DOC 55 **2635/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

20 avril 2022

PROPOSITION DE LOI

modifiant la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques en ce qui concerne l'utilisation obligatoire de réseaux unidirectionnels

(déposée par M. Michael Freilich et consorts)

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

20 april 2022

WETSVOORSTEL

tot wijziging van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren wat de verplichting van het gebruik van unidirectionele netwerken betreft

(ingediend door de heer Michael Freilich c.s.)

N-VA	:	*Nieuw-Vlaamse Alliantie*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
PS	:	*Parti Socialiste*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Open Vld	:	*Open Vlaamse liberalen en democraten*
Vooruit	:	*Vooruit*
Les Engagés	:	*Les Engagés*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de nummering van de publicaties:*	
DOC 55 0000/000	*Document de la 55e législature, suivi du numéro de base et numéro de suivi*	*DOC 55 0000/000*	*Parlementair document van de 55e zittingsperiode + basisnummer en volgnummer*
QRVA	*Questions et Réponses écrites*	*QRVA*	*Schriftelijke Vragen en Antwoorden*
CRIV	*Version provisoire du Compte Rendu Intégral*	*CRIV*	*Voorlopige versie van het Integraal Verslag*
CRABV	*Compte Rendu Analytique*	*CRABV*	*Beknopt Verslag*
CRIV	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*	*CRIV*	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénière*	*PLEN*	*Plenum*
COM	*Réunion de commission*	*COM*	*Commissievergadering*
MOT	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT*	*Moties tot besluit van interpellaties (beigekleurig papier)*

RÉSUMÉ

Les cyberattaques contre des infrastructures critiques ne sont pas un phénomène nouveau. Entre début 2020 et mi-2021, treize cyberincidents visant des infrastructures critiques ont été signalés en Belgique. Une véritable course aux cyberarmes s'est engagée. Les États vont de plus en plus loin en matière d'attaque et d'espionnage en ligne de leurs infrastructures et réseaux mutuels. Les conflits géopolitiques se prolongent dans le cyberespace. Les cyberopérations menées contre des infrastructures critiques peuvent avoir des conséquences plus importantes qu'une attaque au moyen d'armes de destruction massive.

Lorsqu'une cyberattaque contre une infrastructure critique peut conduire à un Mass Casualty Incident, c'est-à-dire un incident faisant un grand nombre de victimes, la meilleure façon de protéger cette infrastructure contre les attaques extérieures est d'utiliser des unidirectional gateways ou réseaux unidirectionnels. Il s'agit d'une nouvelle technologie qui garantit une connexion sûre à cent pour cent entre les systèmes de données sans aucune possibilité de piratage.

L'auteur de cette proposition de loi estime qu'il convient d'accroître la résilience de nos intérêts vitaux et de nos infrastructures. Il pense qu'il faut prendre des mesures supplémentaires adaptées aux nouvelles menaces et aux nouveaux risques et préconise la mise en œuvre de unidirectional gateways pour mieux nous protéger contre les cybermenaces et les cyberincidents, afin que tout accès non autorisé devienne impossible.

En modifiant la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, l'auteur de cette proposition de loi entend rendre obligatoire l'utilisation de réseaux unidirectionnels. Cette obligation s'applique uniquement aux infrastructures critiques dans lesquelles des incidents peuvent gravement déstabiliser la société et faire un très grand nombre de victimes. Un délai d'un an et demi est accordé aux opérateurs concernés pour mettre en œuvre la nouvelle technique de protection.

SAMENVATTING

Cyberaanvallen op kritieke infrastructuur zijn niet nieuw. Van begin 2020 tot halfweg 2021 werden in België dertien cyberincidenten gemeld die gericht waren tegen de kritieke infrastructuur. Er is een echte cyberwapenwedloop aan de gang. Staten gaan almaar verder in het online bestoken en bespioneren van elkaars netwerken en infrastructuur. Geopolitieke conflicten krijgen een verlengstuk in cyberspace. Cyberoperaties tegen kritieke infrastructuren kunnen grotere gevolgen hebben dan een aanval met massavernietigingswapens.

Wanneer een cyberaanval op een kritieke infrastructuur aanleiding kan geven tot een Mass Casualty Incident – incidenten met een massa aan slachtoffers – wordt die infrastructuur best beschermd tegen aanvallen van buitenaf met unidirectional gateways of unidirectionele netwerken. Dit is een nieuwe technologie die een honderd procent veilige verbinding tussen datasystemen garandeert zonder de kans dat ze worden gehackt.

