DOC 55 **1788/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

11 février 2021

PROPOSITION DE RÉSOLUTION

relative à la cyberdéfense et à l'attribution des cyberattaques étatiques

(déposée par M. Michael Freilich et consorts)

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

11 februari 2021

VOORSTEL VAN RESOLUTIE

betreffende cyberdefensie en de attributie van statelijke cyberaanvallen

(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	:	*VB*
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*
sp.a	:	*socialistische partij anders*
cdH	:	*centre démocrate Humaniste*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de numering 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 defi nitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénaire*	*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)*

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

Dans un monde qui se numérise sans cesse davantage, où de plus en plus de systèmes sont interconnectés et où des pans entiers de notre vie sont gérés virtuellement, le besoin de protéger nos infrastructures critiques et nos intérêts nationaux contre les ingérences étrangères se fait également de plus en plus pressant. Aujourd'hui, dans de nombreuses capitales, les autorités se demandent quels pourraient être les effets de la guerre cybernétique, comment protéger les citoyens et les entreprises, quels moyens utiliser, et ce, tout en prenant en compte un aspect qui est loin d'être négligeable: la dimension éthique de cette problématique.

Le gouvernement belge a également clairement indiqué que la cyberdéfense était l'une de ses priorités pour la prochaine législature. L'ambition est de développer davantage la cybercapacité de la Défense et de l'utiliser "au profit" de la société. D'aucuns évoquent même déjà des projets prudents en vue de créer une cybercomposante à part entière au sein de la Défense, afin de renforcer l'architecture de sécurité nationale. Un cadre légal devrait aussi être élaboré "pour empêcher toute intrusion étrangère malveillante dans nos infrastructures critiques".

Miser sur la sensibilisation, la détection et la résilience fait en effet partie de la solution. Mais nous considérons que les autorités doivent également œuvrer au renforcement de la capacité à répondre diplomatiquement et politiquement à de telles cyberopérations subversives étrangères.

Ce n'est un secret pour personne: certains acteurs tels que la Russie, la Chine, l'Iran et la Corée du Nord visent régulièrement les pays européens et de l'OTAN – y compris le nôtre – par des cyberopérations dommageables. Si l'on estime que ces quatre pays représentent 77 % de ces opérations, le lancement de cyberattaques ou leur parrainage par un État contre un autre est un phénomène de plus en plus fréquent. Depuis 2005, pas moins de trente-cinq pays sont suspectés de mener de telles opérations.

Il s'agit donc d'une option intéressante pour de nombreux régimes, dès lors que c'est un outil relativement bon marché qui peut causer d'importants dommages économiques, démocratiques, voire physiques, et que les agresseurs doivent rarement supporter les conséquences de leurs actes. La raison en est que la grande majorité des attaques étatiques consistent en des intrusions

TOELICHTING

DAMES EN HEREN,

In deze al maar digitalere wereld, waarbij steeds meer systemen gekoppeld worden en grote aspecten van ons leven virtueel beheerd worden, groeit ook de nood om onze kritieke infrastructuur en nationale belangen te vrijwaren van buitenlandse interferentie. In menig hoofdstad buigt men zich vandaag de dag over de vraag wat de mogelijke effecten zijn van cyberoorlogsvoering, hoe burgers en bedrijven dienen beschermd te worden, welke middelen kunnen ingezet worden en niet onbelangrijk de ethiek van dit alles.

Ook de Belgische regering maakte duidelijk dat cyberdefensie één van haar krachtlijnen is voor de komende legislatuur. De ambitie is er om de cybercapaciteit van Defensie verder uit te breiden en in te schakelen "ten voordele" van de samenleving. Er worden zelfs al voorzichtige plannen naar voren geschoven om een volwaardige cybercomponent binnen Defensie te creëren, die moet bijdragen tot het versterken van de nationale veiligheidsarchitectuur. Ook zou er een wettelijke regeling worden uitgewerkt die "het mogelijk moet maken om buitenlandse kwaadaardige inmenging in onze kritieke infrastructuren te verhinderen."

Inzetten op sensibilisering, detectie en weerbaarheid, zijn inderdaad deel van de oplossing. Maar wij zijn van oordeel dat de overheid ook werk moet maken van een versterking van de capaciteit om diplomatiek en politiek te kunnen reageren op zulke buitenlandse ondermijnende cyberoperaties.

Het is een publiek geheim dat actoren als Rusland, China, Iran en Noord-Korea bij regelmaat Europese en NAVO-landen – waaronder het onze – viseren met schadelijke cyberoperaties. Er wordt geschat dat deze vier landen goed zijn voor 77 % van zulke operaties, maar het lanceren van cyberaanvallen of hun sponsering door één staat tegen de andere wordt steeds gebruikelijker. Sinds 2005 worden maar liefst 35 landen ervan verdacht zulke operaties te ondernemen.

