DOC 55 **2167/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

30 août 2021

PROPOSITION DE RÉSOLUTION

relative à la protection de notre sécurité nationale et de notre indépendance stratégique contre les cyberattaques étrangères grâce à l'établissement d'une liste de fournisseurs à haut risque

(déposée par M. Michael Freilich et consorts)

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

30 augustus 2021

VOORSTEL VAN RESOLUTIE

betreffende het beschermen van onze nationale veiligheid en strategische onafhankelijkheid tegenover buitenlandse cyberaanvallen door het opstellen van een lijst van hoogrisicoleveranciers

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

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

S'il est vrai que l'espionnage a toujours existé, les acteurs étatiques ont largement déplacé cette activité, dans notre univers toujours plus connecté, du monde physique à la sphère numérique. En effet, les autorités publiques s'efforcent de collecter, par différents moyens, des informations susceptibles de leur apporter un avantage stratégique, compétitif, militaire ou économique.

L'omniprésence d'appareils électroniques dans notre environnement accroît également le risque d'espionnage et d'abus de nos réseaux. La présente proposition de résolution entend dès lors empêcher, autant que possible, toute pénétration dans nos réseaux et toute collecte de données, à l'aide de matériel informatique ou de logiciels courants, au sein de l'administration et des entreprises gérant des infrastructures critiques. Pour y parvenir, notre pays devra prendre certaines mesures, par exemple établir une liste des "fournisseurs" de produits informatiques "à haut risque" qui permette de limiter ou d'interdire totalement de recourir à ceux-ci.

Maillon faible

Les entreprises, les services publics et les sociétés ne vivent pas en vase clos. En effet, pour assurer leur fonctionnement, ils font appel à du personnel et leur personnel constitue souvent le maillon faible qui permet aux pirates informatiques d'infiltrer leurs réseaux. Nous songeons par exemple aux personnes qui se connectent à un réseau à domicile ou aux travailleurs et aux collaborateurs qui consultent leur courrier électronique à distance sur une tablette ou un smartphone. Lorsque ces appareils sont compromis, des pirates peuvent s'infiltrer dans les réseaux d'entreprises et de services publics. Mais même lorsque le réseau d'une entreprise est suffisamment sécurisé, des pirates peuvent exploiter des informations sensibles contenues dans les appareils d'utilisateurs individuels pour les obliger à leur donner accès à des informations sensibles. En d'autres termes, les appareils privés du personnel de la Défense, des autorités publiques, de toute infrastructure critique ou de toute entreprise d'intérêt stratégique ou économique national, notamment, constituent des cibles potentielles pour les acteurs étatiques étrangers.

Par "infrastructures critiques" et "entreprises d'intérêt stratégique ou économique national", nous entendons les entreprises et les secteurs considérés comme des

TOELICHTING

DAMES EN HEREN,

Spionage is van alle tijden, maar in onze steeds verder geconnecteerde digitale wereld hebben statelijke actoren hun actieterrein grotendeels verlegd van het fysieke naar het digitale domein. Overheden proberen op allerhande manieren informatie te verzamelen die hen een strategisch, competitief, militair of economisch voordeel kunnen opleveren.

Doordat digitale apparatuur overal rondom ons aanwezig is, verhoogt ook het risico op spionage en misbruik van onze netwerken. Deze resolutie wil de penetratie van netwerken en het vergaren van data via alledaagse hard- en softwareproducten binnen de overheid en bij bedrijven van kritieke infrastructuren zoveel mogelijk belemmeren. Hiervoor moet ons land bepaalde maatregelen nemen, zoals het beperken van of het totaal verbannen van zogenaamde "hoog-risicoleveranciers" van digitale producten door middel van het opstellen van een lijst die hen identificeert

