor.

Art. 6

De meldplicht heeft primair tot doel om het Ministerieel Comité in staat te stellen om de risico's van de ICT-inbreuk te kunnen inschatten en de door de inbreuk getroffen actor bij te staan.

Het achterliggende belang daarvan is het voorkomen of beperken van maatschappelijke ontwrichting in ons land. De verstrekte gegevens mogen vervolgens ook worden gebruikt als basis voor advies en informatie aan andere actoren, aan door het Ministerieel Comité aangewezen CERT's en aan het publiek. De melding kan bijvoorbeeld aanleiding geven tot het, eveneens met het oog op het beperken of voorkomen van maatschappelijke ontwrichting, waarschuwen van andere partijen binnen de betrokken vitale sector of andere vitale sectoren, door informatie te verstrekken over de herkomst van gerichte aanvallen of over technische kwetsbaarheden in informatiesystemen die op meerdere plaatsen worden gebruikt.

Daarbij spreekt het voor zichzelf dat de informatieverstrekking aan andere actoren vanuit bovenbedoeld oogpunt niet verder gaat dan strikt noodzakelijk is om die actoren in staat te stellen om te bepalen of zij wellicht met een zelfde soort inbreuk of de mogelijkheid daarvan te maken hebben en om de maatregelen te nemen die in geval van een (mogelijke) inbreuk nodig zijn om de beschikbaarheid of betrouwbaarheid van hun voor de samenleving vitale goederen of diensten te waarborgen.

Met de term computercrisisteam (§ 1, 2°) wordt een CERT bedoeld. Een CERT is een team van ICT-experts dat snel en adequaat kan reageren op een beveiligingsincident met computers of netwerken met als doel om schade te beperken en snel herstel van de

ou des réseaux, dans le but de limiter les dégâts et de faciliter le rétablissement rapide du service. Les informations ne peuvent être transmises qu'aux CERT (belges ou étrangères) qui ont été désignées à cette fin par le Comité ministériel, après vérification que l'échange d'informations est légitime et justifié dans ce contexte

Il pourra s'avérer nécessaire de définir des règles supplémentaires relatives à l'article 6, § 1er, par exemple en ce qui concerne la désignation d'équipes d'experts (CERT) sur la base du § 1er, 2°.

À moins que la sécurité de l'État ne soit en cause, les données transmises peuvent également servir à informer le public. Dans ce cadre, il ne sera souvent pas nécessaire de communiquer des données qui peuvent se résumer à des acteurs individuels ou à des biens ou des services spécifiques, par exemple si le public doit être mis en garde contre les risques que représentent les méthodes de travail de criminels opérant sur internet. Mais parfois, l'information peut n'être utile que si l'acteur ou le bien ou le service est concrètement désigné, par exemple, s'il est nécessaire d'avertir le public qu'il est préférable d'éviter d'utiliser, jusqu'à nouvel ordre, un bien ou un service particulier. Avant de décider de communiquer ces informations, les intérêts doivent être mis en balance. Ainsi, l'intérêt du public d'être informé ne contrebalancera pas toujours l'intérêt de l'acteur concerné. Il n'est par ailleurs pas inimaginable que la communication aggrave encore le préjudice subi par la société, plutôt que de le prévenir ou de le limiter. Le Comité ministériel associera autant que possible à cette mise en balance des intérêts des Régions éventuellement concernées.

La peine mentionnée au § 3, prévue à l'article 43, 2° de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, est un emprisonnement de six mois à trois ans et une amende de cinq cents euros à trente mille euros ou une de ces peines seulement.

Le § 4 interdit tout autre utilisation des données que celle nécessaire pour évaluer les risques et aider l'acteur touché ainsi que pour exécuter le § 1er.

