DOC 56 **0196/001**

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

BUITENGEWONE ZITTING 2024

6 september 2024

VOORSTEL VAN RESOLUTIE

betreffende de bevordering van een performanter cybersecuritybeleid ter ondersteuning van onze bedrijven en organisaties in de strijd tegen cybercrime

(ingediend door de heer Steven Matheï en mevrouw Leentje Grillaert)

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

SESSION EXTRAORDINAIRE 2024

6 septembre 2024

PROPOSITION DE RÉSOLUTION

visant à promouvoir une politique de cybersécurité plus performante pour soutenir nos entreprises et nos organisations dans la lutte contre la cybercriminalité

(déposée par M. Steven Matheï et Mme Leentje Grillaert)

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

Abréviations dans la numérotation des publications:		*Afkorting bij de nummering van de publicaties:*	
DOC 56 0000/000	*Document de la 56e législature, suivi du numéro de base et numéro de suivi*	*DOC 56 0000/000*	*Parlementair document van de 56e 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)*

TOELICHTING

DAMES EN HEREN,

Dit voorstel neemt de tekst over van het voorstel DOC 55 2771/001.

Inleiding

Meer en meer bedrijven in ons land worden het slachtoffer van een cyberaanval. Dit voorstel van resolutie doet een aantal aanbeveling aan de overheden in ons land die kunnen bijdragen tot een betere bescherming van onze bedrijven en organisaties tegen cyberaanvallen.

Wat is cybersecurity?

Hoe verder onze leefwereld digitaliseert, hoe groter het belang van een degelijk cybersecuritybeleid. Uit onderzoek blijkt immers dat de internetinfrastructuur van een land steeds vaker een doelwit is bij internationale conflicten. Daarnaast liggen geopolitieke motieven meer en meer aan de basis van een cyberaanval, terwijl vroeger vooral financiële motieven verscholen gingen achter een cyberaanval.[1] De cyberdreigingen en -aanvallen zouden volgens het federaal cybersecurityplan ook steeds geavanceerder worden. Hierdoor is de schade vaak groter en ook moeilijker te herstellen. Het *Computer Emergency Response Team* (CERT), de operationele dienst van het *Center for Cybersecurity Belgium* (CCB)[2] dat instaat voor de registratie van het aantal cyberaanvallen, registreerde in 2018 1.600 meldingen. In 2019 waren er dit al 4.484. In 2020 liep het aantal meldingen op tot 7.433. Vermoedelijk ligt het aantal aanvallen in de realiteit nog hoger aangezien er op dit moment voor veel bedrijven geen meldingsplicht bestaat.

Met deze informatie in het achterhoofd kunnen we ons als land maar beter wapenen tegen dat wat onvermijdelijk lijkt: meer cyberaanvallen die gesofisticeerder zijn. Om hier tegen bestand te zijn, is een gedegen cybersecuritybeleid een absolute noodzaak. *In casu* is een zeer belangrijke rol weggelegd voor de verschillende overheden. Cybersecurity is immers iets wat ons allen aanbelangt. De gevolgen van een cyberaanval houden zelden op bij de poorten van het bedrijf of de organisatie die werd aangevallen.

1 *Cybersecurity strategie België 2.0,* Centre For Cybersecurity Belgium, 2021.
2 *Cybersecurity strategie België 2.0,* Centre For Cybersecurity Belgium, 2021.

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

La présente proposition reprend le texte de la proposition DOC 55 2771/001.

Introduction

De plus en plus d'entreprises sont victimes de cyberattaques dans notre pays. La présente proposition de résolution adresse aux autorités de notre pays plusieurs recommandations susceptibles de contribuer à une meilleure protection de nos entreprises et de nos organisations contre les cyberattaques.

En quoi la cybersécurité consiste-t-elle?

Plus notre monde se numérise, plus il importe de disposer d'une bonne politique de cybersécurité. En effet, des études indiquent qu'en cas de conflit international, l'infrastructure internet des pays est de plus en plus souvent visée. Les cyberattaques, qui étaient autrefois principalement liées à des motifs d'ordre financier, trouvent par ailleurs de plus en plus souvent leurs origines dans des considérations géopolitiques.[1] Selon le cyberplan fédéral, les cybermenaces et les cyberattaques seraient également de plus en plus sophistiquées. Leurs dommages seraient donc souvent plus importants et plus difficiles à réparer. La *Computer Emergency Response Team* (CERT) – le service opérationnel du Centre pour la Cybersécurité Belgique (CCB)[2] chargé de répertorier le nombre de cyberattaques – a enregistré 1.600 signalements en 2018, 4.484 signalements en 2019 et 7.433 signalements en 2020. Le nombre d'attaques réelles est sans doute encore plus élevé, car beaucoup d'entreprises ne sont pas soumises à l'obligation de notification.

Compte tenu de ce qui précède, il s'indiquerait que la Belgique s'arme contre ce qui semble inévitable: des cyberattaques plus nombreuses et plus sophistiquées. Pour pouvoir y faire face, une politique de cybersécurité solide sera une nécessité absolue. Les différents niveaux de pouvoir ont un rôle très important à jouer à cet égard. En effet, la cybersécurité nous concerne tous, car les conséquences des cyberattaques s'arrêtent rarement aux portes de l'entreprise ou de l'organisation attaquée.

1 *Stratégie cybersécurité Belgique 2.0,* Centre pour la Cybersécurité Belgique, 2021.
2 *Stratégie cybersécurité Belgique 2.0,* Centre pour la Cybersécurité Belgique, 2021.

Het fenomeen cyberdreiging wordt door het Centrum voor Cybersecurity in België als volgt omschreven: acties die de integriteit, de beschikbaarheid en de vertrouwelijkheid van informatie bedreigen. Het hoeft geen betoog dat dit een uiterst ruim begrip is. Dit is ook niet vreemd aangezien cybersecurity zowat elk aspect van onze digitaliseerde samenleving aangaat.

Ondanks dit algemene karakter zijn er *grosso modo* vier doelgroepen te bepalen bij een cybersecuritybeleid:

— bedrijven;

— overheden;

— organisaties van vitaal belang;

— consumenten.

Dit voorstel van resolutie focust voornamelijk op de bedrijven en in mindere mate op de organisaties van vitaal belang. Toch werd er geopteerd om beide doelgroepen te behandelen aangezien er zich onder de aanbieders van essentiële diensten ook heel wat bedrijven bevinden. In de NIS-richtlijn[3] definieert de Europese Unie de essentiële diensten namelijk als bedrijven of organisaties die actief zijn in energie, transport, financiën of gezondheidszorg. Ook onlinemarktplaatsen, onlinezoekmachines of cloudcomputerdiensten vallen onder het toepassingsgebied van deze richtlijn. Dat neemt niet weg dat dit voorstel van resolutie niet volledig los gezien kan worden van de overheden en de consumenten.[4] De focus van de verzoeken van dit voorstel van resolutie ligt echter op initiatieven die de overheid kan nemen om bedrijven en organisaties beter te ondersteunen bij hun cybersecuritybeleid.

Met bovenstaande informatie in het achterhoofd lijkt het dus alsof er heel wat bedreigingen op ons afkomen. Het goede nieuws is wel dat er veel startende initiatieven zijn in ons land en in de Europese Unie. Zij zetten de bakens uit voor een degelijk cybersecuritybeleid. Dit voorstel van resolutie overloopt achtereenvolgens de rol die de bedrijven zelf kunnen spelen. Vervolgens worden de bestaande initiatieven op Europees en Belgisch

Le Centre pour la Cybersécurité Belgique définit la cybermenace comme étant une série d'actions qui menacent l'intégrité, la disponibilité et la confidentialité des informations. Il va sans dire qu'il s'agit d'un concept extrêmement vaste, ce qui n'a rien d'étonnant dès lors que la cybersécurité s'étend à pratiquement tous les aspects de notre société numérisée.

Malgré ce caractère général, on peut *grosso modo* distinguer quatre groupes cibles dans les politiques de cybersécurité:

— les entreprises;

— les pouvoirs publics;

— les organisations d'intérêt vital;

— les consommateurs.

La présente proposition de résolution vise principalement les entreprises et, dans une moindre mesure, les organisations d'intérêt vital. Il a toutefois été décidé de la faire porter sur ces deux groupes cibles, car de nombreuses entreprises se retrouvent également parmi les opérateurs de services essentiels. La directive européenne SRI[3] définit en effet les opérateurs de services essentiels comme des entreprises ou des organisations actives dans les domaines de l'énergie, des transports, de la finance ou des soins de santé. Les places de marché en ligne, les moteurs de recherche en ligne ou les services d'informatique en nuage entrent également dans le champ d'application de cette directive. La présente proposition de résolution ne peut cependant pas être entièrement dissociée des groupes cibles des pouvoirs publics et des consommateurs.[4] Son dispositif se concentre néanmoins sur les initiatives qui pourraient être prises par les pouvoirs publics pour mieux soutenir les entreprises et les organisations dans leurs politiques de cybersécurité.