Het is dan ook een aantrekkelijke optie voor vele regimes, daar het een relatief goedkoop instrument is dat aanzienlijke economische, democratische tot zelfs fysieke schade kan toebrengen, maar waarvoor de aanvallers tegelijk slechts zelden de repercussies moeten dragen. Dit omdat de overgrote meerderheid van statelijke aanvallen bestaat uit aanhoudende maar

incessantes mais plutôt limitées, qui restent sous le seuil de ce qui pourrait engager la responsabilité des États en vertu du droit international.

Mais aussi parce qu'il est difficile d'identifier avec une certitude absolue l'origine exacte d'une cyberattaque, ce qui fait que de nombreux pays n'osent pas désigner leurs assaillants par crainte d'une escalade des tensions avec des États étrangers, avec pour conséquence que ces attaques ne donnent lieu à aucune réaction politique et que l'impunité règne dans une large mesure.

Aux niveaux international et européen, on débat toujours sur la question de savoir si ces cyberattaques constituent une violation de la souveraineté aux termes du droit international, où les limites doivent être fixées et quels codes de conduite doivent être imposés aux États dans le cyberespace.

Adopter une attitude purement défensive en essayant de protéger nos réseaux et notre liberté sur l'internet ne sera toutefois d'aucun profit pour l'ordre juridique international ni pour nos intérêts de sécurité nationale, dès lors que cela permettra aux cyberassaillants connus de poursuivre tranquillement leurs activités nuisibles. Nous devons oser aller plus loin. Nous constatons que des pays comme le Royaume-Uni, l'Australie, la France et les Pays-Bas ont déjà contribué à traduire dans une doctrine leur interprétation de la notion de souveraineté dans le cyberespace et de l'application du droit international. Et, depuis 2019, l'Union européenne encourage, elle aussi, ses États membres à dénoncer activement et publiquement les États étrangers qui parrainent des cyberattaques. Cette attitude plus assertive sera nécessaire pour dissuader nos assaillants et décourager leurs activités criminelles aussi longtemps que se poursuivra le débat sur l'application correcte et la portée du droit international dans le cyberespace.

C'est pourquoi l'élaboration d'un mécanisme de cyberattribution, c'est-à-dire de dénonciation publique de l'auteur d'une cyberattaque, devrait être une première étape cruciale pour notre pays dans le cadre de la réponse nationale à apporter à ce type d'attaques. L'élaboration d'options de réponse et la définition de limites claires concernant ces violations de notre souveraineté sont ainsi essentielles pour pouvoir apporter une réponse diplomatique à des cyberopérations indésirables d'origine étatique.

Il n'existe aucun procédé technique simple ni solution automatisée pour identifier les auteurs de cyberattaques hostiles. Mais cela ne signifie pas qu'il est impossible de le faire dès lors que chaque forme de cyberopérations laisse des traces et que de très nombreuses avancées technologiques ont par ailleurs été réalisées

eerder kleinschalige intrusies, die onder de drempel liggen van wat bij internationaal recht tot een statelijke aansprakelijkheid zou kunnen leiden.

Maar ook omdat het moeilijk is om met volle zekerheid de exacte bron van een cyberveiligheidsaanval te achterhalen. Wat vele landen ervoor doet terugschrikken om aanvallers aan te duiden uit vrees voor escalerende spanningen met buitenlandse staten. Met als gevolg dat een politieke reactie ook uitblijft en er in grote mate straffeloosheid heerst.

Internationaal en Europees woedt de discussie verder of zulke cyberoperaties volgens internationaal recht een soevereiniteitsschennis uitmaken, waar de limieten gezet moeten worden, en welke gedragscodes er nu juist aan landen in het cyberdomein opgelegd moeten worden.

Louter defensief proberen onze netwerken en onze vrijheid op het internet af te schermen zal de internationale rechtsorde en nationale veiligheidsbelangen echter niet ten goede komen. Want dan zetten de gekende spelers hun schadelijke activiteiten onverstoord verder. We moeten een stap verder durven zetten. We zien dat landen als het Verenigd Koninkrijk, Australië, Frankrijk en Nederland al hun bijdrage hebben geleverd om hun interpretatie van soevereiniteit in de cyberspace en toepasbaarheid van het internationaal recht in een doctrine te gieten. En ook de EU moedigt haar lidstaten sinds 2019 actief aan om aan "naming and shaming" te doen van buitenlandse staten die cyberveiligheidsaanvallen sponsoren. Deze assertievere houding is nodig om onze aanvallers af te schrikken en hun criminele activiteiten te ontmoedigen, zolang het debat voortloopt over de juiste toepassing en de reikwijdte van het internationaal recht in het digitale domein.