Zwakste schakel

Ondernemingen, overheden en bedrijven leven niet in het luchtledige. Om deze draaiende te houden wordt personeel ingezet en dat personeel vormt vaak de zwakke schakel die hackers toelaten om netwerken te infiltreren. Personen die van thuis uit inloggen op het netwerk, werknemers en medewerkers die vanop afstand hun e-mail nakijken via hun tablet of smartphone. Als deze apparaten gecompromitteerd worden, kunnen hackers via die weg bedrijfs- en overheidsnetwerken infiltreren. Maar ook indien een bedrijfsnetwerk voldoende afgeschermd is, kunnen individuele gebruikers, via gevoelige informatie op hun apparaten, afgeperst worden om hackers alsnog toegang te verschaffen tot gevoelige informatie. Met andere woorden, de privé toestellen van individuen die professioneel actief zijn voor onder andere het leger, de overheid, een kritieke instelling, een bedrijf van nationaal strategisch of economisch belang, vormen potentiële doelwitten voor buitenlandse statelijke actoren.

Voor wat onder een "kritieke instellingen" of een "bedrijf van nationaal strategisch of economisch belang" valt kijken we naar bedrijven en sectoren die onder de

"opérateurs de services essentiels" au regard de la loi relative à la sécurité des réseaux et des systèmes d'information (loi NIS)[1].

Ces opérateurs de services essentiels doivent opérer dans l'un des secteurs suivants: énergie, transports, finances, santé, eau potable ou infrastructures numériques. En outre, ils doivent remplir les conditions suivantes:

— fournir un service essentiel au maintien d'activités sociétales et/ou économiques critiques;

— fournir un service tributaire des réseaux et des systèmes d'information;

— et un incident les concernant doit être susceptible d'avoir un effet perturbateur important.

Par ailleurs, un grand nombre d'appareils sont aujourd'hui déjà utilisés par les services publics, les institutions et les entreprises sans que personne ne se soit interrogé, lors de leur achat, sur les risques liés à leur utilisation. Il s'agit par exemple de télévisions intelligentes, d'imprimantes, de caméras, de systèmes sonores, de drones et d'une liste de centaines d'autres appareils connectés au web et pouvant donc servir de points d'entrée à partir desquels des pirates peuvent pénétrer dans les réseaux des entreprises.

Au cours des auditions visant "les cyberattaques sur les systèmes informatiques de l'État et des services publics" organisées par la commission de l'Intérieur de la Chambre des représentants le 22 juin 2021, plusieurs orateurs, notamment M. Miguel De Bruycker, directeur du *Center for Cybersecurity Belgium* (CCB), et M. Frédéric Van Leeuw, procureur fédéral, ont fait observer qu'une culture de la cybersécurité faisait clairement défaut dans notre pays, et que son absence aggravait encore notre vulnérabilité.

Nous souhaitons dès lors que la Belgique établisse, d'une part, une liste de fournisseurs à haut risque de produits informatiques et, d'autre part, une liste des personnes et des institutions pouvant être considérés comme des cibles potentielles et n'étant dès lors pas autorisés à utiliser ces produits dans le cadre de leurs activités professionnelles ou sur leurs réseaux respectifs.

Contexte

En mai 2021, la Belgique a été victime d'une attaque DDoS (*Distributed Denial of Service*) dirigée contre des

[1] 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.

wet inzake netwerk- en informatiebeveiliging (NIS-wet)[1] geklasseerd worden als 'aanbieders van essentiële diensten".

Aanbieders van essentiële diensten moeten actief zijn in één van de volgende sectoren: energie, transport, financiering, gezondheidszorg, drinkwater of digitale infrastructuren én tevens aan de volgende criteria voldoen:

— een dienst bieden die essentieel is voor het handhaven van kritieke maatschappelijke en/of economische activiteiten;

— een dienst bieden die vertrouwt op netwerk- en informatiesystemen;

— en een significant verstorend effect hebben wanneer zich een incident zou voordoen.

In tweede instantie zijn er een resem apparaten die vandaag reeds in gebruik zijn genomen bij overheden, instellingen en bedrijven en waar men bij de aankoop niet heeft stilgestaan bij de daaraan verbonden risico's. Het gaat dan bijvoorbeeld om slimme televisies, printers, camera's, geluidssystemen, drones en een lijst van wel honderden andere apparaten die verbonden zijn met het internet en aldus een toegangspoort kunnen bieden waarlangs hackers het bedrijfsnetwerk kunnen penetreren.