Eu égard à ce qui précède, il semble que de nombreuses menaces pèsent sur nous. Mais beaucoup d'initiatives ont heureusement été lancées en la matière dans notre pays et dans l'Union européenne. Celles-ci préparent le terrain pour une politique de cybersécurité efficace. La présente proposition de résolution examine d'abord le rôle que les entreprises peuvent jouer. Elle commente ensuite les initiatives prises aux niveaux européen

[3] NIS-richtlijn (*Network and Information Security*) – richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van network- en informatiesystemen in de Unie, bekendgemaakt in het *Publicatieblad van de Europese Unie* op 19 juli 2016, L 194/1.

[4] *Cybersecurity strategie België 2.0,* Centre For Cybersecurity Belgium, 2021.

[3] Directive SRI (sécurité des réseaux et des systèmes d'information) – Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, publiée au *Journal officiel de l'Union européenne* le 19 juillet 2016, L 194/1.

[4] *Stratégie cybersécurité Belgique 2.0,* Centre pour la Cybersécurité Belgique, 2021.

niveau toegelicht. Tot slot worden de tekortkomingen van het huidige beleid opgesomd. Afsluitend wordt er een aantal potentiële oplossingen aangereikt.

Wat kan een bedrijf doen?

Veel bedrijven worden jammer genoeg geconfronteerd met een cyberaanval. Door de toegenomen dreiging, gaat een aantal, vooral grotere, bedrijven over tot de uitbouw van een echt cybersecuritybeleid.[5] Binnen de uitbouw van een cyberbeleid is het belangrijk dat er wordt rekening gehouden met de realiteit van elke onderneming. Zo kan men er niet vanuit gaan dat elk bedrijf over dezelfde kennis en middelen beschikt om zo'n beleid te voeren. De overheid mag in deze zeker niet vervallen in een uniform kader waarbinnen elk bedrijf moet passen. Er moet voldoende aandacht zijn voor de individuele situatie van elke organisatie. Zo moet er binnen de Belgische context voldoende rekening gehouden worden met de situatie van kmo's. Het gros van onze ondernemingen is namelijk een kmo. Uit de cijfergegevens blijkt dat ook kmo's de dans niet ontspringen. 43 % van de bewuste aanvallen werden uitgevoerd op kleine bedrijven.[6] Uit een gids die het Verbond van Belgische Ondernemingen (VBO) publiceerde rond een cyberbeleid voor kleine en grote organisaties, valt op te maken dat er op bedrijfsniveau al heel wat initiatieven kunnen genomen worden voor een betere beveiliging tegen een cyberaanval.

Volgens het Centrum voor Cybersecurity zijn onze bedrijven goed in de toepassing van nieuwe technologieën. De beveiliging daarvan laat soms echter te wensen over.[7] Zo zijn bedrijven erg goed in de beveiliging van de materiële vaste activa maar niet in de beveiliging van hun data.[8] Nochtans zijn dit vandaag vaak de belangrijkste activa.[9] Een gebrekkige beveiliging van de gegevens van een bedrijf kan namelijk een enorme impact hebben op de reputatie van die onderneming. Verder is het een misvatting dat cybersecurity enkel een verantwoordelijkheid is van de IT-afdeling.[10] Zij moeten inderdaad instaan voor een performant softwarepakket dat digitaal correct beveiligd is. Wanneer er met een nieuwe software- of hardwareleveranciers wordt samengewerkt, is het de taak van de IT-afdeling om te bekijken hoe deze partners scoren op het vlak van beveiliging.

5 *Belgische gids voor cyberveiligheid*, ICCBELGIUM, sd.
6 *Organizational science and cybersecurity: abundant opportunities for research at the interface,* Reeshad Dalal; David Howard, Journal of business and psychology, 2021, p. 1-29.
7 *Cybersecurity strategie België 2.0,* Centre For Cybersecurity Belgium, 2021.
8 *Belgische gids voor cyberveiligheid*, ICCBELGIUM, sd.
9 *Belgische gids voor cyberveiligheid*, ICCBELGIUM, sd.
10 IT: *information technology*.

et belge. Elle énumère enfin les lacunes de la politique actuelle et propose, en conclusion, un certain nombre de solutions potentielles.

Que peuvent faire les entreprises?

Beaucoup d'entreprises sont malheureusement confrontées à des cyberattaques. En raison de la menace accrue, certaines d'entre elles, surtout les plus grandes, développent une véritable politique de cybersécurité.[5] Lorsqu'on élabore une politique de ce type, il est important de tenir compte de la réalité de chaque entreprise. Ainsi, il ne faut pas partir du principe que chaque entreprise dispose des mêmes connaissances et des mêmes ressources. Les autorités doivent se garder d'élaborer un cadre uniforme pour l'ensemble des entreprises. Il est important d'accorder une attention suffisante à la situation individuelle de chaque organisation. Ainsi, dans le contexte belge, il convient de tenir compte de la situation des PME – qui représentent la majorité de nos entreprises. Les chiffres montrent que les PME sont, elles aussi, confrontées à ce phénomène. Quarante-trois pour cent des attaques en question ont été menées contre des entreprises de petite taille.[6] Un guide de la Fédération des entreprises de Belgique (FEB) consacré à la cyberpolitique pour les petites et grandes organisations explique que de nombreuses initiatives peuvent déjà être prises au niveau de l'entreprise pour améliorer la sécurité contre les cyberattaques.

D'après le Centre pour la Cybersécurité, nos entreprises appliquent correctement les nouvelles technologies, mais la sécurité de celles-ci laisse parfois à désirer.[7] Ainsi, les entreprises sont très performantes dans la sécurisation de leurs immobilisations corporelles, mais pas dans celle de leurs données[8] – alors que celles-ci constituent souvent à l'heure actuelle les actifs les plus importants.[9] Une sécurisation défaillante des données d'une entreprise peut avoir un impact considérable sur sa réputation. Par ailleurs, il est erroné de penser que la cybersécurité relève uniquement de la responsabilité du département IT (département informatique).[10] Celui-ci doit effectivement veiller à ce que l'entreprise dispose de logiciels performants et correctement sécurisés. Lorsqu'une collaboration est mise en place avec de nouveaux fournisseurs de logiciels ou de matériel, il incombe aussi au département IT d'examiner les performances de ces partenaires dans le domaine de la sécurité.

5 *Guide belge de la cybersécurité*, ICCBELGIUM, sd.
6 *Organizational science and cybersecurity: abundant opportunities for research at the interface,* Reeshad Dalal; David Howard, Journal of business and psychology, 2021, p. 1-29.
7 *Stratégie cybersécurité Belgique 2.0,* Centre pour la Cybersécurité Belgique, 2021.
8 *Guide belge de la cybersécurité*, ICCBELGIUM, sd.
9 *Guide belge de la cybersécurité*, ICCBELGIUM, sd.
10 IT: *information technology*.

Maar een systeem mag technologisch nog zo goed beveiligd zijn, het neemt geenszins het risico op een succesvolle cyberaanval weg. Uit onderzoek blijkt immers dat 35 % van de veiligheidsincidenten werd veroorzaakt door een menselijke fout. Daarnaast zou 65 % van de cyberaanvallen vermeden kunnen worden als er op een veiligere manier met het softwaresysteem was omgegaan door de gebruikers van het systeem.[11]

Om die reden is er een uiterst brede benadering van cybersecurity nodig. Het moet een prioriteit zijn op alle bedrijfsniveaus. Het is daarbij belangrijk dat er een volwaardig cybersecuritybeleid wordt uitgetekend op bedrijfsniveau. Nu beperken deze plannen zich volgens het VBO nog te vaak tot een "checklistbeleid". Hierbij worden enkel de voorgeschreven vakjes afgevinkt zonder dat er sprake is van een coherent beleid. Binnen zo'n beleid is er onder andere nood aan concentratie. Niet alle data die het bedrijf bezit, zijn namelijk even belangrijk. Verder is het zo dat meer moet ingezet worden op het menselijke aspect van cybersecurity. Zoals eerder aangegeven, worden heel veel incidenten veroorzaakt door een menselijke fout. Ook de cybercriminelen zijn zich bewust van deze zwakte. Om die reden wordt er meer en meer gebruikgemaakt van social engineering. Hierbij worden mensen gemanipuleerd zodat ze gevoelige info vrijgeven.[12] Preventie en opleiding van werknemers zijn van primordiaal belang om een bedrijf te wapenen tegen cyberaanvallen die gebruikmaken van social engineering. Een gedegen cybersecuritybeleid is namelijk een keten met vele schakels. De keten is echter maar zo sterk als de zwakste schakel. Daarom is het niet alleen van belang dat de software en gebruikte hardware goed beveiligd zijn, ook de mensen die met deze infrastructuur werken, moeten betrokken zijn bij het cybersecuritybeleid van een bedrijf of een organisatie.

Rol van de overheid?