De indiener van dit wetsvoorstel is van mening dat de weerbaarheid van onze vitale belangen en infrastructuur moet vergroten. Hij is van oordeel dat bijkomende maatregelen moeten worden genomen in functie van de nieuwe dreigingen en risico's en pleit voor de implementatie van unidirectionale gateways om ons beter te beschermen tegen cyberdreigingen en -incidenten zodat ongeautoriseerde toegang onmogelijk wordt.

Door een wijziging van de wet van 1 juli 2011 betreffende de beveiliging van de kritieke infrastructuren beoogt de indiener van het wetsvoorstel het gebruik van unidirectionele netwerken te verplichten. De verplichting geldt enkel voor kritieke infrastructuur waar incidenten ernstige maatschappelijke ontwrichtingen kunnen veroorzaken en waarbij een massa slachtoffers kunnen vallen. De betrokken operatoren krijgen anderhalf jaar tijd om de nieuwe beveiligingstechniek te implementeren.

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

Contexte

Les infrastructures critiques doivent être protégées de manière optimale contre les cyberattaques. Les incidents impliquant ces infrastructures peuvent en effet avoir un impact à grande échelle, un impact national. Les nouvelles techniques de protection doivent suivre les évolutions technologiques. La législation belge sur les NIS[1] fait explicitement référence aux secteurs des transports, de l'énergie, des finances, des communications électroniques, de l'eau potable, de la santé publique, des infrastructures numériques et de l'espace. Un incident ou une attaque dans l'un de ces secteurs peut avoir de graves conséquences pour les fonctions vitales. Les exploitants de ces infrastructures critiques sont déjà tenus d'établir un plan de sécurité, d'organiser des exercices et des inspections, de signaler les incidents et de prendre des mesures supplémentaires en fonction des menaces.

Parmi les différentes infrastructures critiques, nous pouvons établir une distinction entre les organisations d'importance stratégique (telles que les transports et les télécommunications) et les infrastructures critiques qui, si elles sont manipulées de manière malveillante, peuvent directement conduire à des *Mass Casualty Incidents* (ci-après: "MCI"), des incidents pouvant faire de nombreuses victimes. C'est cette dernière catégorie d'infrastructures que nous souhaitons mieux protéger des cyberattaques qui peuvent causer beaucoup de dommages directs et faire de nombreuses victimes.

Nous songeons, par exemple, à l'ouverture d'un barrage entraînant l'inondation d'une vallée, à la manipulation d'une centrale électrique provoquant son explosion ou à l'adaptation des paramètres d'une station d'épuration rendant l'eau potable toxique.

Les cyberattaques contre des infrastructures critiques

Les cyberattaques contre des infrastructures critiques ne sont pas un phénomène nouveau. Il y a près de dix ans, l'opérateur de télécommunications belge Belgacom (aujourd'hui Proximus) a été touché. Entre début 2020 et mi-2021, treize cyberincidents visant des infrastructures critiques ont été signalés en Belgique.

[1] NIS: network and information systems.

TOELICHTING

DAMES EN HEREN,

Achtergrond

Kritieke infrastructuren dienen optimaal te worden beschermd tegen cyberaanvallen. Incidenten ten aanzien van deze infrastructuren kunnen immers een grootschalige, nationale impact hebben. De nieuwe beschermingstechnieken moeten de technologische evoluties volgen. De Belgische NIS-wetgeving[1]verwijst expliciet naar de sectoren vervoer, energie, financiën, elektronische communicatie, drinkwater, volksgezondheid, digitale infrastructuur en ruimtevaart. Een incident of aanval in een van deze sectoren kan ernstige gevolgen hebben voor de vitale functies. De uitbaters van dergelijke kritieke infrastructuren zijn reeds verplicht om een beveiligingsplan op te stellen, oefeningen en inspecties te organiseren, incidenten te melden alsmede bijkomende maatregelen te nemen in functie van de dreigingen.

Binnen de verschillende kritieke infrastructuren kunnen we een onderscheid maken tussen organisaties van strategisch belang (zoals vervoer en telecommunicatie) en kritieke infrastructuren die, indien ze op kwaadaardige wijze worden gemanipuleerd, rechtstreeks kunnen leiden tot *Mass Casualty Incidents* (MCIs). Het is deze laatste categorie die we beter willen beschermen tegen cyberaanvallen die veel directe schade en slachtoffers kunnen veroorzaken.