Tijdens de hoorzittingen over "de cyberaanvallen op het IT-systeem van de Staat en de overheidsdiensten", georganiseerd in de commissie Binnenlandse Zaken in de Kamer van volksvertegenwoordigers op 22 juni 2021, zeiden verschillende sprekers waaronder de heer Miguel De Bruycker, directeur van het "*Center for Cybersecurity Belgium*" (CCB) en federaal procureur Frédéric Van Leeuw, dat het in ons land duidelijk aan een cultuur van cyberveiligheid ontbreekt waardoor we extra kwetsbaar zijn.

Wij willen daarom dat ons land enerzijds een lijst opstelt van hoogrisicoleveranciers van digitale producten en anderzijds een lijst opstelt van personen en instellingen die als potentieel doelwit kunnen worden aanzien en om die reden geen gebruik mogen maken van deze producten tijdens hun professionele activiteiten en op hun netwerk.

Achtergrond

In mei 2021 werd ons land getroffen door een zogenaamde DDoS aanval tegen Belgische overheidswebsites.

[1] Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

sites publics belges et très probablement orchestrée par des acteurs étatiques. Quelques semaines plus tard, il est apparu que les réseaux du Service public fédéral Intérieur avaient certainement été espionnés durant deux ans.

Le 1er juin 2021, le journal *De Tijd* a évoqué un risque grandissant de cyberguerres[2]. Selon le *Cyber Operations Tracker* du *Council on Foreign Relations* américain, trente-quatre pays sont soupçonnés d'avoir financé des cyberopérations depuis 2005. Et pour de nombreux pays, il est aujourd'hui plus intéressant d'investir dans les technologies d'espionnage et les outils cybernétiques que dans le développement d'armes militaires traditionnelles. Au premier rang de ceux-ci figurent la Chine, la Russie, l'Iran et la Corée du Nord.

Depuis plusieurs décennies, la Chine investit dans la formation de toute une armée spécialisée dans les technologies de l'information afin de pratiquer de l'espionnage industriel à l'étranger. Les données, la propriété intellectuelle et les secrets d'affaires collectés par les pirates lui ont permis de se hisser au rang de deuxième économie mondiale. Les pays comme la Russie, la Corée du Nord ou l'Iran sont quant à eux plus connus pour une stratégie à court terme visant surtout une démonstration de force. Ces pays procèdent également, de plus en plus souvent, à la manipulation active de données et au sabotage de réseaux d'infrastructures critiques.

Nous songeons par exemple aux attaques russes contre le réseau électrique en Ukraine. Il suffit de laisser libre cours à son imagination pour envisager les dégâts pouvant être causés par toute personne dont l'objectif n'est pas seulement de saboter des réseaux, mais bien de faire effectivement autant de victimes humaines que possible. La modification de la composition des stations d'épuration, des barrages ou des infrastructures nucléaires peut avoir des conséquences catastrophiques. Chaque jour, on prend donc de plus en plus conscience de leurs conséquences potentielles pour la politique, l'économie et la société.

Il est dès lors parfaitement justifié que la cybersécurité s'invite de plus en plus dans les débats, y compris au cours de la concertation diplomatique sur la scène internationale. En outre, il ne faut pas s'étonner qu'un nombre croissant de pays entreprennent des actions afin de mieux sécuriser leur cyberespace et de tenter d'exclure les menaces le plus possible. Les États-Unis ont par exemple établi une liste noire d'entreprises qui

[2] *De Tijd*, 1 juin 2021, "geopolitieke machtsstrijd almaar meer uitgevochten in cyberspace".

Een aanval die hoogst waarschijnlijk door statelijke actoren werd opgezet. Enkele weken later kwam aan het licht dat de netwerken van de federale overheidsdienst Binnenlandse Zaken zeker twee jaar lang bespioneerd werden.