Door toegenomen onlineactiviteiten en een verhoogd risico voor burgers organisaties en de overheid wordt cybersecurity meer en meer een belangrijke politiek thema. Om die reden moeten we bekijken welke aspecten van cybersecurity we moeten behandelen als een publiek goed. Dit is een moeilijke oefening aangezien vele toepassingen voor cybersecurity volledig door de private sector zijn gecreëerd. Het gegeven dat er in de technologie sprake is van een sterke machtsconcentratie bij een aantal multinationals maakt het plaatje alleen maar complexer. Ook de EU is bezorgd over de falende marktwerking voor cybersecurity. Indien er enkel oplossingen worden aangeboden die economisch rendabel zijn,

11 *Belgische gids voor cyberveiligheid*, ICCBELGIUM, sd.
12 *Belgische gids voor cyberveiligheid*, ICCBELGIUM, sd.

Mais aussi sécurisé soit-il technologiquement parlant, aucun système ne sera jamais à l'abri d'une cyberattaque. En effet, il ressort d'une étude que 35 % des incidents liés à la sécurité sont imputables à une erreur humaine. En outre, 65 % des cyberattaques auraient pu être évitées si les utilisateurs du système avaient utilisé le système logiciel de manière plus sûre.[11]

C'est la raison pour laquelle il convient d'adopter une approche de la cybersécurité extrêmement large et d'en faire une priorité à tous les niveaux de l'entreprise. À cet égard, il est important qu'une véritable politique de cybersécurité soit déployée à l'échelle de l'entreprise. Aujourd'hui, ces projets se limitent encore trop souvent, selon la FEB, à une "politique de listes de contrôle" consistant à ne cocher que les cases prescrites sans qu'il soit question de politique cohérente. Pareille politique exige notamment de la concentration. En effet, toutes les données de l'entreprise n'ont pas le même degré d'importance. En outre, force est d'admettre qu'il faut se concentrer davantage sur l'aspect humain de la cybersécurité. Ainsi qu'il a déjà été indiqué, très nombreux sont les incidents provoqués par une erreur humaine, une faiblesse que les cybercriminels ont, eux aussi, parfaitement intégrée. C'est pourquoi l'ingénierie sociale est de plus en plus utilisée. Celle-ci consiste à manipuler les gens afin qu'ils divulguent des informations sensibles.[12] La prévention et la formation des travailleurs revêtent une importance cruciale pour armer une entreprise contre les cyberattaques utilisant l'ingénierie sociale. En effet, une politique de cybersécurité de qualité est une chaîne composée de nombreux maillons, mais dont la solidité n'excède pas celle de son maillon le plus faible. Il faut donc à la fois disposer de logiciels et de matériel correctement sécurisés et impliquer le personnel utilisant l'infrastructure dans la cybersécurité d'une entreprise ou d'une organisation.

Quel rôle attribuer aux pouvoirs publics?

En raison de l'augmentation des activités en ligne et du risque accru pour les citoyens, les organisations et les pouvoirs publics, la cybersécurité s'impose de plus en plus comme un thème politique majeur. C'est pourquoi nous devons examiner quels aspects de la cybersécurité nous devons traiter comme un bien public. Sachant que de nombreuses applications de cybersécurité ont été intégralement créées par le secteur privé, l'exercice est ardu. Et le fait que la technologie se caractérise par une forte concentration de pouvoir au sein de quelques multinationales complique encore les choses. L'Union européenne se dit également préoccupée par la défaillance du fonctionnement du marché de la cybersécurité. Si l'on

11 *Guide belge de la cybersécurité*, ICCBELGIUM, sd.
12 *Guide belge de la cybersécurité,* ICCBELGIUM, sd.

dreigt ons onlinebeveiligingsysteem op andere vlakken erg kwetsbaar te worden.[13] Het is bijgevolg de taak van de overheid om zich te mengen in de marktwerking. De overheid zal ze er moeten op toezien dat de markt kan blijven spelen zodat innovatie gestimuleerd wordt en de kosten gedrukt worden.[14]

Naast het spanningsveld tussen het algemeen belang en de belangen van de private spelers, is er nog een ander typerend kenmerk voor cybersecurity. Zo is nagenoeg elk element van ons dagelijks leven gebaat bij een degelijk cybersecuritybeleid. Met de nieuwe technologische evoluties zoals het internet of things (IoT) zal deze digitale verbondenheid van alle aspecten van onze samenleving alleen maar toenemen. Uit de vakliteratuur blijkt een eensgezindheid over het gegeven dat de overheid minimaal een coördinerende rol moet opnemen als het om cybersecurity gaat. Gelukkig zijn er zowel op Europees als op nationaal niveau al heel wat initiatieven om hieraan tegemoet te komen.

Europese initiatieven

Aangezien cybersecurity niet ophoudt bij de landsgrenzen, is het de logica zelve dat er ook op Europees niveau de nodige initiatieven worden genomen. Dit deed de Europese Unie onder andere met de NIS-richtlijn in 2019. Het doel van de NIS-richtlijn is om cyberrisico's beter te stroomlijnen en de bewustwording te vergroten.[15] Deze richtlijn kan algemeen beschouwd worden als een eerste echte Europese wetgeving rond cybersecurity.[16] Naast de NIS-richtlijn vaardigde de EU reeds de algemene verordening gegevensbescherming (AVG)[17] uit. Deze verordening, beter bekend als de GDPR[18], heeft voornamelijk betrekking op de bescherming van persoonlijke data. Bij een cyberaanval is de kans echter reëel dat er persoonlijke data worden vrijgegeven. Om die reden bestaat er dus een kans op overlap in het toepassingsgebied van beide richtlijnen.

[13] *Advancing the concept of cybersecurity as a public good,* Mazaher Kianpur; Stewart Kowalski; Harald Overby, Simulation Modelling Practive Theory, 2022.

[14] *Advancing the concept of cybersecurity as a public good,* Mazaher Kianpur; Stewart Kowalski; Harald Overby, Simulation Modelling Practive Theory, 2022

[15] *QUaternota aan de Vlaamse regering*, sd.

[16] *NIS richtlijn: Een mijlpaalnu één jaar geleden,* Ruben Roex, sd.

[17] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de richtlijn 65/46/EG (algemene verordening gegevensbescherming), bekendgemaakt in het *Publicatieblad van de Europese Unie* op 5 mei 2016, L 119/1.

[18] GDPR: *General Data Protection Regulation*.

se cantonne à des solutions économiquement rentables, on risque de fragiliser considérablement notre système de sécurisation en ligne sur d'autres plans.[13] Il incombe dès lors aux pouvoirs publics de s'immiscer dans le fonctionnement du marché en s'assurant que ce dernier puisse continuer à jouer afin de stimuler l'innovation et de comprimer les coûts.[14]

Outre les tensions entre l'intérêt général et les intérêts des acteurs privés, il est une autre caractéristique typique de la cybersécurité. Ainsi, pratiquement tous les éléments de notre quotidien sont mieux servis par une politique de cybersécurité de qualité. Avec les nouvelles évolutions technologiques, comme l'internet des objets (IoT), cette connectivité numérique de tous les aspects de notre société ne fera que s'accroître. Dans la littérature spécialisée, les avis sont unanimes pour dire que les pouvoirs publics doivent à tout le moins endosser un rôle de coordinateur lorsqu'il s'agit de cybersécurité. Heureusement, les initiatives allant dans ce sens sont déjà nombreuses, tant au niveau européen que national.

Initiatives européennes

Dès lors que la cybersécurité ne s'arrête pas aux frontières nationales, il était logique que l'Europe prenne également les initiatives qui s'imposent. C'est ce qu'elle a fait en adoptant entre autres la directive SRI en 2019. L'objectif de la directive est de mieux identifier les risques en matière de cybersécurité et de renforcer la sensibilisation.[15] D'une manière générale, cette directive peut être considérée comme la première véritable législation européenne en matière de cybersécurité.[16] Outre la directive SRI, l'Union a déjà promulgué le Règlement général sur la protection des données[17]. Ce règlement, mieux connu sous l'acronyme RGPD[18], porte essentiellement sur la protection des données à caractère personnel. Or, en cas de cyberattaque, le risque que des données à caractère personnel soient divulguées est réel. C'est ce qui explique d'ailleurs la probabilité de chevauchement des deux directives quant à leur champ d'application.

[13] *Advancing the concept of cybersecurity as a public good,* Mazaher Kianpur; Stewart Kowalski; Harald Overby, Simulation Modelling Practive Theory, 2022.

[14] *Advancing the concept of cybersecurity as a public good,* Mazaher Kianpur; Stewart Kowalski; Harald Overby, Simulation Modelling Practive Theory, 2022.

[15] *QUaternota aan de Vlaamse regering*, sd.

[16] *NIS richtlijn: Een mijlpaalnu één jaar geleden,* Ruben Roex, sd.

[17] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE (règlement général sur la protection des données), publié au *Journal officiel de l'Union européenne* le 5 mai 2016, L 119/1.

[18] RGPD: *Règlement général sur la protection des données*.