Wij denken bijvoorbeeld aan een waterdam die opengezet wordt en een vallei doet overstromen, een elektriciteitscentrale die gemanipuleerd wordt en ontploft, een waterzuiveringsinstallatie waarvan de parameters worden aangepast waardoor het drinkwater kan vergiftigd worden.

Cyberaanvallen op kritieke infrastructuur

Cyberaanvallen op kritieke infrastructuur zijn niet nieuw. Bijna tien jaar geleden raakte bekend dat de Belgische telecomoperator Belgacom (nu Proximus) werd getroffen. Van begin 2020 tot halfweg 2021 werden in België dertien cyberincidenten gemeld die gericht waren tegen de kritieke infrastructuur.

[1] NIS: network and information systems.

L'année dernière à Genève, le président américain Joe Biden et son homologue russe Vladimir Poutine ont discuté des cyberattaques visant les infrastructures critiques américaines (ministères et entreprises). L'une des plus grandes cyberattaques de l'histoire s'était produite sur la côte est des États-Unis. Au moyen d'une attaque numérique utilisant un rançongiciel (*ransomware*), les pirates avaient réussi à pénétrer de l'extérieur dans les systèmes informatiques de *Colonial Pipeline*. La quasi-totalité du réseau de pipelines de la société américaine avait été paralysée à la suite de ce piratage. Cela avait entraîné une grave pénurie de carburant dans plusieurs États. Début 2021, une station d'épuration a été touchée à Oldsmar, en Floride. Les pirates avaient tenté de multiplier par 100 le niveau d'hydroxyde de sodium, ce qui peut avoir de graves conséquences pour la santé publique.

Une véritable course aux cyberarmes s'est engagée. Les États vont de plus en plus loin en matière d'attaque et d'espionnage en ligne de leurs infrastructures et réseaux mutuels. Le monde numérique est devenu le reflet des tensions qui règnent dans le monde. Les conflits géopolitiques se prolongent dans le cyberespace. Les cyberopérations menées contre des infrastructures critiques peuvent avoir des conséquences plus importantes qu'une attaque au moyen d'armes de destruction massive.

Nous assistons aujourd'hui à une guerre hybride en Ukraine. C'est la toute première fois que nous constatons des cyberattaques d'une telle ampleur. Les bombes et les obus virtuels ne se limitent pas nécessairement à Kiev et Moscou. Une cyberattaque bien ciblée contre la Belgique n'est certainement pas inconcevable. Lorsqu'une cyberattaque dirigée contre une infrastructure critique peut engendrer un MCI, il est préférable de protéger cette infrastructure contre les attaques de l'extérieur au moyen de réseaux unidirectionnels.

Unidirectional gateways (UDG's)

Jusqu'il y a deux décennies, il n'existait pas de connexions entre les systèmes de contrôle et le monde extérieur dans le monde industriel. À l'époque, les opérateurs ont découvert que les systèmes de contrôle contenaient une mine d'informations qui pouvaient les aider à gérer leur entreprise. Pour pouvoir collecter ces données, ils ont connecté leurs réseaux de contrôle à leurs réseaux d'entreprise et à l'internet. Ils ont alors également introduit les enjeux de sécurité. Les réseaux connectés les ont exposés à des risques et à des menaces, comme les virus notamment. Ceux-ci peuvent être introduits par le biais des réseaux. À l'heure actuelle, les pare-feu ne suffisent plus à écarter les dangers. De nouvelles technologies de protection ont donc été développées.

Vorig jaar bespraken de Amerikaanse president Joe Biden en zijn Russische collega Vladimir Poetin in Genève de cyberaanvallen op Amerikaanse kritieke infrastructuur (ministeries en bedrijven). Aan de oostkust van de Verenigde Staten had zich een van de grootste cyberaanvallen uit de geschiedenis voorgedaan. Met een digitale aanval die gebruikmaakte van ransomware slaagden hackers er in om de computersystemen van Colonial Pipeline van buitenaf binnen te dringen. Vrijwel het hele pijpleidingennetwerk van het Amerikaanse bedrijf viel door die hack stil. Er ontstond een schrijnend tekort aan brandstof in diverse staten. Begin 2021 werd in Oldsmar (Florida) een waterzuiveringsinstallatie getroffen. De hackers probeerden het niveau van sodium hydroxide op te drijven met een factor 100 wat ernstige gevolgen kon hebben voor de volksgezondheid.