Op 1 juni 2021 berichtte de krant *De Tijd* over het steeds groter wordende gevaar van cyberoorlogen[2]. Volgens de *Cyber Operations Tracker* van de Amerikaanse *Council on Foreign Relations* worden 34 landen ervan verdacht sinds 2005 cyberoperaties gefinancierd te hebben. Voor vele landen is het interessanter geworden om te investeren in spionagetechnologie en cybertools, eerder dan het ontwikkelen van traditionele militaire wapens. Koplopers hierin zijn China, Rusland, Iran en Noord-Korea.

China zet al enkele decennia in op het opleiden van een heel IT leger om aan industriële spionage te doen in het buitenland. Met behulp van data, intellectuele eigendom en bedrijfsgeheimen die de hackers verzamelden, zijn zij erin geslaagd om op te klimmen tot de tweede economie van de wereld. Landen als Rusland, Noord-Korea of Iran staan eerder gekend voor een korte termijn strategie, waarbij het vooral gaat over machtsvertoon. Zij gaan ook steeds vaker over tot actieve manipulatie van gegevens en sabotage aan netwerken van kritieke infrastructuur.

Denk bijvoorbeeld aan de Russische aanvallen op het elektriciteitsnetwerk in Oekraïne. Je moet je verbeelding maar de vrije loop laten om te bedenken wat voor schade iemand kan aanrichten als het doel niet enkel is om netwerken te saboteren, maar om effectief zoveel mogelijk menselijke slachtoffers te maken. Het aanpassen van de samenstelling in waterzuiveringsinstallaties, waterdammen of nucleaire infrastructuur kan catastrofale gevolgen hebben. Het besef over mogelijke consequenties voor de politiek, economie en maatschappij groeit dus met de dag.

Het is dan ook absoluut terecht dat cyberveiligheid een steeds meer besproken onderwerp wordt, ook tijdens internationaal diplomatiek overleg. Het mag bovendien niet verbazen dat steeds meer landen actie ondernemen om hun cyberspace beter te beveiligen en proberen dreigingen zoveel mogelijk uit te sluiten. De Verenigde Staten hanteren bijvoorbeeld een zwarte lijst van ondernemingen die banden zouden hebben met het

[2] *De Tijd*, 1 juni 2021, "geopolitieke machtsstrijd almaar meer uitgevochten in cyberspace".

entretiendraient des liens avec l'armée chinoise, et ils interdisent aux Américains de continuer à investir dans ces entreprises. Le 4 juin 2021, le journal *De Standaard*[3] rapportait que le géant du secteur des technologies Huawei avait également été ajouté à cette liste.

Des actions sont également menées en Europe. Dans le cadre du déploiement de la 5G, plusieurs États membres de l'Union européenne se sont dotés de dispositions légales pour éviter que ces infrastructures critiques tombent entre de mauvaises mains. À cet effet, ils se sont basés sur la boîte à outils 5G de la Commission européenne que les États membres doivent mettre en œuvre. Les fournisseurs d'équipements de réseaux pouvant être considérés comme des fournisseurs à haut risque, appelés "*High Risk Vendors*", ne sont pas autorisés à accéder aux parties cruciales des réseaux.

Étranger

Le 3 février 2021, le ministère néerlandais de la Justice et de la Sécurité a publié un rapport intitulé *Dreigingsbeeld Statelijke Actoren (Évaluation de la menace des acteurs étatiques*), où on lit:

"Les acteurs étatiques ne jouent pas toujours à armes égales, par exemple dans le cyberespace. La Chine et la Russie disposent de capacités, de connaissances et d'une expertise tellement importantes que lorsque ces acteurs souhaitent pénétrer quelque part par la voie numérique, leurs chances de réussite sont élevées. Il est possible de réduire leurs chances de succès en prenant des contre-mesures.". (traduction)

Ce rapport indique que les menaces d'espionnage visent la sécurité territoriale, la sécurité économique, la stabilité sociale et politique et l'ordre juridique international du pays. Selon ce rapport, l'espionnage et les techniques de piratage mis en œuvre par les acteurs étatiques se concentrent principalement sur: les hauts potentiels, les institutions et les fonctionnaires de l'État de droit démocratique, les organes consultatifs, les établissements d'enseignement, la science (enseignement supérieur et universitaire), les groupes de réflexion et les centres de connaissance (y compris les centres de recherche [appliquée]), la société civile, les organisations internationales, les entreprises et les secteurs d'excellence, les infrastructures vitales et les organisations internationales cruciales comme l'Union européenne et l'OTAN.