Binnen de NIS-richtlijn staan vooral de Europese en nationale coördinatie van cybersecurity vanuit de overheid voorop. Vanuit die optiek moeten de lidstaten een nationaal contactpunt of CSIRT (*Computer Security Incident Response Team*) oprichten. Dit contactpunt moet vooral instaan voor een correcte registratie van de meldingen van cyberaanvallen. De EU hecht immers veel belang aan de meldingsplicht voor de getroffen bedrijven of organisaties.[19] Een snelle en grondige melding van het incident draagt namelijk bij tot een mogelijke snelle opstart van de organisatie na een incident. Zoals gebruikelijk is het aan de lidstaten om structuren uit te werken die bedrijven en organisaties toelaten om tegemoet te komen aan de Europese richtlijnen.[20] Naast de meldingsplicht breidt de NIS-richtlijn het mandaat van ENISA (Europees agentschap voor cyberbeveiliging) verder uit. Het agentschap staat na de invoering van de richtlijn in voor een betere samenwerking tussen de verschillende nationale CSIRT's. Verder moet ENISA de lidstaten helpen bij de implementatie van de NIS-richtlijn.[21]

Een ander gegeven waarin deze richtlijn voorziet, is een beleid rond de certificering van producten inzake cyberveiligheid. De richtlijn creëert op dit vlak een eerder vrijblijvend kader. Op lange termijn wil de Europese Unie dat er een algemeen Europees kader komt rond de certificering van de cyberveiligheid van producten. Dit moet bijdragen tot de Europese eengemaakte markt. Om die reden moet de nationale certificeringspolitiek geleidelijk aan uitdoven.[22] De NIS-richtlijn voorziet niet in de vermelding van beveiligingsmaatregelen voor de kritieke sectoren.[23] Bij de omzetting van richtlijn moet de Belgische wetgever rekening houden met het kader dat er al is voor kritieke sectoren in de wet van 1 juli 2011 betreffende de bescherming en de beveiliging van de kritieke infrastructuren.[24] Waarin de NIS-richtlijn wel voorziet is een verplichting voor de lidstaten om essentiële sectoren op te lijsten. De EU zelf vermeldt de volgende sectoren: de banksector, de infrastructuur voor de financiële markten, de gezondheidszorg, het drinkwater en de digitale infrastructuur.[25] Volgens de Belgische omzetting van

Dans le cadre de la directive SRI, la coordination européenne et la coordination nationale de la cybersécurité par les pouvoirs publics occupent une place prépondérante. Dans cette optique, les États membres doivent créer un point de contact central, ou CSIRT (Centre de réponse aux incidents de sécurité informatique). Ce point de contact doit essentiellement assurer un enregistrement correct des notifications de cyberattaques. L'Union attache en effet beaucoup d'importance à l'obligation de notification imposée aux entreprises ou organisations touchées.[19] Une notification rapide et détaillée de l'incident contribue en effet à permettre à l'organisation de redémarrer rapidement après un incident. Comme de coutume, il incombe aux États membres d'élaborer les structures permettant aux entreprises et organisations de se conformer aux directives européennes.[20] Outre l'obligation de notification, la directive SRI étend davantage le mandat de l'Agence de l'Union européenne pour la cybersécurité (ENISA). Une fois la directive instaurée, l'Agence assurera une meilleure collaboration entre les différentes équipes nationales (CSIRT), en plus d'aider les États membres à mettre en œuvre la directive SRI.[21]

Une autre mesure prévue par cette directive vise une politique de certification des produits de cybersécurité. La directive a établi à cet égard un cadre relativement peu contraignant. À long terme, l'Union européenne entend créer un cadre européen général pour la certification de la cybersécurité des produits. Ce cadre doit contribuer au marché unique européen. C'est pourquoi la politique de certification nationale devra progressivement prendre fin.[22] La directive SRI ne prévoit pas la mention de mesures de sécurité pour les secteurs critiques.[23] Lors de la transposition de la directive, le législateur belge doit tenir compte du cadre déjà prévu par la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.[24] La directive SRI impose toutefois bien aux États membres l'obligation d'établir une liste de secteurs essentiels. L'Union européenne mentionne elle-même les secteurs suivants: le secteur bancaire, l'infrastructure pour les marchés financiers, les soins de santé, l'eau potable et l'infrastructure numérique.[25] Selon les dispositions transposant la directive

19 *Cyberbeveiliging: een blik op het amalgaam van Europese en Belgische regels,* M. Fierens; S. Royer; P. Valcke, sd.
20 *NIS richtlijn: Een mijlpaalnu één jaar geleden,* Ruben Roex, sd.
21 *Cyberbeveiliging: een blik op het amalgaam van Europese en Belgische regels,* M. Fierens; S. Royer; P. Valcke, sd.
22 *Cyberbeveiliging: een blik op het amalgaam van Europese en Belgische regels,* M. Fierens; S. Royer; P. Valcke, sd.
23 *NIS richtlijn: Een mijlpaalnu één jaar geleden,* Ruben Roex, sd.
24 *NIS richtlijn: Een mijlpaalnu één jaar geleden,* Ruben Roex, sd, wet van 1 juli 2011 betreffende de bescherming en de beveiliging van de kritieke infrastructuren, bekendgemaakt in het *Belgisch Staatsblad* op 15 juli 2011.
25 *NIS richtlijn: Een mijlpaalnu één jaar geleden,* Ruben Roex, sd.

19 *Cyberbeveiliging: een blik op het amalgaam van Europese en Belgische regels,* M. Fierens; S. Royer; P. Valcke, sd.
20 *NIS richtlijn: Een mijlpaalnu één jaar geleden,* Ruben Roex, sd.
21 *Cyberbeveiliging: een blik op het amalgaam van Europese en Belgische regels,* M. Fierens; S. Royer; P. Valcke, sd.
22 *Cyberbeveiliging: een blik op het amalgaam van Europese en Belgische regels,* M. Fierens; S. Royer; P. Valcke, sd.
23 *NIS richtlijn: Een mijlpaalnu één jaar geleden,* Ruben Roex, sd.
24 *NIS richtlijn: Een mijlpaalnu één jaar geleden,* Ruben Roex, sd, loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, publiée au *Moniteur belge* du 15 juillet 2011.
25 *NIS richtlijn: Een mijlpaalnu één jaar geleden,* Ruben Roex, sd.

de NIS-richtlijn in de NIB-wet[26] moeten alle aanbieders van essentiële diensten en digitale dienstverleners alle incidenten met aanzienlijke gevolgen melden. Deze melding moet gebeuren aan het *Computer Security Incident Response Team* (CSIRT). Er wordt een onlineplatform gecreëerd voor deze meldingen.[27]

Nationale initiatieven

Het federaal cybersecurityplan heeft als missie om van België een van de minst kwetsbare landen te maken inzake cybersecurity tegen 2025.[28] Op dit moment scoort ons land al relatief goed op het vlak van cyberveiligheid. Zo prijken we in de *global security index* (GCI) België op een verdienstelijke dertigste plaats. Vooral Vlaanderen heeft een goede reputatie op het vlak cyberveiligheid. Zeker op het vlak van cryptografie nemen we een prominente positie in.[29]

In ons land zijn er reeds heel wat initiatieven en structuren die bijdragen tot een beter cyberbeleid. Zo werd in 2014 het Centrum voor Cybersecurity Belgium (hierna: "CCB") opgericht. Dit centrum staat in voor coördinatie en veiligheid van het cybersecuritybeleid. Het CCB analyseert alle info over cyberdreigingen en stuurt waarschuwingen uit. Hiervoor kan het zich beroepen op BE-Alert.[30]

Daarnaast is er in ons land een nationaal crisiscentrum dat de coördinatie van een cybernoodplan op nationaal niveau voor zijn rekening neemt. Samen met CCB staat het crisiscenturm in voor het crisisbeheer van een (potentiële) aanval. Het CCB heeft ook een earlywarningsystem voor vitale sectoren. Op die manier worden deze sectoren met extra aandacht gemonitord. Verder worden bedrijven en organisaties conform de Europese meldingsplicht aangemoedigd om de kwetsbaarheden van hun infrastructuur te publiceren.

Daarnaast beschikt ons land sinds enkele jaren over een Gegevensbeschermingsautoriteit (hierna: "GBA"). Zoals besproken bij het hoofdstuk rond de Europese initiatieven is een goede samenwerking tussen het CCB en de GBA een absolute noodzaak. Er kan bij een

[26] NIB (Netwerk- en Infomatiebeveiliging) – Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, bekendgemaakt in het *Belgisch Staatsblad* op 3 mei 2019.

[27] *Cyberbeveiliging: een blik op het amalgaam van Europese en Belgische regels,* M. Fierens; S. Royer; P. Valcke, sd.

[28] *Cybersecurity strategie België 2.0,* Centre For Cybersecurity Belgium, 2021.

[29] *QUaternota aan de Vlaamse regering,* sd.

[30] *Cybersecurity strategie België 2.0,* Centre For Cybersecurity Belgium, 2021.