Er is een echte cyberwapenwedloop aan de gang. Staten gaan almaar verder in het online bestoken en bespioneren van elkaars netwerken en infrastructuur. De digitale wereld is een afspiegeling geworden van de heersende mondiale spanningen. Geopolitieke conflicten krijgen een verlengstuk in cyberspace. Cyberoperaties tegen kritieke infrastructuren kunnen grotere gevolgen hebben dan een aanval met massavernietigingswapens.

Vandaag zijn we getuige van een hybride oorlogsvoering in Oekraïne. Het is de allereerste keer dat we cyberaanvallen op zo'n grote schaal vaststellen. De virtuele bommen en granaten beperken zich niet noodzakelijk tot Kiev en Moskou. Een goed gemikte cyberaanval tegen België is zeker niet ondenkbaar. Wanneer een cyberaanval op een kritieke infrastructuur aanleiding kan geven tot een MCI wordt die infrastructuur best beschermd tegen aanvallen van buitenaf met unidirectionele netwerken.

Unidirectional gateways (UDG's)

Tot twee decennia geleden bestonden er in de industriële wereld geen connecties tussen controlesystemen en de buitenwereld. Toen ontdekten operatoren dat die controlesystemen een schat aan informatie bevatten die hen kunnen helpen bij het beheer van hun bedrijf. Om deze data te kunnen verzamelen koppelden ze hun controlenetwerken met hun ondernemingsnetwerken en het internet. Op dat moment introduceerden ze ook de veiligheidsuitdagingen. De gekoppelde netwerken stelden hen bloot aan risico's en dreigingen zoals virussen en andere. Die kunnen via de netwerken worden binnengebracht. Vandaag volstaan firewalls niet langer om de gevaren buiten te houden. Dus werden nieuwe beschermingstechnologiën ontwikkeld.

Il existe aujourd'hui une nouvelle technologie qui garantit une connexion sûre à cent pour cent entre les systèmes de données sans aucune possibilité de piratage. C'est une sorte de circulation à sens unique sûre et garantie, dans laquelle les pirates informatiques ne peuvent pas s'introduire. Il s'agit de réseaux unidirectionnels, en anglais '*unidirectional gateways'*. Ces réseaux transfèrent les données sans donner accès aux systèmes qui génèrent ces données. Il est matériellement impossible d'envoyer des données dans l'autre sens. Ce système permet d'éviter une partie significative des cyberattaques.

Le *US National Institute of Standards and Technology (*NIST) définit les réseaux unidirectionnels comme suit: "*Unidirectional gateways are a combination of hardware and software. The hardware permits data to flow from one network to another but is physically unable to send any information at all back into the source network. […] The guide positions unidirectional gateways as stronger than firewall protection for sensitive industrial control system networks*."

Le noyau d'un réseau unidirectionnel est constitué de hardware. C'est lui qui impose l'unidirectionnalité matérielle. Le flux d'informations ne circule que dans un seul sens. Les données (par exemple, les mesures comme la température et d'autres paramètres) peuvent être transférées d'un réseau à l'autre, mais le réseau émetteur est protégé contre les attaques venant de l'extérieur. L'émergence de l'Internet des Objets (IdO) et la numérisation amènent les entreprises à utiliser de plus en plus souvent des réseaux unidirectionnels pour protéger leurs systèmes de contrôle et de sécurité. Les normes et les réglementations industrielles évoluent, intègrent cette alternative aux pare-feu et encouragent ou imposent son utilisation.

Cette technique de sécurisation s'applique dans un nombre croissant de secteurs industriels. Tous les générateurs nucléaires américains l'utilisent aujourd'hui, de même que les installations nucléaires situées en Israël, au Canada, en Espagne et en Corée du Sud. La technologie s'impose également dans une série d'autres secteurs comme les raffineries, les entreprises chimiques, les stations d'épuration d'eau, les installations pétrolières et gazières (les plateformes de production et les pipelines), … En cas de cyberattaque, tous ces secteurs constituent une menace qui pourrait bien faire un grand nombre de victimes. La nouvelle technologie est utilisée dans un grand nombre d'infrastructures critiques.