Au cours du discours qu'il a prononcé au *Hudson Institute* le 7 juillet 2020, le directeur du FBI des États-Unis, Christopher Wray, a fait la déclaration suivante:

[3] *https://www.standaard.be/cnt/dmf20210604_91153942*

Chinese leger. Het is voor Amerikanen verboden om nog langer te investeren in deze bedrijven. Op 4 juni 2021 berichtte De Standaard[3] nog dat ook technologiegigant Huawei aan de lijst werd toegevoegd.

Ook in Europa wordt er actie ondernomen. In het kader van de uitrol van 5G hebben verschillende Europese lidstaten wetgeving aangenomen om ervoor te zorgen dat deze kritieke infrastructuur niet in de foute handen kan terechtkomen. Ze baseren zich hiervoor op de 5G toolbox van de Europese Commissie, die lidstaten moeten ten uitvoer leggen. Aanbieders van netwerkapparatuur die als hoog-risico leveranciers aanzien worden, de zogenaamde *High Risk Vendors*, mogen dan geen toegang krijgen tot cruciale onderdelen van het netwerk.

Buitenland

Het Nederlandse ministerie van Justitie en Veiligheid publiceerde op 3 februari 2021 een rapport genaamd Dreigingsbeeld Statelijke Actoren.

Daarin lezen we: "Het speelveld van statelijke actoren is niet altijd gelijk. Dit is bijvoorbeeld zichtbaar op het gebied van cyber. De capaciteit, kennis en expertise van China en Rusland zijn dermate groot, dat wanneer deze actoren ergens digitaal binnen willen dringen, de slagingskans groot is. Deze slagingskans kan met het nemen van tegenmaatregelen kleiner worden gemaakt.".

De dreigingen van spionage manifesteren zich volgens het rapport tegen de territoriale veiligheid, de economische veiligheid, de sociale en politieke stabiliteit en de internationale rechtsorde van het land. Volgens het rapport focussen statelijke actoren hun spionage en hacking-technieken voornamelijk op: *high potentials*, instituties en functionarissen van de democratische rechtsstaat, adviesorganen, onderwijsinstellingen, wetenschap (hoger en academisch onderwijs), denktanks en kennisinstellingen (inclusief instituten voor (toegepast) onderzoek), het maatschappelijk middenveld, internationale organisaties, het bedrijfsleven en topsectoren, vitale infrastructuur en cruciale internationale verbanden zoals de EU en NAVO.

Het Amerikaanse hoofd van de FBI, Christopher Wray, gaf op 7 juli 2020 een toespraak in het Hudson Institute, waarin die stelde:

[3] *https://www.standaard.be/cnt/dmf20210604_91153942*

"*The greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It's a threat to our economic security—and by extension, to our national security. It's the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history. If you are an American adult, it is more likely than not that China has stolen your personal data. Our data isn't the only thing at stake here – so are our health, our livelihoods, and our security.*

The Chinese government is engaged in a broad, diverse campaign of theft and malign influence, and it can execute that campaign with authoritarian efficiency. They're calculating. They're persistent. They're patient. And they're not subject to the righteous constraints of an open, democratic society or the rule of law.China, as led by the Chinese Communist Party, is going to continue to try to misappropriate our ideas, influence our policymakers, manipulate our public opinion, and steal our data. They will use an all-tools and all-sectors approach – and that demands our own all-tools and all-sectors approach in response.Chinese companies of any real size are legally required to have Communist Party "cells" inside them to keep them in line.[…] These kinds of features should give all Americans pause, when relying on such a company's devices and networks. […] In our modern world, there is perhaps no more ominous prospect than a hostile foreign government's ability to compromise our country's infrastructure and devices.".