Het uitwerken van een mechanisme voor cyberattributie, of de publieke identificatie van de actor die verantwoordelijk is voor een cyberaanval, zou daarom voor ons land een cruciale eerste stap moeten zijn in het formuleren van een nationale reactie op dergelijke aanvallen. Het uitwerken van responsopties en het scherp stellen van lijnen voor deze inbreuken op onze soevereiniteit zijn dan weer essentieel om diplomatiek op te kunnen treden tegen ongewenste statelijke cyberoperaties.

Er is geen eenvoudig technisch proces of geautomatiseerde oplossing om de verantwoordelijkheid voor vijandige cyberoperaties te bepalen. Maar dat betekent niet dat het onmogelijk is, elke vorm van cyberoperatie laat een spoor achter en er is in de laatste jaren ook heel wat technologische vooruitgang geboekt. Met

ces dernières années. Le renforcement des capacités de la Défense dans le cyberespace devrait permettre aux analystes de l'État d'être davantage en mesure de recourir à l'analyse scientifique, à ses outils et à ses méthodes, pour désigner avec un certain degré de certitude les assaillants malveillants.

Depuis la loi NIS de 2019, les entreprises de notre pays qui fournissent des services vitaux dans six secteurs – l'énergie, les transports, la finance, les soins de santé, l'eau potable et les infrastructures numériques – sont également tenues de signaler de telles attaques au Centre pour la cybersécurité Belgique (CCB). Il est donc déjà procédé à une collecte systématique des informations sur les cyberattaques sur notre territoire.

Dans le cas de telles cyberattaques ou opérations, la Défense devrait pouvoir se baser sur un cadre clair et systématique pour les évaluations d'attribution permettant d'indiquer aux autorités l'identité probable de leurs auteurs, leurs motivations possibles, l'étendue et la gravité de l'incident, la solidité de la charge de la preuve et surtout l'implication d'une autorité étrangère.

À l'issue de cette enquête, il devrait également y avoir un volet politique approprié, les autorités décidant du sort à réserver aux informations recueillies et s'il y a suffisamment d'éléments pour procéder à une attribution publique de la cyberattaque contre sa souveraineté par un autre pays. Compte tenu du caractère sensible de la question, des arguments de preuve souvent indirects ou contextuels et des conséquences potentiellement importantes, le Parlement devrait également être associé à ce processus, afin de déterminer si l'on peut identifier les agresseurs avec un degré élevé de certitude et fournir une réponse proportionnée.

L'organisation d'un tel processus nécessite la mise en place d'un cadre juridique solide par les autorités. Il convient de développer une vision claire sur la manière dont le gouvernement interprète les principales règles du droit international qui s'appliquent dans le domaine numérique, sur les critères qu'il utilisera pour évaluer une cyberattaque étatique, sur les facteurs qu'il prendra en compte pour déterminer l'existence d'un lien entre l'agresseur et un État, sur la question de savoir s'il prendra en compte l'accumulation d'événements, sur ses options de réponse en cas de cyber-action indésirable perpétrée par un autre État et sur la manière dont il souhaite agir contre les agresseurs en coordination avec des États partageant les mêmes vues.

Par la présente résolution, nous voulons, d'une part, inviter le gouvernement, en collaboration avec le Parlement, à élaborer et à préciser un cadre permettant d'identifier les cyberattaques étatiques et de les

het versterken van de capaciteiten van Defensie in de cybersfeer zouden de analisten van de overheid in toenemende mate in staat moeten zijn om forensisch onderzoek te gebruiken om aan de hand van de tools en methoden de kwaadwillende actoren met een mate van zekerheid te kunnen aanduiden.

Sinds de NIS-wet van 2019 is er tevens al een meldplicht voor bedrijven in ons land bij het Centrum voor Cybersecurity (CCB) die vitale diensten leveren in zes sectoren: energie, vervoer, financiën, gezondheidszorg, drinkbaar water en digitale infrastructuur. Er is dus al een systematische instroom en vergaring van informatie over cyberaanvallen op ons grondgebied.

Bij zulke cyberaanvallen of operaties zou Defensie met een duidelijk en systematisch kader voor attributiebeoordelingen moeten kunnen werken dat aan de overheid kenbaar maakt wie de waarschijnlijke dader was, hun mogelijke motivatie, omvang en ernst van het incident, sterkte van de bewijslast en vooral de betrokkenheid van een buitenlandse overheid.

Aan het eind van dit onderzoek zou ook een gepast politiek luik moeten komen waarin de overheid beslist hoe om te gaan met de vergaarde informatie en of er voldoende elementen zijn waarop ze kan overgaan tot een publieke attributie van de cyberaanval op haar soevereiniteit door een ander land. Gezien de gevoeligheid van de materie, de vaak indirecte of contextuele bewijsargumenten en de potentieel verstrekkende gevolgen zou ook het Parlement in dit proces betrokken moeten worden, om na te gaan of ze met een grote mate van zekerheid haar aanvallers kan aanduiden en een proportionele respons kan geven.