Les avis, les normes et les régulations modernes contiennent des recommandations ou des obligations d'utiliser des réseaux unidirectionnels pour les réseaux de commande critiques. S'ils sont utilisés comme seule

Er bestaat vandaag nieuwe technologie die een honderd procent veilige verbinding tussen datasystemen garandeert zonder de kans dat het wordt gehackt. Een soort gegarandeerd veilig eenrichtingsverkeer waar hackers niet op kunnen inbreken. Het gaat om '*unidirectional gateways*'. Die verplaatsten de data zonder toegang te geven tot de systemen die de data genereren. Het is fysiek onmogelijk om data de andere kant in te sturen. Daarmee kunnen we een significant deel van de cyberaanvallen vermijden.

De *US National Institute of Standards and Technology* (NIST) definieert *unidirectional gateway* als: "*Unidirectional gateways are a combination of hardware and software. The hardware permits data to flow from one network to another but is physically unable to send any information at all back into the source network. […] The guide positions unidirectional gateways as stronger than firewall protection for sensitive industrial control system networks*."

De kern van een unidirectioneel netwerk is hardware. Die dwingt de fysieke unidirectionaliteit af. De informatiestroom gaat slechts in één richting. Data kunnen worden getransfereerd (bijvoorbeeld metingen zoals temperatuur en andere parameters), van het ene netwerk naar het andere, maar het verzendende netwerk wordt beschermd tegen aanvallen van buitenaf. Met de opkomst van het *Internet of Things* (IoT) en digitalisering wordt door bedrijven steeds vaker gebruikgemaakt van unidirectionele netwerken om hun controle- en veiligheidssystemen te beschermen. Industriële standaarden en reglementeringen evolueren en nemen dit alternatief voor firewalls op en moedigen het gebruik ervan aan of leggen het op.

Deze beveiligingstechniek vindt toepassing in steeds meer industriële sectoren. Alle Amerikaanse nucleaire generatoren maker er vandaag al gebruik van, net zoals nucleaire installaties in Israël, Canada, Spanje en Zuid-Korea. De technologie vindt ook ingang in een reeks andere sectoren zoals raffinaderijen, chemische bedrijven, waterzuiveringsinstallaties, olie- en gasinstallaties (productieplatformen en pijpleidingen), … Al deze sectoren vormen bij een cyberaanval een bedreiging waarbij wel eens veel slachtoffers zouden kunnen vallen. In heel wat kritieke infrastructuren wordt van de nieuwe technologie gebruikgemaakt.

Modern advies, standaarden en reguleringen bevatten aanbevelingen of verplichtingen om unidirectionele netwerken te gebruiken voor besturingskritieke netwerken. Indien die worden ingezet als de enige connectie tussen

connexion entre les réseaux de contrôle critiques et les réseaux critiques pour les entreprises, ces réseaux unidirectionnels éliminent totalement les possibilités d'attaques en ligne. Les sites protégés par une technologie unidirectionnelle sont complètement sécurisés contre les rançongiciels ciblés, les services de renseignement étatiques et d'autres acteurs de la menace en ligne, quel que soit leur degré d'équipement ou de sophistication. Ces sites bénéficient également d'un accès aux données industrielles nécessaires pour permettre une automatisation moderne des entreprises. Les réseaux unidirectionnels offrent aux systèmes de contrôle, aux infrastructures (industrielles) critiques et aux réseaux technologiques opérationnels (réseaux OT) la plus forte protection.

Certains pays ont déjà adopté une législation et des directives intégrant les réseaux unidirectionnels. C'est le cas des États-Unis au travers de la *US Nuclear Regulatory Commission 5.71 regulation (US NRC 5.71), du US Nuclear Energy Institute 08-09 (US NEI 08-09) et de la North American Electric Reliability Corporations Critical Infrastructure Protection (NERC CIP).* Aux États-Unis, tous les réacteurs nucléaires sont protégés grâce à cette technologie, de même que de nombreuses infrastructures critiques. On citera comme autres pays Israël ((*Israel's Cyber Manual, Israeli Critical Infrastructure*), Singapour (*Singaporean Critical Infrastructure*) et la Corée du Sud (*South Korean Critical Infrastructure*). Plus près de nous, on citera la France (*Agence nationale de la sécurité des systèmes d'information (ANSSI) - Industrial Control Systems*) et le Royaume-Uni (*Rail Cybersecurity - Guidance to Industry*).