En mai 2018, les autorités néerlandaises ont décidé que les organisations publiques et semi-publiques néerlandaises ne pouvaient plus utiliser le logiciel antivirus de la société de sécurité russe Kaspersky Lab en raison d'un risque possible d'espionnage par les autorités russes par le biais de ce logiciel.[4] En septembre 2019, les autorités américaines avaient également décidé d'interdire aux instances publiques d'utiliser les produits du Kaspersky Lab destinés aux instances publiques. Cette interdiction s'applique à tout système informatique associé aux autorités publiques américaines, y compris, par exemple, aux systèmes de gestion des salaires (*payroll*).[5]

En juin 2021, M. Joe Biden, président des États-Unis, a déclaré qu'il disposait d'une liste actualisée des entreprises chinoises dans lesquelles les entreprises américaines ne peuvent pas investir. Selon les États-Unis, ces cinquante-neuf entreprises se livrent à de l'espionnage

4 *https://www.channelconnect.nl/security-en-avg/overheid-moet-transparanter-zijn-over-kaspersky-verbod/*

5 *https://www.nextgov.com/cybersecurity/2019/09/us-finalizes-rule-banning-kaspersky-products-government-contracts/159742/*

"*The greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It's a threat to our economic security—and by extension, to our national security. It's the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history. If you are an American adult, it is more likely than not that China has stolen your personal data. Our data isn't the only thing at stake here – so are our health, our livelihoods, and our security.*

The Chinese government is engaged in a broad, diverse campaign of theft and malign influence, and it can execute that campaign with authoritarian efficiency. They're calculating. They're persistent. They're patient. And they're not subject to the righteous constraints of an open, democratic society or the rule of law. China, as led by the Chinese Communist Party, is going to continue to try to misappropriate our ideas, influence our policymakers, manipulate our public opinion, and steal our data. They will use an all-tools and all-sectors approach – and that demands our own all-tools and all-sectors approach in response. Chinese companies of any real size are legally required to have Communist Party "cells" inside them to keep them in line.[…] These kinds of features should give all Americans pause, when relying on such a company's devices and networks. […] In our modern world, there is perhaps no more ominous prospect than a hostile foreign government's ability to compromise our country's infrastructure and devices.".

In mei 2018 besloot de Nederlandse overheid dat overheidsorganisaties en semioverheidsinstellingen niet langer antivirussoftware van het Russische beveiligingsbedrijf Kaspersky Lab mochten gebruiken vanwege het mogelijke risico dat de Russische overheid via een achterdeur in de software zou spioneren.[4] Ook in september 2019 besloot de Amerikaanse overheid om een verbod uit te vaardigen voor producten van Kaspersky Lab voor overheidsinstanties. Het gebruik van Kaspersky-producten wordt verboden voor elk IT-systeem dat met de Amerikaanse overheid gelieerd is, zoals ook de *payroll*systemen.[5]

In juni 2021 kondigde de Amerikaanse president Joe Biden aan dat hij een aangepaste lijst klaar heeft van Chinese ondernemingen waar Amerikaanse bedrijven niet in mogen investeren. Volgens de VS houden die 59 ondernemingen zich bezig met industriële spionage.

4 *https://www.channelconnect.nl/security-en-avg/overheid-moet-transparanter-zijn-over-kaspersky-verbod/*

5 *https://www.nextgov.com/cybersecurity/2019/09/us-finalizes-rule-banning-kaspersky-products-government-contracts/159742/*

industriel. Il s'agit d'entreprises actives dans la défense ou le secteur de la surveillance, notamment du géant du secteur des technologies Huawei, de China Mobile, de China Telecom et China Unicom et de SMIC, qui est le plus grand fabricant de puces électroniques du pays.[6]

Belgique

Dans sa réponse à une question parlementaire[7] posée par le député M. Michael Frielich, M. Van Quickenborne, ministre de la Justice, indique que nous devons être conscients de certains risques posés par les smartphones chinois. Selon lui, il est de notoriété publique, par exemple, que le fabricant Xiaomi collecte secrètement à l'étranger des données d'utilisateur qu'il transmet à des serveurs chinois. Dès lors que cette entreprise opère dans le même contexte juridique et politique que Huawei, ZTE, Oppo et OnePlus, le ministre estime qu'il est possible que ces entreprises soient coupables de pratiques similaires.