Zulk een proces organiseren vereist een stevige juridische inbedding door de overheid. Er zou een duidelijke visie moeten ontwikkeld worden over hoe de regering de belangrijkste internationaalrechtelijke regels die gelden in het digitale domein interpreteert, welke criteria ze zal hanteren om een statelijke cyberaanval te beoordelen, met welke factoren ze rekening zal houden bij het vaststellen van het bestaan van een verband tussen de aanvaller en een staat, of ze accumulatie van gebeurtenissen zal hanteren, welke haar responsopties zijn bij ongewenst cyberoptreden door een andere staat en hoe ze gecoordineerd wenst op te treden met gelijkgezinde staten tegen de agressors.

Met deze resolutie willen we enerzijds de regering uitnodigen om samen met het Parlement over te gaan tot het uitwerken en verduidelijken van een kader om statelijke cyberaanvallen te kunnen aanwijzen en in een

sanctionner à un stade ultérieur; d'autre part, encourager également le gouvernement à nommer dans l'intervalle plus clairement les atteintes à notre souveraineté dans le domaine cybernétique perpétrées par d'autres pays ou leurs agents et à prendre les sanctions appropriées.

later stadium te bestraffen. Anderzijds ook de regering aanmoedigen om in tussentijd aantastingen van onze soevereiniteit op het cyberdomein door andere landen of hun proxies duidelijker te benoemen en de gepaste sancties te nemen.

Michael FREILICH (N-VA)
Peter BUYSROGGE (N-VA)
Theo FRANCKEN (N-VA)
Darya SAFAI (N-VA)

PROPOSITION DE RÉSOLUTION

La Chambre des représentants,

A. consciente de la difficulté d'attribuer des cyberattaques à des acteurs étatiques et des défis qui en découlent tant sur le plan technique que sur le plan politique;

B. prenant acte des rapports de consensus de 2010, 2013 et 2015 rédigés par le Groupe d'experts gouvernementaux des Nations Unies chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (GEG), qui stipulaient que les principes contenus dans la Charte des Nations Unies s'appliquent aux actions menées par des pays dans le cyberespace;

C. considérant que, bien que le cyberespace n'ait pas de frontières territoriales, une cyberattaque menée par un État peut être considérée comme une violation de la souveraineté d'un État, du principe de non-ingérence voire de l'intégrité territoriale ou de l'indépendance politique d'un État et donc comme une violation de l'article 2 (4) de la Charte des Nations Unies;

D. considérant que la majorité des cyberattaques menées par des États restent en deçà du niveau de violence à partir duquel l'article 51 de la Charte des Nations Unies reconnaît aux États le droit de légitime défense, individuelle ou collective, dans le cadre d'attaques conventionnelles;

E. considérant que lorsqu'un agresseur est identifié, l'État concerné peut également être tenu responsable en vertu des articles sur la responsabilité des États pour fait internationalement illicite (ARSIWA) figurant dans la résolution A/56/589 de l'Assemblée générale des Nations Unies;

F. considérant que l'accord du gouvernement De Croo dispose ce qui suit: "Les menaces ne s'arrêtent pas aux frontières. C'est aussi le cas des cybermenaces. Le gouvernement assurera la mise en œuvre effective de la directive sur la sécurité des réseaux et des systèmes d'information, un instrument important pour le renforcement des capacités de défense informatique de nos services essentiels. Un cadre légal sera aussi élaboré pour empêcher toute intrusion étrangère malveillante dans nos infrastructures critiques. Enfin, la coopération est essentielle pour assurer notre cybersécurité de manière efficace et coordonnée. Pour la gestion du cyber-renseignement et l'échange d'informations, nous veillerons à une coopération renforcée entre les services de sécurité et de renseignement, y compris la

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. bewust van de complexiteit van de attributie van statelijke cyberaanvallen en de uitdagingen die er zowel technisch als politiek mee gepaard gaan;

B. akte nemend van de consensusrapporten van de *UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (UN GGE) van 2010, 2013 en 2015 die bepaalden dat de principes uit het VN Charter van toepassing zijn op de acties van landen in de cyberspace;

C. overtuigd dat hoewel cyberspace geen territoriale grenzen heeft, een statelijke cyberaanval als een schending van de soevereiniteit van een staat, het beginsel van niet-interventie tot zelfs van de territoriale integriteit of politieke onafhankelijkheid van een staat kan worden aangemerkt en aldus een inbreuk uitmaakt van artikel 2 (4) van het VN-Handvest;

D. overwegende dat het gros van statelijke cyberaanvallen onder het geweldniveau blijven waar artikel 51 VN-Handvest bij conventionele aanvallen een staat het recht geven op individuele of collectieve zelfverdediging;