Art. 9

Bien que notre intention soit que la loi entre en vigueur dans son intégralité, nous n'excluons pas la possibilité d'une entrée en vigueur différenciée. Cette disposition n'a toutefois pas pour objectif de permettre une entrée en vigueur de l'obligation de signalement à des moments différents pour les différents acteurs, biens ou services concernés. Si une telle différenciation devait

dienstverlening te bevorderen. Informatieverstrekking kan alleen plaatsvinden aan die (buitenlandse of Belgische) CERT's die, na toetsing of gegevensuitwisseling daarmee gerechtvaardigd en verantwoord is, daartoe door het Ministerieel Comité zijn aangewezen.

Het kan wenselijk blijken om nadere regels te stellen over artikel 6, § 1, bijvoorbeeld over de aanwijzing van CERT's op grond van § 1, 2°.

Tenzij de staatsveiligheid in het geding is, mogen de verstrekte gegevens ook worden gebruikt als basis voor publieksvoorlichting. Daarbij zal het veelal niet nodig zijn om gegevens te verstrekken die herleid kunnen worden tot afzonderlijke actoren of afzonderlijke goederen en diensten, bijvoorbeeld als het publiek moet worden gewaarschuwd voor de risico's van een door internetcriminelen gehanteerde werkwijze. Maar soms zal de voorlichting alleen effectief kunnen zijn als de actor of het goed of de dienst concreet wordt aangeduid, bijvoorbeeld als het nodig is om het publiek te waarschuwen dat een bepaald goed of een bepaalde dienst tot nader order beter niet gebruikt kan worden. De beslissing om dergelijke voorlichting te geven, vergt een belangenafweging. Zo zal het belang van het publiek om op de hoogte te zijn niet altijd opwegen tegen het belang van de betrokken actor. Denkbaar is ook dat de bekendmaking de maatschappelijke schade juist vergroot in plaats van voorkomt of beperkt. Het Ministerieel Comité zal zo mogelijk eventuele betrokken gewesten betrekken bij deze belangenafweging.

De in § 3 vermelde straf, bepaald in artikel 43, 2° van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, is een gevangenisstraf van zes maanden tot drie jaar en een geldboete van vijfhonderd euro tot dertigduizend euro of een van die straffen alleen.

§ 4 verbiedt ander gebruik dan nodig is voor risicoinschatting en hulp aan de getroffen actor, dan wel de uitvoering van § 1.

Art. 9

Hoewel het in de bedoeling ligt om deze wet als één geheel in werking te laten treden, is de mogelijkheid van gedifferentieerde inwerkingtreding opengehouden. De bepaling is niet bedoeld om de meldplicht voor afzonderlijke actoren, goederen of diensten op verschillende tijdstippen in werking te kunnen laten treden. Mocht een dergelijke differentiatie nodig zijn, dan kan zij eventueel

s'avérer nécessaire, elle pourrait éventuellement être formalisée dans l'arrêté royal visé à l'article 3.

worden vormgegeven in het koninklijk besluit, bedoeld in artikel 3.

Karolien GROSEMANS (N-VA)
Theo FRANCKEN (N-VA)
Jan JAMBON (N-VA)
Bert MAERTENS (N-VA)

PROPOSITION DE LOI

Article 1er

La présente loi règle une matière visée à l'article 78 de la Constitution.

Art. 2

Pour l'application de la présente loi, on entend par:

1° acteur: toute personne physique ou morale qui exploite, gère ou met à disposition un bien ou un service:

2° système d'information: système piloté, en tout ou en partie, par des moyens électroniques, dont dépend la réalisation d'un bien ou d'un service;

3° comité ministériel: le comité ministériel qui a, dans ses attributions, la politique générale en matière de renseignement et de sécurité.

Art. 3

§ 1er. Les acteurs de biens ou de services d'une importance telle pour la société qu'une rupture au niveau de leur disponibilité ou fiabilité peut avoir des conséquences sociales graves, sont soumis à une obligation de signalement.