Selon M. Van Quickenborne, la Sûreté de l'État (VSSE) n'a pas encore trouvé de preuve d'activités d'espionnage, mais le risque théorique existe que ces appareils et les informations qu'ils traitent soient utilisés par la Chine dans le cadre d'activités d'espionnage. En effet, les intrications entre ces entreprises et les autorités chinoises sont démontrables dès lors que le Parti communiste chinois exerce une emprise idéologique très forte sur les entreprises chinoises. Par exemple, le Parti communiste siège dans les grandes entreprises (comme Huawei, Xiaomi, Oppo et OnePlus) afin de pouvoir peser sur leurs décisions politiques. En outre, les intrications précitées sont établies sur le plan juridique, de sorte que les entreprises n'ont pas d'autre choix que de collaborer étroitement avec les autorités chinoises.

Logiciels

En ce qui concerne les smartphones, les tablettes, les télévisions et les montres intelligentes d'origine chinoise, ce risque s'est encore accru récemment, car il ne concerne plus seulement le matériel informatique chinois, mais aussi, depuis peu, les systèmes d'exploitation propres à ces appareils. Cette situation découle d'une décision par laquelle les États-Unis ont interdit toute collaboration entre les entreprises américaines et les fabricants de smartphones chinois à l'avenir, cette interdiction ayant empêché Google de vendre son système d'exploitation Android aux acteurs chinois.

6 *De Tijd*, 3 juin 2021, Biden zet 59 Chinese bedrijven op 'zwarte lijst'.

7 Question n° 55-2-000466 du 13 avril 2021 posée par le député M. Michael Freilich à M. Vincent Van Quickenborne, vice-premier ministre et ministre de la Justice et de la Mer du Nord.

Het gaat om bedrijven die actief zijn in defensie of de bewakingssector. Het gaat onder andere over technologiegigant Huawei, China Mobile, China Telecom en China Unicom en SMIC, de grootste chipfabkrikant van het land.[6]

België

In een antwoord op een parlementaire vraag[7] van Kamerlid Michael Freilich, liet minister van Justitie Van Quickenborne weten dat we ons bewust moeten zijn van bepaalde risico's verbonden aan Chinese smartphones. Hij verklaarde dat het van producent Xiaomi bijvoorbeeld publiekelijk gekend was dat het op heimelijke wijze gebruikersgegevens verzamelt in het buitenland en doorstuurt naar Chinese servers. Aangezien dit bedrijf werkt in dezelfde juridische en politieke context als Huawei, ZTE, Oppo en OnePlus, is het mogelijk dat ook zij zich aan dergelijke feiten schuldig maken, waarschuwde de minister.

De veiligheid van de Staat (VSSE) heeft tot nog toe geen bewijs waargenomen over spionage, maar de theoretische mogelijkheid bestaat dat deze apparaten en de informatie die ze verwerken gebruikt worden voor Chinese spionage, aldus Van Quickenborne. Er kan immers vermenging tussen de genoemde bedrijven en de Chinese overheid worden aangetoond, aangezien de Chinese Communistische Partij een stevige ideologische grip op de Chinese bedrijven houdt. Zij zetelen bijvoorbeeld binnen grotere bedrijven (zoals Huawei, Xiaomi, Oppo en OnePlus) om zo invloed te kunnen uitoefenen op beleidsbeslissingen. Bovendien wordt deze vermenging ook juridisch vastgelegd, waardoor het bedrijfsleven daar niet anders kan dan nauw samen te werken met de Chinese overheid.

Software

Wat betreft Chinese smartphones, tablets, televisies en smartwatches is het gevaar recentelijk nog vergroot aangezien deze niet enkel Chinese hardware betreffen, maar sinds kort ook draaien op eigen besturingssystemen. Dat komt door het Amerikaanse verbod aan bedrijven uit hun land om nog verder samen te werken met Chinese smartphonemakers, waardoor Google zijn Android besturingssysteem niet meer kan verkopen aan Chinese spelers.