E. in aanmerking nemend dat bij identificatie van een aanvaller ook de betrokken staat kan worden verantwoordelijk gehouden onder de *Articles on the Responsibility of States for Internationally Wrongful Acts* (ARSIWA), die zijn opgenomen in resolutie A/56/589 van de Algemene Vergadering van de Verenigde Naties;

F. inroepende het regeerakkoord van De Croo dat stelt: "Dreigingen stoppen niet aan onze landsgrenzen. Dit geldt ook voor cyberdreiging. De regering verzekert de verdere effectieve implementatie van de Netwerk- en Informatiebeveiliging richtlijn, die een belangrijk instrument is om de cyberparaatheid van onze essentiële diensten te versterken. Er wordt tevens een wettelijke regeling uitgewerkt die het mogelijk moet maken om buitenlandse kwaadaardige inmenging in onze kritieke infrastructuren te verhinderen. Samenwerking ten slotte is essentieel om onze cyberveiligheid op een effectieve en gecoördineerde wijze te verzekeren. Voor het beheer van *cyber intelligence* en de uitwisseling van *cyber intelligence* informatie zorgen we voor een versterkte samenwerking tussen de veiligheids- en inlichtingendiensten, waarbij

coopération avec des organisations supranationales telles que l'OTAN. Le gouvernement renforcera la résilience de notre pays en cas de crise nationale ou internationale, et s'appuiera à cette fin sur une forte coordination avec tous les acteurs concernés.";

G. constatant que tant l'exposé d'orientation politique que la note de politique générale de la ministre de la Défense, Ludivine Dedonder, préconisent de déployer plus largement la capacité cyber de la Défense au profit de la société et de confier un rôle clairement prépondérant à la Défense dans la stratégie déployée par le gouvernement pour défendre notre souveraineté dans le domaine cybernétique;

H. invoquant le passage suivant extrait de l'exposé d'orientation politique et de la note de politique générale de la Défense: "Alors que le plan de relance et de transition interfédéral identifie la cybersécurité comme l'un des domaines prioritaires, la Défense approfondira significativement sa capacité cyber, ce qui devrait à terme se traduire par la création d'une composante à part entière. En premier lieu, la cybercapacité existante au sein du service de renseignement militaire devra être encore renforcée. À cette fin, la Défense examinera comment recruter plus facilement des cyberprofils hautement spécialisés et quelles mesures sont nécessaires pour en améliorer la rétention. En outre, des investissements complémentaires garantiront que la cybercapacité continue de disposer de ressources modernes et adaptées. À partir de cette cybercapacité renforcée au sein du SGRS, une composante cyber de la Défense peut être développée à un horizon de cinq ans, sans affaiblir la capacité de cyber-renseignement du SGRS. Les opérations de la future composante Cyber pourront aller au-delà de la cyberdéfense et nécessitent un cadre juridique qui sera créé au cours de cette législature.";

I. relevant le hiatus dans la stratégie du gouvernement et faisant observer qu'en plus d'investir les moyens qui s'imposent dans les capacités cyber et de renseignement, le gouvernement devra également développer des processus politiques et administratifs afin de pouvoir attribuer correctement et efficacement les cyberattaques perpétrées à l'encontre de sa souveraineté;

J. renvoyant au processus permanent de Tallinn mené par l'OTAN et à la publication qui en découle – le "Manuel de Tallinn 2.0 sur l'applicabilité du droit international à la guerre cybernétique" – qui a été facilitée par le Centre d'excellence de cyberdéfense coopérative de l'OTAN (CCDCOE) et est parue en 2017 avec une analyse juridique des cyberincidents les plus fréquents et un spectre complet du droit international applicable aux cyberopérations;

ook samenwerking met supranationale organisaties zoals NAVO versterkt wordt. De regering zal de weerbaarheid van ons land in geval van nationale of internationale crisissen versterken en daarvoor inzetten op een sterke coördinatie met alle betrokken actoren";

G. constaterend dat zowel de beleidsverklaring als de beleidsnota van minister van Defensie Ludivine Dedonder een bredere inzet van de cybercapaciteit van Defensie ten voordele van de samenleving bepleiten en een duidelijke hoofdrol voor Defensie naar voren schuiven in de strategie van de regering tot verdediging van onze soevereiniteit in het cyberdomein;