SRI dans la loi SRI belge[26], tout opérateur de services essentiels et tout prestataire de services numériques doit notifier tous les incidents ayant un impact significatif sur la disponibilité au centre national de réponse aux incidents de sécurité informatique (CSIRT national). Une plateforme en ligne a été créée pour ces notifications.[27]

Initiatives nationales

Le plan fédéral concernant la cybersécurité vise à faire de la Belgique l'un des États les moins vulnérables en matière de cybersécurité à l'horizon 2025.[28] Pour l'heure, la Belgique est relativement performante en matière de cybersécurité, comme l'indique son honorable trentième place dans l'indice global de sécurité (GSI – *global security index*). C'est principalement la Flandre qui a bonne réputation en matière de cybersécurité, certainement dans le domaine de la cryptographie, où elle joue un rôle majeur.[29]

Dans notre pays, un grand nombre d'initiatives et de structures contribuent déjà à une meilleure cybersécurité. Par exemple, le Centre pour la Cybersécurité Belgique (CCB ci-après) créé en 2014 est chargé de la coordination et de la sécurité de la politique en matière de cybersécurité. Le CCB analyse l'ensemble des informations concernant les cybermenaces et émet des avertissements au moyen du système BE-Alert.[30]

La Belgique s'est en outre dotée d'un centre de crise national qui prend en charge la coordination d'un cyberplan d'urgence au niveau national. Conjointement avec le CCB, le centre de crise assure la gestion de crise en cas d'attaque (potentielle). Le CCB dispose également d'un système d'alerte précoce pour les secteurs vitaux qui permet de surveiller ces secteurs avec une attention particulière. En outre, conformément à l'obligation de notification européenne, les entreprises et les organisations sont encouragées à publier les vulnérabilités de leur infrastructure.

En outre, depuis quelques années, la Belgique dispose d'une Autorité de protection des données (APD ci-après). Comme indiqué au cours de la discussion à propos du chapitre consacré aux initiatives européennes, une bonne coopération entre le CCB et l'APD

[26] SRI (sécurité des réseaux et des systèmes d'information) – Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, publiée au *Moniteur belge* du 3 mai 2019.

[27] *Cyberbeveiliging: een blik op het amalgaam van Europese en Belgische regels,* M. Fierens; S. Royer; P. Valcke, sd.

[28] *Stratégie cybersécurité Belgique 2.0,* Centre pour la Cybersécurité Belgique, 2021.

[29] *Quaternota aan de Vlaamse regering,* sd.

[30] *Stratégie cybersécurité Belgique 2.0,* Centre pour la Cybersécurité Belgique, 2021.

cyberaanval namelijk sprake zijn van een mogelijk datalek. Op zo'n moment zullen beide instanties geïnformeerd moeten worden. Naast alle bovengenoemde organen is er ook nog de *Cyber Security Coalition Belgium*. Deze coalitie brengt domeinexperten uit private, academische en publieke sectoren bij elkaar rond cyberveiligheid.[31] Een ander expertisenetwerk dat in ons land werkzaam is, is de (REN) Cybercrime. Ook zij brengen specialisten bij elkaar in een periodiek overleg.[32] Daarnaast is er ook nog het CSI DPO-platform. Zij brengen veiligheidsadviseurs en databeschermingsverantwoordelijken van elke overheidsdienst bij elkaar.[33] Tot slot zijn er bij de federale politie, de Veiligheid van de Staat, het openbaar ministerie en Defensie gespecialiseerde diensten die zich uitsluitend bezighouden met cyberveiligheid.

Bovenop de bovengenoemde structuren en organen nemen verschillende beleidsniveaus in ons land ook concrete initiatieven in de strijd tegen cybersecurity. Zo zal de federale overheid in 2024 een "*Cyber Green House*" oprichten. Deze instantie zal een testomgeving faciliteren waarin IT-infrastructuur getest kan worden alvorens ze op de markt wordt gebracht. In antwoord op een parlementaire vraag gaf de premier aan dat het *Cyber Green House* "zal fungeren als een centraal onderzoeks- en innovatiecentrum dat alle relevante actoren uit de academische, private en publieke sector en hun kennisbehoeften, onderzoek, vraag en aanbod op het gebied van cyberveiligheid samenbrengt in een integraal ecosysteem."[34]

Verder geeft de federale overheid in haar nationaal plan voor cybersecurity aan dat ze verder zal investeren in onderzoek en ontwikkeling op het vlak van cyberveiligheid voor openbare instellingen en onderwijssectoren.[35] Ook de Vlaamse regering heeft in haar beleidsagenda drie thema's opgenomen om het cybersecuritybeleid verder te ondersteunen. Zo wordt er geïnvesteerd in strategisch basisonderzoek, wordt er gewerkt met een centrale focus op de implementatie van cybersecuritytoepassingen en wordt er, ten slotte, een flankerend beleid gevoerd inzake cybersecurity. Concreet wil de Vlaamse overheid inzetten op meer training en opleiding binnen de industrie van de cybersecurity. Om van een globaal

[31] *Cybersecurity strategie België 2.0,* Centre For Cybersecurity Belgium, 2021.
[32] *Cybersecurity strategie België 2.0,* Centre For Cybersecurity Belgium, 2021.
[33] *Cybersecurity strategie België 2.0,* Centre For Cybersecurity Belgium, 2021.
[34] Schriftelijke vraag nr. 0140 van de heer Steven Matheï aan premier Alexander De Croo van 9 november 2021 over de "Campus Cybersecurity", *Bulletin van Vragen en Antwoorden* van 18 november 2011, B069.
[35] *Cybersecurity strategie België 2.0,* Centre For Cybersecurity Belgium, 2021.

est absolument nécessaire. En effet, toute cyberattaque peut entraîner une fuite de données. Dans ce cas, ces deux organismes devront s'échanger les informations nécessaires. Outre les organes précités, la *Cyber Security Coalition Belgium* a été instituée. Cette coalition rassemble des experts des secteurs privé, académique et public dans le domaine de la cybersécurité.[31] Un autre réseau actif dans notre pays est le réseau d'expertise (REN) Cybercriminalité. Ce réseau réunit également des spécialistes lors d'une concertation périodique.[32] On peut également citer la plateforme CSI/DPO, qui réunit les conseillers en sécurité de l'information et les délégués à la protection des données de chaque service public.[33] Enfin, la Police fédérale, le Sûreté de l'État, le ministère public et la Défense disposent de services spécialisés qui s'occupent exclusivement de cybersécurité.

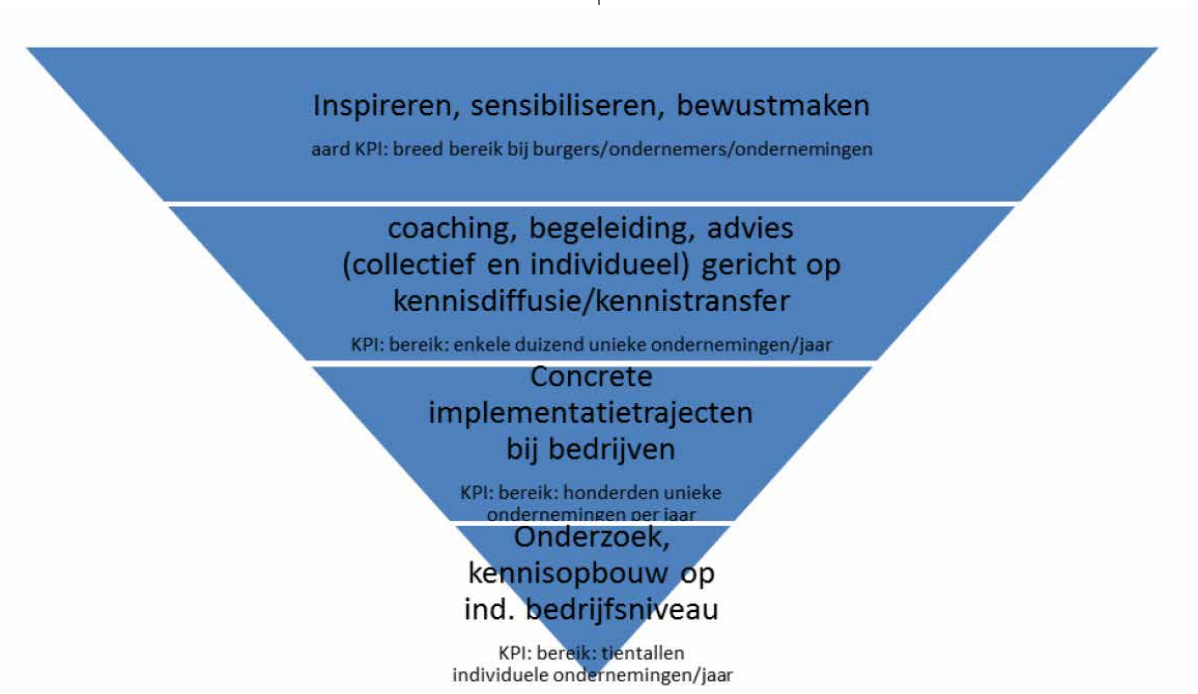
Outre les structures et les organes précités, différents niveaux de pouvoir prennent des initiatives dans la lutte contre les cybermenaces. Les autorités fédérales créeront par exemple, en 2024, une *Cyber Green House*. Cette instance facilitera la mise en place d'un environnement de test où les infrastructures informatiques pourront être testées avant leur mise sur le marché. En réponse à une question parlementaire, le premier ministre a indiqué que la *Cyber Green House* "fonctionnera comme un centre de recherche et d'innovation central réunissant dans un écosystème global tous les acteurs concernés des secteurs universitaire, privé et public ainsi que leurs besoins en matière de connaissances, de recherche, d'offre et de demande dans le domaine de la cybersécurité".[34]