Les études montrent que le nombre d'attaques perpétrées contre des infrastructures critiques est en hausse et que ces attaques deviennent de plus en plus sophistiquées. Les pirates informatiques ciblent des installations liées à l'énergie, à internet, à l'eau potable, aux transactions financières et aux services de transport essentiels. La pression sur les infrastructures critiques, dont font partie les installations nucléaires, s'accroît donc. Certaines de ces attaques sont très probablement soutenues par des services étrangers. L'avertissement est donc clair: la menace d'attaque contre les infrastructures critiques, y compris les installations nucléaires, est en progression.

Il importe à nos yeux d'accroître la résilience de nos intérêts vitaux et de nos infrastructures. Nous devons prendre des mesures supplémentaires adaptées aux nouvelles menaces et aux nouveaux risques. Nous préconisons la mise en œuvre de mesures préventives pour mieux nous protéger contre les cybermenaces et les cyberincidents, afin que tout accès non autorisé devienne impossible. Nous entendons dès lors rendre obligatoire l'utilisation de réseaux unidirectionnels qui élimineront

controlekritieke en bedrijfskritische netwerken, elimineren zij volledig de mogelijkheden van onlineaanvallen. Unidirectioneel beschermde sites genieten volledige beveiliging tegen gerichte ransomware, statelijke inlichtingendiensten en andere onlinedreigingsactoren, ongeacht hoe goed uitgerust en gesofisticeerd deze actoren zijn. Die sites genieten eveneens toegang tot de industriële data die noodzakelijk zijn om moderne bedrijfsautomatisering mogelijk te maken. Unidirectionale netwerken bieden de sterkste bescherming voor controlesystemen, kritieke (industriële) infrastructuur en operationele technologische netwetwerken (OT-netwerken).

In een aantal landen werd al wetgeving en richtlijnen aangenomen waarin unidirectionele netwerken zijn opgenomen. Dat is het geval in de Verenigde Staten met de *US Nuclear Regulatory Commission 5.71 regulation (US NRC 5.71), US Nuclear Energy Institute 08-09 (US NEI 08-09) en de North American Electric Reliability Corporations Critical Infrastructure Protection (NERC CIP).* Alle nucleaire reactoren in de Verenigde Staten zijn met deze technologie beschermd, net zoals veel kritieke infrastructuren. Andere landen zijn Israël (*Israel's Cyber Manual, Israeli Critical Infrastructure*), Singapore (*Singaporean Critical Infrastructure*) en Zuid-Korea (*South Korean Critical Infrastructure*). Dichterbij hebben we Frankrijk (*Agence nationale de la sécurité des systèmes d'information (ANSSI) Industrial Control Systems*) en het Verenigd Koninkrijk (*Rail Cybersecurity - Guidance to Industry*).

Uit onderzoeken blijkt dat het aantal aanvallen op kritieke infrastructuren toeneemt en steeds geavanceerder wordt. Hackers richten hun aanvallen op voorzieningen zoals de energie, het internet, het drinkwater, het betalingsverkeer en de essentiële transportdiensten. De druk op kritieke infrastructuren waar nucleaire installaties bij horen, neemt dus toe. Een deel van de aanvallen wordt hoogstwaarschijnlijk door buitenlandse diensten gesteund. Daarom wordt gewaarschuwd voor het feit dat de aanvalsdreiging voor kritieke infrastructuren, met inbegrip van nucleaire installaties, groter wordt.

Wij zijn van mening dat de weerbaarheid van onze vitale belangen en infrastructuur moet vergroten. We moeten bijkomende maatregelen nemen in functie van de nieuwe dreigingen en risico's. Wij pleiten voor de implementatie van preventieve maatregelen om ons beter te beschermen tegen cyberdreigingen en -incidenten zodat ongeautoriseerde toegang onmogelijk wordt. Daarom willen wij het gebruik van unidirectionele netwerken die de mogelijkheden van onlinecyberaanvallen drastisch

radicalement, voire complètement, les possibilités de cyberattaques en ligne. Nous devons utiliser la nouvelle technique de protection des *unidirectional gateways* ou réseaux unidirectionnels dans les infrastructures critiques où des incidents peuvent gravement déstabiliser la société et faire un très grand nombre de victimes, ce que l'on appelle des *Mass Casualty Incidents* (MCI).