H. inroepende volgende passage uit de beleidsverklaring en beleidsnota Defensie: "Terwijl het relance en het interfederaal transitieplan cybersecurity identificeert als een van de prioritaire domeinen, zal Defensie haar cybercapaciteit aanzienlijk verdiepen, wat zich op termijn moet vertalen in de creatie van een volwaardige component. In eerste instantie zal de bestaande cybercapaciteit binnen de militaire inlichtingendienst nog moeten versterkt worden. Hiervoor zal Defensie nagaan hoe gemakkelijker hooggespecialiseerde cyberprofielen aan te werven en welke maatregelen nodig zijn om de retentie te verbeteren. Bovendien zullen bijkomende investeringen een garantie bieden dat de cybercapaciteit verder zal kunnen beschikken over moderne en aangepaste middelen. Vertrekkende van deze cybercapaciteit binnen de ADIV kan een cybercomponent ontwikkeld worden binnen een horizon van vijf jaar, zonder de capaciteit cyberinlichtingen van de ADIV te verzwakken. De operaties van de toekomstige cybercomponent kunnen gaan boven cyberdefensie en noodzaken een wettelijk kader dat zal aangemaakt worden tijdens deze legislatuur.";

I. attenderend op het hiaat in de strategie van de regering en opmerkende dat er naast de nodige investeringen in cyber- en inlichtingencapaciteiten er ook dient gewerkt te worden aan politieke en administratieve processen om de vastgestelde cyberaanvallen op haar soevereiniteit correct en effectief te kunnen attribueren;

J. refererend naar het doorlopende proces van Talinn dat de NAVO onderneemt en de hieruit voortvloeiende publicatie "Tallinn Manual 2.0 *on the International Law Applicable to Cyber Operations*" dat werd gefaciliteerd door het *NAVO Cooperative Cyber Defence Center of Excellence* (CCDCOE) en gepubliceerd in 2017 met een juridische analyse van de meest voorkomende cyberincidenten en een volledig spectrum van internationaal recht dat van toepassing is op cyberoperaties;

K. soulignant qu'en mai 2019, le Conseil de l'Union européenne a adopté, dans le cadre de la Politique étrangère et de sécurité commune (PESC) – Décision PESC 2019/797 et Règlement UE 2019/796 du Conseil –, une boîte à outils mieux connue sous la dénomination "*EU Cyber Diplomacy Toolbox* (CDT)";

L. signalant que la CDT prévoit notamment ce qui suit: les attributions relèvent d'une décision politique souveraine des États membres; l'attribution peut être communiquée et accompagnée d'une réaction diplomatique; les États membres de l'Union européenne peuvent coordonner l'attribution au niveau de l'Union européenne; et, en conséquence, il peut être décidé conjointement de geler des fonds et d'imposer des restrictions en matière de déplacements aux personnes physiques et morales directement responsables de cyberattaques constituant une menace extérieure pour l'Union;

M. observant que, pour imposer des sanctions, le Conseil a besoin d'un niveau d'attribution aussi précis que possible, fondé sur des preuves numériques légales, qui permette de constater une violation du cadre CDT établi en 2019;

N. rappelant que, le 30 juillet 2020, le Conseil de l'Union européenne a imposé à l'unanimité, pour la première fois, des mesures restrictives à six personnes et à trois entités – règlement UE 2020/1125 du 30 juillet 2020 – jugées responsables de la cyber-opération contre l'Organisation pour l'interdiction des armes chimiques, des attaques *WannaCry et NotPetya* et de l'opération *Cloud-Hopper*;

O. considérant que le ministère allemand des Affaires étrangères a annoncé, le 28 mai 2020, qu'il souhaitait recourir aux "cyber-sanctions" de l'Union européenne dans l'affaire à l'encontre de l'officier de renseignement militaire russe Dmitri Sergeyevich Badin et de toute autre personne impliquée dans le piratage du Bundestag en 2015;

P. considérant que, dans une communication officielle de la Commission au Parlement européen et au Conseil du 13 juin 2018 – JOIN (2018) 16 final –, Mme Frederica Mogherini, Haute représentante de l'Union européenne, a encouragé les pays de l'Union européenne à désigner les États étrangers commanditant des cyberattaques de sécurité en les dénonçant (selon le principe "*naming and shaming*") et a affirmé que "l'UE et ses États membres doivent renforcer leur capacité à attribuer l'origine des cyberattaques, notamment en améliorant l'échange de renseignements. L'attribution de l'origine dissuaderait les agresseurs potentiels d'agir et augmenterait les chances que les responsables d'attaques répondent dûment de leurs actes.";

K. aanstippende dat in mei 2019, door de Raad van de Europese Unie, een instrument aangenomen werd binnen het Gemeenschappelijk Buitenlands en Veiligheidsbeleid (GBVB) – Besluit GBVB 2019/797 en Verordening EU 2019/796 van de Raad – beter gekend onder de naam *EU Cyber Diplomacy Toolbox* (CDT);

L. signalerende dat de CDT onder meer bepaalt dat: toewijzingen een soevereine politieke beslissing van de lidstaten zijn, attributie kan meegedeeld en vergezeld worden van een diplomatieke reactie, EU-lidstaten attributie op EU-niveau kunnen coördineren en dat als gevolg hiervan de gezamenlijke beslissing kan genomen worden om tegoeden te bevriezen en reisverboden op te leggen aan natuurlijke personen en rechtspersonen die rechtstreeks verantwoordelijk zijn voor cyberaanvallen die een externe dreiging voor de Unie vormen;