§ 2. Les acteurs visés au § 1er sont:

1° les personnes physiques et morales figurant sur la liste approuvée par le Comité ministériel, visées à l'article 11, § 1er, 1°, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2° les personnes physiques et morales soumises à l'application du décret flamand du 15 juin 2012 concernant l'importation, l'exportation, le transit et le transfert de produits liés à la défense, d'autre matériel à usage militaire, de matériel de maintien de l'ordre, d'armes à feu civiles, de pièces et de munitions, dit "Décret sur le commerce des armes";

3° les personnes physiques et morales soumises à l'application du décret wallon du 21 juin 2012 relatif à l'importation, à l'exportation, au transit et au transfert d'armes civiles et de produits liés à la défense;

WETSVOORSTEL

Art. 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

Art. 2

Voor de toepassing van deze wet wordt verstaan onder:

1° actor: elk natuurlijk of rechtspersoon die een goed of dienst exploiteert, beheert of beschikbaar stelt;

2° informatiesysteem: geheel of gedeeltelijk met elektronische middelen bestuurd systeem waarvan de realisatie van een goed of dienst afhankelijk is;

3° het Ministerieel Comité: het Ministerieel Comité dat de vaststelling van de algemene politiek inzake inlichtingen en veiligheid onder zijn bevoegdheden heeft.

Art. 3

§ 1. Actoren van goederen of diensten die van zodanig belang zijn voor de samenleving dat onderbreking van de beschikbaarheid of betrouwbaarheid daarvan kan leiden tot ernstige maatschappelijke gevolgen hebben meldplicht.

§ 2. De actoren bedoeld in § 1 zijn:

1° de natuurlijke en rechtspersonen die opgenomen zijn in de door het Ministerieel Comité goedgekeurde lijst, bedoeld in artikel 11, § 1, 1°, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst;

2° de natuurlijke en rechtspersonen die vallen onder de toepassing van het Vlaams decreet betreffende de in-, uit-, doorvoer en overbrenging van defensiegerelateerde producten, ander voor militair gebruik dienstig materiaal, ordehandhavingsmateriaal, civiele vuurwapens, onderdelen en munitie Wapenhandeldecreet van 15 juni 2012;

3° de natuurlijke en rechtspersonen die vallen onder de toepassing van het Waals decreet betreffende de invoer, uitvoer, doorvoer en overdracht van civiele wapens en van defensiegerelateerde producten van 21 juni 2012;

4° les personnes physiques et morales soumises à l'application de l'ordonnance de la Région de Bruxelles-capitale du 20 juin 2013 relative à l'importation, à l'exportation, au transit et au transfert de produits liés à la défense, d'autre matériel pouvant servir à un usage militaire, de matériel lié au maintien de l'ordre, d'armes à feu à usage civil, de leurs pièces, accessoires et munitions;

5° les personnes physiques et morales soumises à l'application de la loi du 22 mai 2001portant assentiment à l'Accord de coopération du 21 juin 1999 entre l'État fédéral, les régions flamande, wallonne et de Bruxelles-Capitale relatif à la maîtrise de dangers liés aux accidents majeurs impliquant des substances dangereuses.

§ 3. Sur proposition du Comité ministériel, le Roi peut désigner des acteurs supplémentaires.

Le Comité ministériel demande d'abord l'avis des gouvernements régionaux.

Art. 4

§ 1er. L'acteur informe sans délai le Comité ministériel de toute atteinte à la sécurité ou de toute perte d'intégrité de son système informatique entraînant ou pouvant entraîner une importante rupture de disponibilité ou de fiabilité d'un bien ou service.

§ 2. La notification mentionne en tout cas les éléments suivants:

1° la nature et l'ampleur de l'atteinte ou de la perte;

2° le moment du début de l'atteinte ou de la perte;

3° les conséquences potentielles de l'atteinte ou de la perte;

4° un pronostic du temps de réparation;

5° si possible, les mesures prises ou à prendre par l'acteur afin de limiter les conséquences de l'atteinte ou de la perte ou de prévenir sa répétition;

6° les coordonnées de l'agent responsable de la notification et agissant dès lors en qualité de personne de contact;

§ 3. Sur proposition du Comité ministériel, le Roi fixe les modalités d'application, et notamment:

4° de natuurlijke en rechtspersonen die vallen onder de toepassing van de ordonnantie van het Brussels Hoofdstedelijk Gewest betreffende de in-, uit-, doorvoer en overbrenging van defensiegerelateerde producten, ander voor militair gebruik dienstig materiaal, ordehandhavingsmateriaal, civiele vuurwapens, onderdelen, toebehoren en munitie ervan van 20 juni 2013;

5° de natuurlijke en rechtspersonen die vallen onder de toepassing van de wet van 22 mei 2001 houdende instemming met het Samenwerkingsakkoord van 21 juni 1999 tussen de Federale Staat, het Vlaams, het Waals en het Brussels Hoofdstedelijk Gewest betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken.

§ 3. Op voorstel van het Ministerieel Comité kan de Koning bijkomende actoren aanwijzen.

Het Ministerieel Comité vraagt eerst advies aan de gewestregeringen.

Art. 4

§ 1. De actor geeft het Ministerieel Comité onverwijld kennis van een inbreuk op de veiligheid of een verlies van integriteit van zijn informatiesysteem waardoor de beschikbaarheid of betrouwbaarheid van een goed of dienst in belangrijke mate wordt of kan worden onderbroken.

§ 2. De kennisgeving omvat in ieder geval:

1° de aard en omvang van de inbreuk of het verlies;

2° het tijdstip van de aanvang van de inbreuk of het verlies;

3° de mogelijke gevolgen van de inbreuk of het verlies;

4° een prognose van de hersteltijd;

5° zo mogelijk de door de actor genomen of te nemen maatregelen om de gevolgen van de inbreuk of het verlies te beperken of herhaling hiervan te voorkomen;

6° de contactgegevens van de functionaris die verantwoordelijk is voor het doen van de kennisgeving en aldus optreedt als contactpersoon.

§ 3. Op voorstel van het Ministerieel Comité bepaalt de Koning de nadere regelen waaronder:

1° les données à fournir en application des § 1er et 2;

2° la manière dont une notification au sens des § 1er et 2 doit être faite.

Art. 5

Les acteurs auxquels la présente loi ne s'applique pas, peuvent également signaler au Comité ministériel une atteinte ou une perte visée à l'article 4, § 1er.

Le traitement d'un signalement visé au § 1er s'effectue selon les modalités prévues aux articles 6 et 7.

Art. 6

§ 1er. Afin de prévenir ou de limiter les conséquences sociales dommageables, en Belgique ou à l'étranger, d'une atteinte ou d'une perte visée à l'article 4, § 1er, le Comité ministériel peut utiliser les données reçues de l'acteur touché pour informer ou conseiller:

1° d'autres acteurs;

2° une cellule de crise informatique désignée par le Comité ministériel en Belgique ou à l'étranger;

3° le public, pour autant que la sécurité de l'État ne puisse en être compromise.

Sur proposition du Comité ministériel, le Roi fixe les modalités de l'utilisation visée au § 1er.

§ 2. À moins que l'intérêt général ne l'exige, les données pouvant être rapportées à des acteurs, des biens ou des services distincts ne sont pas fournies au public.

§ 3. Le ministre, l'autorité ou le fonctionnaire qui viole l'obligation visée au § 2 est puni de la peine visée à l'article 43, 2°, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

§ 4. Sans préjudice de dispositions légales contraires, les données sont utilisées exclusivement:

1° pour évaluer les risques de l'atteinte au système ICT;

1° de gegevens die ter uitvoering van de §§ 1 en 2 worden verstrekt;

2° de wijze waarop een kennisgeving als bedoeld in de §§ 1 en 2 wordt gedaan.

Art. 5

Actoren waarop deze wet niet van toepassing is, kunnen eveneens een inbreuk of een verlies als bedoeld in artikel 4, § 1, melden bij het Ministerieel Comité.

De afhandeling van een kennisgeving bedoeld in § 1 geschiedt op de wijze bedoeld in de artikelen 6 en 7.