En outre, l'autorité fédérale indique dans son plan national pour la cybersécurité qu'elle investira davantage dans la recherche et le développement dans le domaine de la cybersécurité pour les institutions publiques et les secteurs de l'enseignement.[35] Dans son agenda politique, le gouvernement flamand a lui aussi inclus trois thèmes visant à soutenir davantage la politique de cybersécurité. Des investissements seront ainsi réalisés dans la recherche fondamentale stratégique, l'accent central sera mis sur la mise en œuvre d'applications de cybersécurité et, enfin, une politique d'accompagnement sera menée en matière de cybersécurité. Concrètement, l'autorité flamande entend se concentrer sur une intensification

[31] *Stratégie cybersécurité Belgique 2.0,* Centre pour la Cybersécurité Belgique, 2021.
[32] *Stratégie cybersécurité Belgique 2.0,* Centre pour la Cybersécurité Belgique, 2021.
[33] *Stratégie cybersécurité Belgique 2.0,* Centre pour la Cybersécurité Belgique, 2021.
[34] Question écrite n° 0140 de M. Steven Matheï au premier ministre Alexandre De Croo du 9 novembre 2021 sur le "Campus cybersécurité", *Bulletin des Questions et Réponses* du 18 novembre 2021, B069.
[35] *Stratégie cybersécurité Belgique 2.0,* Centre For Cybersecurity Belgium, 2021.

beleidsplan tot concrete realisaties te komen, stelt zij volgend investeringsplan inzake cyberveiligheid voor:[36]

de la formation dans l'industrie de la cybersécurité. Afin de passer d'un projet politique global à des réalisations concrètes, elle propose le plan d'investissement suivant en matière de cybersécurité:[36]



De huidige problemen en de mogelijke oplossingen

Vanuit overheidshoek zijn er al heel wat initiatieven genomen die kunnen bijdragen aan een effectiever cyberbeleid. Hoe meer structuren en organisaties er worden opgericht, hoe groter de nood aan centralisatie en coördinatie. Laat dit nu net een element zijn dat in de vakliteratuur als een van de belangrijkste voorwaarden voor een doortastend cyberbeleid wordt beschouwd. Zeker indien we het wijdverspreide karakter dat cyberveiligheid zo typeert in rekening nemen, kunnen we niet anders dan besluiten dat de coördinatie een absolute noodzaak is. Deze overkoepelende blik komt bij voorbaat toe aan de overheid. Ook ons land kan nog meer inzetten op een centrale sturing vanuit de overheid inzake cybersecurity. Ons typerende complexe politieke landschap maakt een eenduidig beleid moeilijk. Om die reden moet er een sterke regulator komen die de politiek overstijgt.[37] De oprichting van een centraal Centrum voor Cybersecurity is in casu een stap in de goede richting. Een concreet voorbeeld dat makkelijker verholpen kan worden door een meer uniform en gecentraliseerd beleid is de meldingsplicht die geldt voor gelekte persoonsgegevens aan de GBA en de meldingstermijn voor een

Les problèmes actuels et les solutions possibles

Du côté des autorités, de nombreuses initiatives qui pourraient contribuer à optimiser la cyberpolitique ont déjà été prises. Plus le nombre de structures et d'organisations mises en place est élevé, plus le besoin de centralisation et de coordination est important. Il s'agit d'un élément qui est considéré dans la littérature spécialisée comme l'une des conditions les plus importantes pour une cyberpolitique dynamique. Surtout si l'on tient compte du caractère très universel de la cybersécurité, on ne peut s'empêcher de conclure que la coordination est une nécessité absolue. Cette vue d'ensemble incombe en premier lieu aux autorités. Notre pays pourrait également faire davantage pour mettre en place un pilotage central par les autorités en matière de cybersécurité. Compte tenu de la complexité qui caractérise notre paysage politique, il est difficile de mener une politique univoque. C'est pourquoi nous avons besoin d'un régulateur fort qui dépasse la politique.[37] En l'espèce, la création d'un point de contact central en matière de cybersécurité va dans la bonne direction. Un exemple concret auquel il est plus facile de remédier par une politique plus uniforme et centralisée est l'obligation de signaler les fuites de

[36] KPI is de *key performance indicator* (kritieke prestatie-indicator).

[37] *België heeft een sterke autoriteit op het vlak van cybersecurity nodig,* Filip Verstockt, sd.

[36] KPI est l'acronyme de *key performance indicator* (indicateur clé de performance).

[37] *België heeft een sterke autoriteit op het vlak van cybersecurity nodig,* Filip Verstockt, sd.

cyberaanval aan het CCB. Beide termijnen verschillen van elkaar. Een centraal meldpunt en een uniforme tijdspanne waarbinnen een incident gemeld moet worden, kunnen hier soelaas bieden.

Een centrale aansturing van alle instanties die zich exclusief bezighouden met cybersecurity zal echter niet volstaan. Aangezien cyberveiligheid betrekking heeft op nagenoeg alle aspecten van onze samenleving is het een noodzaak dat alle overheidsdiensten binnen hun eigen expertise aandacht hebben voor een component cybersecurity. Zo zou er bij de overheidsdiensten zoals de Rijksdienst voor Sociale Zekerheid (RSZ) of de Federale Overheidsdienst Financiën niet altijd begrip zijn voor de onmogelijkheid van bedrijven, die getroffen werden door een cyberaanval, om aan hun verplichtingen te voldoen binnen de algemeen geldende termijnen. Ook bij de lokale politie bijvoorbeeld zou er niet altijd even accuraat gereageerd worden op een melding van een cyberaanval. Ook hier moet de overheid inzetten op preventie en opleiding van haar personeel.

Uiteraard moeten de federale initiatieven goed afgestemd worden op de initiatieven die de deelstaten nemen. Om verwarring bij de betrokken partijen te vermijden, is een goede samenwerking tussen alle beleidsniveaus daarom sterk aangewezen.

Een ander probleem waarmee velen van onze bedrijven en organisaties geconfronteerd worden, is de kostprijs die verbonden is aan een degelijk cybersecuritybeleid. De bedrijven kunnen verzekeringen afsluiten die hen beschermen en bijstaan in het geval van een cyberaanval. Zo kan men verzekeringen vinden voor de exploitatieverliezen, de kosten voor het herstel van de gegevens en de software, de eventuele reputatieschade of nog de kosten bij onderhandelingen met de daders, en in het uiterste geval zelfs het betalen van losgeld.[38] De prijzen die voor deze polissen worden gevraagd, zouden voor sommige sectoren en organisaties meer dan aanzienlijk zijn. De vraag of hier in overleg met de verzekeringssector een bijsturing door de overheid vereist is, dringt zich op. Ook een mogelijke verplichte verzekering, naar analogie met de verplichte brandverzekering, is een piste die moet overwogen worden.

[38] Schriftelijke vraag nr. 0779 van mevrouw Leen Dlerick aan minister van Economie Pierre-Yves Dermagne van 23 februari 2022, over "de schade en de verzekering tegen cyberaanvallen", *Bulletin van Vragen en Antwoorden* van 5 april 2022, B082.

données personnelles à l'APD et le délai de signalement d'une cyberattaque au CCB. Les deux délais diffèrent l'un de l'autre. Un point de contact central et un délai uniforme dans lequel un incident doit être signalé pourraient déjà améliorer la situation.

Toutefois, un pilotage centralisé de l'ensemble des organes qui s'occupent exclusivement de cybersécurité ne suffira pas. La cybersécurité touchant à presque tous les aspects de notre société, il faudrait en effet que l'ensemble des services publics accordent de l'attention à l'aspect de la cybersécurité dans le cadre de leur expertise propre. Ainsi, des services publics comme l'Office national de la sécurité sociale (ONSS) ou le Service public fédéral Finances ne se montreraient pas toujours compréhensifs face à des entreprises qui, après avoir subi une cyberattaque, ne sont pas en mesure de satisfaire à leurs obligations dans les délais généraux en vigueur. Un autre exemple est la police locale, qui ne réagirait pas non plus toujours de manière adéquate aux notifications de cyberattaque. Ici aussi, les pouvoirs publics doivent miser sur la prévention et sur la formation de son personnel.

Il conviendrait effectivement d'harmoniser correctement les initiatives fédérales et les initiatives des entités fédérées. Pour éviter toute confusion dans le chef des parties concernées, il serait donc fortement souhaitable de mettre en place une bonne collaboration entre tous les niveaux de pouvoir.