M. opmerkende dat om sancties te kunnen opleggen, de Raad een zo nauwkeurig mogelijk toeschrijvingsniveau, dat gebaseerd is op digitaal forensisch bewijs, nodig heeft om een inbreuk vast te stellen van het in 2019 vastgestelde kader van de CDT;

N. inroepende dat op 30 juli 2020 de Raad van de Europese Unie voor het eerst unaniem beperkende maatregelen heeft opgelegd tegen zes personen en drie entiteiten – Verordening EU 2020/1125 van 30 juli 2020 – die verantwoordelijk werden bevonden bij de cyberoperatie tegen de Organisatie voor het Verbod op Chemische Wapens, de *WannaCry- en NotPetya*-aanvallen en Operatie *Cloud-Hopper*;

O. gezien het Duitse ministerie van Buitenlandse Zaken op 28 mei 2020 liet weten dat ze gebruik wenst te maken van de zogenaamde EU-cybersancties in de zaak tegen de Russische militaire inlichtingenofficier Dmitriy Sergejevitsj Badin en iedereen anders die betrokken is bij de hack van de Bundestag in 2015;

P. gelet dat de Hoge Vertegenwoordiger van de EU, Frederica Mogherini, in een officiële communicatie van de commissie aan het Europees Parlement en de Raad op 13 juni 2018 – JOIN (2018) 16 final – de EU-landen aangemoedigd heeft om buitenlandse staten die cyberveiligheidsaanvallen sponsoren, aan te duiden door "*naming and shaming*" en dat "de EU en haar lidstaten moeten hun capaciteit om cyberaanvallen toe te schrijven, verbeteren, niet in de laatste plaats door het delen van informatie. Attributie zou potentiële agressors afschrikken en de kans vergroten dat de verantwoordelijken naar behoren verantwoording afleggen"*;*

Q. vu le *Guide to Cyber Attribution* publié le 14 septembre 2018 par le *US Office of the Director of National Intelligence*;

R. renvoyant à la lettre sur l'ordre juridique international dans le domaine numérique adressée par le gouvernement néerlandais à la Deuxième chambre des Pays-Bas le 5 juillet 2019 *(Kamerstuk 33 694, n° 47)* dans laquelle le gouvernement néerlandais expose sa conception des dimensions internes et externes de la souveraineté dans le cyberespace;

S. s'inspirant de la déclaration du ministère français des Armées de septembre 2019 intitulée "Droit international appliqué aux opérations dans le cyberespace", dans laquelle il expose une interprétation détaillée et cohérente du droit international applicable au cyberespace et établit déjà une liste non exhaustive de facteurs permettant d'identifier et de constater l'existence d'un lien entre l'instigateur d'une attaque et un État, et prescrit une doctrine fondée sur l'accumulation des événements;

T. avertissant que, dans son rapport du 4 août 2020, INTERPOL observe, dans le contexte de la crise COVID-19, une augmentation spectaculaire de la cybercriminalité, criminalité qui cible aujourd'hui nettement moins les individus et les petites entreprises que les grandes entreprises, les pouvoirs publics et les infrastructures critiques;

U. considérant qu'il ressort de la réponse à une question adressée au premier ministre Alexander De Croo par la députée Katrien Houtmeyers (N-VA) le 28 octobre 2020 (55009190C) que le nombre de cyberattaques est en constante augmentation en Belgique et qu'en septembre 2020, le Centre pour la Cybersécurité Belgique avait déjà reçu, pour l'année 2020, 5 387 signalements de cyberattaques ou de cyberincidents visant des citoyens, des entreprises et des partenaires;

V. observant que, dans la banque de données *Cyber Operations Tracker* de l'organisation *Council on Foreign Relations*, la Belgique a déjà été enregistrée, depuis 2013, pas moins de neuf fois en tant que victime potentielle d'une cyberattaque visant un État dans le cadre des opérations *PLA Unit 61398, Red October, The Dukes, Regin, Machete, APT 28, Axiom, Project Sauron* et *APT 3*;

W. observant que le SPF Affaires étrangères a été victime de cyberattaques avancées en 2011, en 2014 et en 2017 et que des infections similaires ont été observées en février et en avril 2018 ainsi qu'en mars 2019;

Q. notitie nemend van "*A Guide to Cyber Attribution*", gepubliceerd door de *US Office of the Director of National Intelligence* op 14 September 2018;

R. verwijzend naar de Kamerbrief van 5 juli 2019 van de Nederlandse regering over Internationale rechtsorde in het digitale domein (Kamerstuk 33 694, nr. 47) waarin ze haar visie over de interne en externe aspecten van soevereiniteit in het cyberdomein uiteenzet;