Les secteurs auxquels s'appliquera la loi sont les installations de production d'énergie (centrales à hydrogène, centrales hydroélectriques, centrales à gaz, centrales nucléaires et autres centrales et turbines), les barrages, les centrales d'eau potable, les raffineries, les usines chimiques, les installations de traitement des eaux et les installations de pétrole et de gaz. Le Roi peut compléter cette liste.

La loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques[2]

L'article 13, § 1er, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques impose aux exploitants d'infrastructures critiques l'élaboration d'un plan de sécurité (plan de sécurité de l'exploitant, ci-après: "P.S.E."), visant à prévenir, à atténuer et à neutraliser les risques d'interruption du fonctionnement ou de destruction de l'infrastructure critique par la mise au point de mesures matérielles et organisationnelles internes. Ce plan contient au moins les mesures internes de sécurité permanentes devant être appliquées en toutes circonstances et des mesures internes de sécurité graduelles à appliquer en fonction de la menace (article 13, § 2, de la même loi). Les exploitants sont également tenus d'organiser des exercices et d'actualiser le P.S.E., en fonction des enseignements des exercices ou de toute modification de l'analyse des risques (article 13, § 6, de la même loi).

La loi n'impose toutefois pas l'utilisation de réseaux unidirectionnels. La présente proposition de loi entend y remédier. À cette fin, elle insère dans la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques l'obligation d'utiliser cette nouvelle technique de protection. L'article 13 de la loi est complété par un paragraphe instaurant cette obligation, qui s'applique uniquement aux infrastructures critiques dans lesquelles des incidents peuvent gravement déstabiliser la société et faire un très grand nombre de victimes, ce que l'on appelle des *Mass Casualty Incidents* (MCI).

[2] Loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, publiée au *Moniteur belge* le 15 juillet 2011.

tot volledig doen verdwijnen, verplichten. We moeten gebruikmaken van de nieuwe beschermingstechniek van *unidirectional gateways* of unidirectionele netwerken bij kritieke infrastructuren waar incidenten ernstige maatschappelijke ontwrichtingen kunnen veroorzaken en waarbij een massa slachtoffers kunnen vallen, de zogenaamde *Mass Casualty Incidents* (MCIs).

Sectoren waarop deze wet toepassing zal hebben zijn energieproducerende installaties (waterstofcentrales, waterkrachtcentrales, gascentrales, nucleaire centrales en andere centrales en turbines), waterdammen, drinkwatercentrales, raffinaderijen, chemische bedrijven, waterzuiveringsinstallaties en olie- en gasinstallaties. De Koning kan deze lijst verder aanvullen.

De wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren[2]

Volgens artikel 13, § 1, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren zijn de exploitanten van kritieke infrastructuren verplicht om een beveiligingsplan (een beveiligingsplan van de exploitant (hierna: "B.P.E.")) uit te werken met het oog op het voorkomen, beperken en neutraliseren van de risico's op verstoring van de werking of van de vernietiging van de kritieke infrastructuur door het op punt stellen van interne materiële en organisatorische maatregelen. Dit plan bevat minstens de permanente interne beveiligingsmaatregelen, die moeten worden toegepast in alle omstandigheden en de graduele interne beveiligingsmaatregelen, toe te passen in functie van de dreiging (artikel 13, § 2 van dezelfde wet). De exploitanten zijn eveneens verantwoordelijk voor het organiseren van oefeningen en het actualiseren van het B.P.E., in functie van de lessen getrokken uit de oefeningen of uit elke wijziging van de risicoanalyse (artikel 13, § 6 van dezelfde wet).

In de wet is echter geen verplichting opgenomen om gebruik te maken van *unidirectional gateways* of unidirectioneel netwerken. Met dit wetsvoorstel willen wij daar verandering in brengen. Daartoe wordt in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren de verplichting opgenomen om van deze nieuwe beschermingstechniek gebruik te maken. Artikel 13 van de wet wordt aangevuld met een nieuwe paragraaf die deze verplichting invoert. De verplichting geldt enkel voor kritieke infrastructuren waar incidenten ernstige maatschappelijke ontwrichtingen kunnen veroorzaken en massaal veel slachtoffers kunnen maken, de zogenaamde *Mass Casualty Incidents* (MCIs).