Le coût d'une politique de cybersécurité de qualité constitue un autre problème auquel nombre de nos entreprises et organisations sont confrontées. Les entreprises peuvent souscrire des assurances qui les protègent et prévoient une assistance en cas de cyberattaque. Il existe par exemple des assurances couvrant les pertes d'exploitation, le coût de la reconstitution des données et de la réparation des logiciels, les dommages éventuels à la réputation ou encore les coûts supportés dans le cadre des négociations avec les auteurs de l'attaque, voire, dans le pire des cas, le paiement d'une rançon.[38] Le prix demandé pour ces polices d'assurance serait plus que considérable pour certains secteurs et organisations. Il est urgent de répondre à la question de savoir si les pouvoirs publics devraient apporter une correction en la matière, en concertation avec le secteur des assurances. L'instauration éventuelle d'une assurance obligatoire, par analogie avec l'assurance incendie obligatoire, est aussi une piste à envisager.

[38] Question écrite n° 0779 de Mme Leen Dlerick au ministre de l'Économie Pierre-Yves Dermagne du 23 février 2022, sur "Les dommages et les assurances en matière de cyberattaques", *Bulletin des Questions et Réponses* du 5 avril 2022, B082.

Overigens gaat de kostprijs die verbonden is aan een cybersecuritybeleid veel verder dan enkel een verzekering tegen een mogelijke aanval. Ook de performante beveiliging van de IT-systemen zelf gaat gepaard met aanzienlijke vaak wederkerende kosten. Daarnaast moeten ook de investering van de bedrijven en de organisaties in de opleiding en sensibilisering van hun personeel mee in rekening gebracht worden. De overheid moet bekijken hoe zij bedrijven kan stimuleren om te investeren in cybersecurity door hen op een nader te bepalen manier tegemoet te komen in de kosten die ermee gepaard gaan.

Tot slot is er mogelijk ook een financiële impact voor de organisaties omdat er losgeld betaald moet worden om de IT-systemen opnieuw vrij te geven. Minister Van Peteghem gaf in een antwoord op parlementaire vragen aan dat de kosten die een cyberaanval teweegbrengt mogelijk nu al beschouwd kunnen worden als een aftrekbare beroepskost. Hiertoe moet wel voldaan zijn aan een aantal voorwaarden die het Wetboek van Inkomstenbelasting 92 bepaalt.[39] [40]

Onze bedrijven en organisaties zijn niet alleen verantwoordelijk voor de veiligheid van de software en de hardware die zij gebruiken. Ook de producenten van deze producten en diensten moeten hun verantwoordelijkheid nemen. De invoering van een certificering voor veilige IT-apparatuur zou hier een oplossing kunnen bieden. De producten die op de markt worden gebracht, zouden dan eerst een certificaat van cyberveiligheid moeten aanvragen bij een door de overheid erkende auditeur. Er zou bij dit certificaat kunnen gewerkt worden met een schaal die aangeeft hoe veilig een cyberproduct is. Inspiratie kan worden gezocht in de ranking toegepast op het energiegebruik van elektronische toestellen of in de nutriscore die wordt toegekend aan voedingsproducten. Of deze certificering al dan niet verplicht moet worden voor de producenten is voer voor verdere discussie. Binnen deze optiek wordt in het cybersecurityplan vermeld dat de federale regering werk zal maken van een kader voor de certificatie van software. België zal hiertoe een *cybersecurity certification authority* (NCCA) oprichten. Volgens het cybersecurityplan zal deze autoriteit daartoe samenwerken met de Belgische

Par ailleurs, le coût d'une politique de cybersécurité va bien au-delà de la seule assurance contre de potentielles cyberattaques. La sécurisation performante des systèmes informatiques à proprement parler implique un coût considérable et souvent récurrent. En outre, il convient aussi de tenir compte des investissements réalisés par les entreprises et les organisations dans la formation et la sensibilisation des membres de leur personnel. Les pouvoirs publics devraient examiner comment ils pourraient encourager les entreprises à investir dans la cybersécurité en intervenant dans leurs coûts d'investissement selon des modalités à définir.

Enfin, toute cyberattaque peut aussi avoir des répercussions financières pour les organisations lorsque celles-ci doivent payer une rançon en échange du déblocage de leurs systèmes informatiques. En réponse à plusieurs questions parlementaires à ce sujet, le ministre Van Peteghem a indiqué que les frais découlant des cyberattaques pouvaient déjà être considérées comme des frais professionnels déductibles, pour autant que plusieurs conditions prévues par le Code des impôts sur les revenus 1992 soient remplies.[39] [40]

Nos entreprises et nos organisations ne sont pas les seules responsables de la sécurité des logiciels et du matériel informatique qu'elles utilisent. Les fabricants de ces produits et les fournisseurs de ces services doivent également prendre leurs responsabilités. L'instauration d'une certification pour la sécurité des équipements informatiques pourrait constituer une solution à cet égard. Les fabricants des produits mis sur le marché devraient alors demander un certificat de cybersécurité à un auditeur agréé par les autorités publiques avant leur commercialisation. L'établissement de ce certificat pourrait reposer sur l'utilisation d'une échelle indiquant le degré de sécurité des produits informatiques. À cet égard, on pourrait s'inspirer de la classification appliquée à la consommation énergétique des appareils électroniques ou du nutriscore attribué aux produits alimentaires. La question de savoir si cette certification devra être rendue obligatoire ou non pour les fabricants devra être examinée ultérieurement. Dans cette optique, le plan concernant la cybersécurité indique que le gouvernement fédéral élaborera un cadre pour la certification des logiciels. À cette fin, la Belgique créera une autorité nationale de

[39] Schriftelijke vraag nr. 0755 van de heer Steven Matheï aan minister van Financiën Vincent van Peteghem van 8 november 2021 over de "Losgeld bij cyberaanvallen", *Bulletin van Vragen en Antwoorden* van 11 februari 2022, B077.

[40] Schriftelijke vraag nr. 0711 van de heer Steven Matheï aan minister van Financiën Vincent van Peteghem van 8 november 2021 over de "Aftrekbaarheid beroepskost losgeld cyberaanvallen", *Bulletin van Vragen en Antwoorden* van 6 december 2022, B071.

[39] Question écrite n° 0755 de M. Steven Matheï au ministre des Finances Vincent van Peteghem du 8 novembre 2021 sur "Les rançons versées à la suite de cyberattaques", *Bulletin des Questions et Réponses* du 11 février 2022, B077.

[40] Question écrite n° 0711 de M. Steven Matheï au ministre des Finances Vincent van Peteghem du 8 novembre 2021 sur "La déductibilité des rançons au titre de frais professionnels", *Bulletin des Questions et Réponses* du 6 décembre 2021, B071.

accreditatie-organisatie (Belac).[41] Daarbij aansluitend is het van belang dat bedrijven de gehele keten van alle software- en hardwaretoepassingen laten controleren op cyberveiligheid. Het is niet omdat een individueel product veilig is dat het dat ook nog is wanneer het wordt verbonden met andere apparaten.

Tot slot blijkt uit de praktijk dat er een groot tekort is aan cybersecuritytalent op de arbeidsmarkt. Het onderwerp zou te weinig aan bod komen in de schoolopleidingen *(Centre For Cybersecurity Belgiu*m 2021)[42]. Door meer in te zetten op opleiding, zowel op de werkvloer als voor voltijdse studenten, kan dit weggewerkt worden. Ook een specifieke promotiecampagne rond het imago van IT en cybersecurity kan daaraan bijdragen.

Dit valt echter voornamelijk onder de bevoegdheden van de deelstaten. Het is de taak van de federale overheid om de deelstaten hierbij binnen haar bevoegdheden te ondersteunen.

Steven Matheï (cd&v)
Leentje Grillaert (cd&v)

certification de la cybersécurité (*cybersecurity certification authority* (NCCA)). Le plan cybersécurité indique que cette autorité coopérera avec l'organisme belge d'accréditation BELAC.[41] Dans le même ordre d'idées, il importe que les entreprises fassent contrôler la cybersécurité de l'ensemble de leur chaîne de logiciels et d'équipements informatiques. En effet, ce n'est pas parce qu'un produit individuel est sécurisé qu'il le reste lorsqu'il est connecté à d'autres appareils.

Enfin, la pratique enseigne que le marché du travail manque cruellement de spécialistes de la cybersécurité. Cette thématique serait trop peu abordée dans les formations scolaires (Centre pour la Cybersécurité Belgique, 2021)[42]. On pourrait y remédier en formant davantage de travailleurs et d'étudiants à temps plein dans ce domaine. Une campagne promotionnelle visant spécifiquement l'image de l'informatique et de la cybersécurité pourrait également y contribuer.

Toutefois, cette initiative relèverait principalement de la compétence des entités fédérées. Il incombera dès lors à l'autorité fédérale de soutenir, dans le cadre de ses compétences, les entités fédérées en la matière.

41 *Cybersecurity strategie België 2.0,* Centre For Cybersecurity Belgium, 2021.
42 *Cybersecurity strategie België 2.0,* Centre For Cybersecurity Belgium, 2021.

41 *Stratégie cybersecurité Belgique 2.0*, Centre pour la Cybersécurité Belgique, 2021.
42 *Stratégie cybersecurité Belgique 2.0*, Centre pour la Cybersécurité Belgique, 2021.