Art. 6

§ 1. Ter voorkoming of beperking van schadelijke maatschappelijke gevolgen in of buiten België, van een inbreuk of een verlies bedoeld in artikel 4, § 1, kan het Ministerieel Comité gegevens die werden ontvangen van de getroffen actor gebruiken voor het geven van informatie en advies aan:

1° andere actoren;

2° een door het Ministerieel Comité aangewezen computercrisisteam in of buiten België;

3° het publiek, mits de veiligheid van de Staat daarmee niet geschaad kan worden.

Op voorstel van het Ministerieel Comité bepaalt de Koning de nadere regelen van het gebruik bedoeld in het eerste lid.

§ 2. Tenzij het maatschappelijke belang dat vergt, worden aan het publiek geen gegevens verstrekt die herleid kunnen worden tot afzonderlijke actoren, goederen of diensten.

§ 3. De minister, overheid of ambtenaar die de verplichting bedoeld in § 2 schendt, wordt gestraft met de straf bedoeld in artikel 43, 2°, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst.

§ 4. Onverminderd andersluidende wettelijke bepalingen worden de gegevens uitsluitend gebruikt:

1° om de risico's van de ICT-inbreuk in te schatten;

2° pour aider l'acteur touché par l'atteinte à prendre des mesures pour garantir ou rétablir la disponibilité et la fiabilité du bien ou du service;

3° pour exécuter le § 1er.

Art. 7

§ 1er. Le Comité ministériel examine l'atteinte ou la perte visée à l'article 4, § 1er, et établit un rapport dans les trois mois qui suivent la déclaration.

§ 2. Ce rapport est communiqué aux gouvernements régionaux.

§ 3. Sur proposition du Comité ministériel, le Roi fixe les modalités d'application, notamment:

1° la manière dont le Comité ministériel examine l'atteinte ou la perte visée à l'article 7, § 1er;

2° la manière dont le rapport visé à l'article 7, § 2, est transmis.

Art. 8

La présente loi est également appelée 'loi relative au signalement des atteintes aux systèmes d'information électroniques'.

Art. 9

La présente loi entre en vigueur le premier jour du douzième mois qui suit celui au cours duquel elle aura été publiée au *Moniteur belge*.

Le Roi peut fixer une date d'entrée en vigueur antérieure à celle mentionnée à l'alinéa 1er pour chacune des dispositions de la présente loi.

30 octobre 2013

2° om de door de inbreuk getroffen actor bij te staan bij het treffen van maatregelen om de beschikbaarheid en betrouwbaarheid van het goed of de dienst te waarborgen of te herstellen;

3° ter uitvoering van § 1.

Art. 7

§ 1. Het Ministerieel Comité onderzoekt een inbreuk of een verlies bedoeld in artikel 4, § 1 en maakt binnen drie maanden na de aangifte hiervan een verslag op.

§ 2. Dit verslag wordt bezorgd aan de gewestregeringen.

§ 3. Op voorstel van het Ministerieel Comité bepaalt de Koning de nadere regelen, waaronder:

1° de wijze waarop het Ministerieel Comité een inbreuk of een verlies bedoeld in artikel 7, § 1 onderzoekt;

2° de wijze waarop een verslag bedoeld in artikel 7, § 2 wordt overgemaakt.

Art. 8

Deze wet wordt ook 'wet melding inbreuken elektronische informatiesystemen' genoemd.

Art. 9

Deze wet treedt in werking op de eerste dag van de twaalfde maand na die waarin ze is bekendgemaakt in het *Belgisch Staatsblad*.

De Koning kan voor ieder bepaling ervan een datum van inwerkingtreding bepalen voorafgaand aan de datum vermeld in het eerste lid.

30 oktober 2013

Karolien GROSEMANS (N-VA)
Theo FRANCKEN (N-VA)
Jan JAMBON (N-VA)
Bert MAERTENS (N-VA)

Centrale drukkerij – Imprimerie centrale