[2] Wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, bekendgemaakt in het *Belgisch Staatsblad* op 15 juli 2011.

COMMENTAIRE DES ARTICLES

Article 2

L'absence d'obligation d'utiliser des réseaux unidirectionnels est une lacune qu'il convient de combler dans la loi actuelle. C'est pourquoi l'article 13 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques est complété par un § 8 qui impose cette obligation.

Cette obligation n'est imposée qu'aux infrastructures critiques dans lesquelles des incidents peuvent gravement déstabiliser la société et faire un très grand nombre de victimes. Il s'agit au minimum des installations de production d'énergie (centrales à hydrogène, centrales hydroélectriques, centrales à gaz, centrales nucléaires et autres centrales et turbines), des barrages, des centrales d'eau potable, des raffineries, des usines chimiques, des installations de traitement des eaux et des installations de pétrole et de gaz. Le Roi peut éventuellement compléter cette liste.

Art. 3

Cet article fixe la date d'entrée en vigueur de la loi. Un délai de dix-huit mois est accordé aux opérateurs concernés pour mettre en œuvre la nouvelle technique de protection.

TOELICHTING BIJ DE ARTIKELEN

Artikel 2

Het ontbreken van de verplichting om gebruik te maken van *unidirectional gateways* of unidirectionele netwerken is een lacune in de huidige wet die moet worden ingevuld. Daartoe wordt artikel 13 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren aangevuld met een nieuwe paragraaf 8 die deze verplichting oplegt.

Deze verplichting wordt enkel opgelegd aan kritieke infrastructuren waar incidenten ernstige maatschappelijke ontwrichtingen kunnen veroorzaken en massaal veel slachtoffers kunnen maken. Het gaat dan minstens over de energieproducerende installaties (nucleaire centrales, waterstofcentrales, waterkrachtcentrales, gascentrales), de waterdammen, de drinkwatercentrales, de raffinaderijen, de chemische bedrijven, de waterzuiveringsinstallaties en de olie- en gasinstallaties. De Koning kan deze lijst eventueel verder aanvullen.

Art. 3

Dit artikel bepaalt de datum van inwerkingtreding van de wet. De betrokken operatoren krijgen achttien maanden tijd om de nieuwe beveiligingstechniek te implementeren.

Michael FREILICH (N-VA)
Theo FRANCKEN (N-VA)
Sander LOONES (N-VA)
Wim VAN der DONCKT (N-VA)
Joy DONNÉ (N-VA)
Björn ANSEEUW (N-VA)
Frieda GIJBELS (N-VA)
Anneleen VAN BOSSUYT (N-VA)
Darya SAFAI (N-VA)

PROPOSITION DE LOI

Article 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2

L'article 13 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, modifié en dernier lieu par la loi du 8 mai 2019, est complété par un paragraphe 8 rédigé comme suit:

"§ 8. Pour les installations qui produisent de l'énergie, les barrages, les stations de production d'eau potable, les raffineries, les entreprises chimiques, les stations d'épuration et les installations pétrolières et gazières, l'utilisation de réseaux unidirectionnels est obligatoire.

Le Roi peut compléter cette liste."

Art. 3

La présente loi entre en vigueur le premier jour du dix-huitième mois qui suit celui de sa publication au *Moniteur belge.*

22 mars 2022

WETSVOORSTEL

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2

Artikel 13 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, laatstelijk gewijzigd bij de wet van 8 mei 2019, wordt aangevuld met een paragraaf 8 luidende:

"§ 8. Voor energieproducerende installaties, waterdammen, drinkwatercentrales, raffinaderijen, chemische bedrijven, waterzuiveringsinstallaties en olie- en gasinstallaties is het gebruik van unidirectionele netwerken verplicht.

De Koning kan deze lijst verder aanvullen."

Art. 3

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

22 maart 2022

Michael FREILICH (N-VA)
Theo FRANCKEN (N-VA)
Sander LOONES (N-VA)
Wim VAN der DONCKT (N-VA)
Joy DONNÉ (N-VA)
Björn ANSEEUW (N-VA)
Frieda GIJBELS (N-VA)
Anneleen VAN BOSSUYT (N-VA)
Darya SAFAI (N-VA)

Imprimerie centrale – Centrale drukkerij