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. gelet op de toenemende digitalisering en interconnectie van onze samenleving;

B. gelet op de verdeelde bevoegdheid tussen de federale overheid en de deelstaten inzake cybersecurity;

C. gelet op de toenemende dreiging van cyberincidenten;

D. gelet op het toenemend belang van cybersecurity in geopolitieke conflicten;

E. gelet op het wijde spectrum aan gebieden dat wordt beïnvloed door cyberveiligheid wat kenmerkend is voor cybersecurity;

F. gelet op de Europese NIS-richtlijn die de lidstaten verplicht tot de oprichting van een *Computer Security Incident Response Team* (CSIRT);

G. gelet op de grote kosten en financiële risico's die voor bedrijven en organisaties verbonden zijn aan cybersecurity;

H. gelet op de technologische ontwikkelingen zoals artificiële Intelligentie, kwatumcomputing en het internet of things waardoor het belang van cybersecurity alleen maar zal toenemen;

I. gelet op de nood aan kennisdeling die noodzakelijk is voor een competitief cybersecuritybeleid;

J. gelet op de nood aan meer arbeidskrachten met een expertise in cybersecurity;

K. gelet op de doelstelling van de federale regering om ons land tot een van de 25 minst kwetsbare landen te maken op het vlak van cybersecurity tegen 2025;

L. gelet op de afhankelijkheid van onze bedrijven en organisaties van internationale software providers;

M. gelet op het belang van de menselijke factor in de cyberveiligheid;

N. gelet op het belang van coherente en representatieve data in de strijd tegen cybercrime;

PROPOSITION DE RÉSOLUTION

La Chambre des représentants,

A. vu la numérisation et l'interconnexion croissantes de notre société;

B. considérant que les compétences en matière de cybersécurité sont partagées entre l'autorité fédérale et les entités fédérées;

C. vu la menace croissante de cyberincidents;

D. vu l'importance croissante de la cybersécurité dans les conflits géopolitiques;

E. vu le large spectre des domaines influencés par la cybersécurité, une caractéristique marquante de cette matière;

F. vu la directive européenne SRI, qui impose aux États membres l'obligation de créer un *Centre de réponse aux incidents de sécurité informatique* (CSIRT);

G. vu les coûts et les risques financiers importants assumés par les entreprises et les organisations en matière de cybersécurité;

H. vu les évolutions technologiques telles que l'intelligence artificielle, l'informatique quantique et l'internet des objets, qui ne feront qu'accroître l'importance de la cybersécurité;

I. considérant qu'un partage des connaissances est nécessaire pour mener une politique de cybersécurité compétitive;

J. vu la nécessité de disposer de davantage de personnel spécialisé dans le domaine de la cybersécurité;

K. considérant que le gouvernement fédéral entend faire de la Belgique l'un des 25 pays les moins vulnérables en termes de cybersécurité d'ici 2025;

L. vu la dépendance de nos entreprises et organisations vis-à-vis des fournisseurs de logiciels internationaux;

M. vu l'importance du facteur humain dans la cybersécurité;

N. considérant qu'il est essentiel de disposer de données cohérentes et représentatives dans la lutte contre la cybercriminalité;

VERZOEKT DE FEDERALE REGERING:

1. in overleg met de deelstaten, de vele instanties en initiatieven die reeds bestaan in ons land rond cybersecurity beter te stroomlijnen en op elkaar af te stemmen;

2. één centraal aanspreekpunt aan te stellen inzake cybersecurity zoals de Gegevensbeschermingsautoriteit (GBA) het aanspreekpunt is inzake de bescherming van persoonsgegevens;

3. in overleg met de verzekeringssector, te onderzoeken of de huidige marktwerking rond cybersecurityverzekeringen moet worden bijgestuurd;

4. te onderzoeken of een fiscale aanmoediging of een eventuele wettelijke verplichting van cybersecurityverzekering voor bedrijven, organisaties en vereniging wenselijk is;

5. te onderzoeken of een prijsvergelijking tussen de verschillende aangeboden verzekeringen vanuit de overheid opgezet kan worden;

6. te bekijken hoe bedrijven en organisaties financieel ondersteund kunnen worden in de kosten waarmee zij geconfronteerd worden bij de uitbouw van een cybersecuritybeleid;

7. de kennisdeling vanuit wetenschappelijk onderzoek, overheidsinstellingen en vanuit de praktijk te stimuleren;

8. de deelstaten te ondersteunen in hun beleid om cybersecurity meer aan bod te laten komen in het onderwijs en in opleidingen op de werkvloer;

9. te bekijken hoe een certifiëringsbeleid voor software- en hardwaretoepassingen kan ingevoerd worden;

10. te voorzien in een formele rapportage aan de raad van bestuur van Overheidsbedrijven met betrekking tot het gevoerde cybersecuritybeleid binnen deze bedrijven;

11. private bedrijven te stimuleren om een formele rapportage te voorzien aan de raad van bestuur met betrekking tot het gevoerde cybersecuritybeleid binnen het bedrijf;

12. te bekijken hoe bedrijven en organisaties financieel ondersteund kunnen worden bij het uitvoeren van een audit inzake cybersecurity, naar het voorbeeld van de

DEMANDE AU GOUVERNEMENT FÉDÉRAL:

1. de mieux rationaliser et coordonner, en concertation avec les entités fédérées, les nombreuses instances et initiatives qui existent déjà dans notre pays en matière de cybersécurité;

2. de désigner un point de contact central unique en matière de cybersécurité, à l'instar de l'Autorité de protection des données (APD), qui est le point de contact en matière de protection des données à caractère personnel;

3. d'examiner en concertation avec le secteur des assurances si le fonctionnement actuel du marché doit être modifié en ce qui concerne les assurances en matière de cybersécurité;

4. d'examiner s'il est opportun d'instaurer un incitant fiscal ou une éventuelle obligation légale en matière de cyberassurance pour les entreprises, les organisations et les associations;

5. d'étudier la possibilité de mise en place par les pouvoirs publics d'une comparaison des prix des différentes assurances proposées;

6. d'examiner comment les entreprises et les organisations peuvent être soutenues financièrement pour faire face aux coûts liés au développement d'une politique de cybersécurité;

7. de stimuler le partage des connaissances issues de la recherche scientifique, des institutions publiques et de la pratique;

8. de soutenir les entités fédérées dans leur politique visant à accorder une plus grande attention à la cybersécurité dans l'enseignement et dans les formations sur le lieu de travail;

9. d'examiner comment une politique de certification des applications logicielles et matérielles pourrait être mise en place;

10. de prévoir un rapportage formel au conseil d'administration des entreprises publiques à propos de la politique qui y est menée en matière de cybersécurité;

11. d'encourager les entreprises privées à prévoir un rapportage formel au conseil d'administration de la politique menée au sein de l'entreprise en matière de cybersécurité;

12. d'examiner comment les entreprises et les organisations peuvent bénéficier d'un soutien financier pour la réalisation d'un audit de cybersécurité, par analogie

financiële ondersteuning voor de Vlaamse gemeenten bij het uitvoeren van een gelijkaardige audit;

13. de bevolking en bedrijven te sensibiliseren inzake cybersecurity met een focus op het belang van de individuele waakzaamheid van elke gebruiker;

14. overheidsinstanties en -organisaties te stimuleren in de verzameling en de analyse van data in het kader van cybersecurity;

15. de verschillende meldingstermijnen bepaald door enerzijds de NIS-richtlijn en anderzijds de GBA-verordening te uniformiseren;

16. één centraal meldpunt op te richten om onduidelijkheid te vermijden;

17. meer expertise en preventie inzake cybersecurity uit te bouwen binnen alle overheidsdiensten die in contact staan met onze bedrijven en organisaties;

18. In overleg met de deelstaten, de lokale besturen verder te sensibiliseren inzake cybersecurity;

19. de expertise inzake cybersecurity aanwezig bij de lokale politie en de federale politie verder uit te bouwen.

29 augustus 2024

Steven Matheï (cd&v)
Leentje Grillaert (cd&v)

avec le soutien financier dont bénéficient les communes flamandes pour la réalisation d'un tel audit;

13. de sensibiliser la population et les entreprises à la cybersécurité en mettant l'accent sur l'importance de la vigilance individuelle de chaque utilisateur;

14. d'encourager les instances et les organisations publiques à procéder à la collecte et à l'analyse des données dans le cadre de la cybersécurité;

15. d'uniformiser les différents délais de notification définis par la directive SRI, d'une part, et par le règlement APD, d'autre part;

16. de créer un point de contact central afin d'éviter toute ambiguïté;

17. de développer une plus grande expertise et davantage de prévention en matière de cybersécurité au sein de tous les services publics en contact avec nos entreprises et nos organisations;

18. de continuer à sensibiliser les pouvoirs locaux à la cybersécurité en concertation avec les entités fédérées;

19. de continuer à développer l'expertise acquise en matière de cybersécurité par la police locale et la police fédérale.

29 août 2024

Centrale drukkerij - Imprimerie centrale