S. geïnspireerd door de Franse verklaring van het *Ministère des Armées* van september 2019 "*Droit International Applique Aux Operations Dans Le Cyberspace*" dat een gedetailleerde en coherente interpretatie geeft van het internationaal recht dat van toepassing is op de cyberspace en waarin het al werk maakt van een niet-uitputtende lijst van factoren voor de identificatie en het vaststellen van het bestaan van een verband tussen de aanvaller en een staat en het een doctrine van accumulatie van gebeurtenissen voorschrijft;

T. waarschuwend dat INTERPOL in haar rapport van 4 augustus 2020 een dramatische stijging noteert van cybercriminaliteit in het licht van de COVID-19-crisis waarbij er ook een aanzienlijke verschuiving van het doelwit is van individuen en kleine bedrijven naar grote bedrijven, overheden en kritieke infrastructuur;

U. inroepende dat uit een vraag van N-VA Kamerlid Katrien Houtmeyers aan eerste minister Alexander De Croo op 28 oktober 2020 ((55009190C) blijkt dat het aantal cyberaanvallen in dit land in stijgende lijn is en dat het Centrum voor Cybersecurity België tegen september al 5 387 meldingen over cyberaanvallen en -incidenten tegen burgers, bedrijven en partners voor het jaar 2020 ontvangen heeft;

V. bemerkende dat *Cyber Operations Tracker* van de organisatie "*Council on Foreign Relations*" sinds 2013 België tot negenmaal toe registreert als een mogelijk slachtoffer van een statelijke cyberaanval bij operaties: *PLA Unit 61398, Red October, The Dukes, Regin, Machete, APT 28, Axiom, Project Sauron en APT 3*;

W. opmerkende dat zowel in 2011, 2014, 2017 de FOD Buitenlandse Zaken het slachtoffer van geavanceerde cyberaanvallen. En soortgelijke besmettingen werden vastgesteld in februari en april 2018, alsook in maart 2019;

X. rappelant les cyberattaques massives auxquelles la mission économique belge en Chine a été confrontée en novembre 2019, dont le nombre a atteint jusque 135 attaques à l'heure,

Demande au gouvernement fédéral:

1. de témoigner d'une propension accrue à identifier clairement les attaques organisées par des États étrangers, à dissuader de futures cyberattaques et à agir contre l'impunité internationale;

2. de recourir à la *Cyber Diplomacy Toolbox* (CDT) de l'UE afin de prendre des sanctions en temps utile;

3. à l'instar des Pays-Bas, de la France et de l'Estonie, notamment, d'effectuer une déclaration sur l'application des principes de souveraineté et de non-ingérence et sur l'application du droit international dans le cyberespace;

4. d'établir un cadre de réponse clair sur ce qui caractérise une cyberattaque étatique, la classification des différentes intrusions, les contre-mesures potentielles et les possibilités d'attribution publique de ces atteintes à notre souveraineté;

5. d'élaborer, de concert avec la Chambre des représentants, un système d'attribution politique des attaques;

6. d'œuvrer au renforcement de ce cadre de réponse dans les contextes de l'Union européenne et de l'OTAN et avec les pays partageant les mêmes vues.

14 janvier 2021

X. herinnerende aan de massale cyberaanvallen waarmee Belgische Economische Missie in China in november 2019 werd geconfronteerd met zelfs tot 135 aanvallen per uur,

Verzoekt de federale regering:

1. een grotere bereidheid te tonen om buitenlandse staatsgeorganiseerde aanvallen duidelijk aan te wijzen, om toekomstige cyberaanvallen te ontraden en op te treden tegen de internationale straffeloosheid;

2. gebruik te maken van de *EU Cyber Diplomacy Toolbox* (CDT) om tijdig over te kunnen gaan tot het nemen van sancties;

3. naar voorbeeld van onder andere Nederland, Frankrijk en Estland een statement maken over de toepassing van de principes van soevereiniteit, non-interventie en de toepassing van internationaal recht in cyberspace;

4. een duidelijk responskader te creëren over wat het aanmerkt als een statelijke cyberaanval, classificatie van de diverse intrusies, potentiële tegenmaatregelen en mogelijkheden tot publieke attributie van deze inbreuken op onze soevereiniteit;

5. met de Kamer van volksvertegenwoordigers een regeling uit te werken voor de uiteindelijke politieke attributie van aanvallen;

6. te streven naar de versterking van dit responskader in EU- en NAVO verband en met gelijkgezinde landen.

14 januari 2021

Michael FREILICH (N-VA)
Peter BUYSROGGE (N-VA)
Theo FRANCKEN (N-VA)
Darya SAFAI (N-VA)

Imprimerie centrale – Centrale drukkerij