6 *De Tijd*, 3 juni 2021, "Biden zet 59 Chinese bedrijven op 'zwarte lijst".

7 Vraag nr. 55-2-000466 van volksvertegenwoordiger Michael Freilich van 13 april 2021 aan de vice-eersteminister en minister van Justitie en Noordzee Vincent Van Quickenborne.

Pour illustrer les risques que ces logiciels peuvent présenter, nous renvoyons à la réponse à une question parlementaire[8] posée par le député Michael Freilich au sujet de l'application TikTok.

Réponse du ministre Van Quickenborne: "En tant que plateforme de médias sociaux, TikTok appartient à l'entreprise chinoise ByteDance. Cette entreprise est dès lors soumise aux règles de compliance chinoises relatives à l'accès des autorités chinoises aux données collectées par ByteDance. L'entreprise entretient de bons rapports de collaboration avec les autorités chinoises. TikTok n'est pas disponible en Chine et, d'après ByteDance, les données ne sont pas stockées dans ce pays. Les conditions d'utilisation de TikTok stipulent cependant bien que les données peuvent être partagées au sein du groupe. En outre, des experts (Penetrum) ont constaté que plus de 30 % des connexions de TikTok aux adresses IP allaient en Chine. Les mêmes experts affirment que les données de TikTok sont enregistrées sur des serveurs du fournisseur d'accès à internet chinois Alibaba, très proche des autorités chinoises, et que TikTok se livrerait à un traçage poussé des utilisateurs. En d'autres termes, ces utilisateurs ne peuvent pas s'attendre à la même protection de leurs données privées que dans l'Union européenne.

À cet égard, nous souhaitons attirer l'attention sur deux lois chinoises applicables à ByteDance, et donc également aux données collectées via TikTok. Tout d'abord, la loi sur la cybersécurité, qui oblige les opérateurs de réseaux à collaborer avec les services de police et de sécurité chinois. À la demande des services de sécurité, ces entreprises sont tenues de donner intégralement accès à leurs données. Mentionnons également l'existence d'une obligation d'"assistance technique", non définie plus précisément. Deuxièmement, la "loi sur le renseignement", qui régit les relations entre les services de sécurité et la société chinoise. Cette loi oblige les institutions, les organisations et les citoyens à fournir aux services de sécurité le soutien, l'assistance et la collaboration nécessaires. Par ailleurs, elle confère à ces services le droit d'accéder à tous les lieux et sources non publics "pertinents" et d'y recueillir des informations. Quels sont les éléments pertinents dans ce contexte? Il s'agit notamment de la publication ou la diffusion de messages qui mettent en péril la Sûreté de l'État et de faits fabriqués ou manipulés, d'idées pouvant être très largement interprétées par un régime qui développe une vision particulière de certains principes, tels que les droits de l'homme, la protection de la vie privée, la liberté d'expression ou encore la séparation de la justice et de l'État.".

[8] Question n° 55-2-000049 du 13 avril 2021 posée par le député M. Michael Freilich à M. Vincent Van Quickenborne, vice-premier ministre et ministre de la Justice et de la Mer du Nord.

Als voorbeeld van de gevaren die dergelijke software kan betekenen, verwijzen we naar het antwoord op een parlementaire vraag[8] van Kamerlid Michael Freilich over de app TikTok.

Minister Van Quickenborne: "TikTok is als social media platform in handen van het Chinese bedrijf ByteDance. Dit bedrijf is dus onderworpen aan de Chinese compliance regels met betrekking tot de toegang van de Chinese overheid tot de data verzameld door ByteDance. Dit bedrijf heeft een track record van goede samenwerking met de Chinese overheid. Tiktok is niet beschikbaar in China en de data worden volgens ByteDance ook niet opgeslagen in China. Maar in de gebruiksvoorwaarden van Tiktok wordt wel degelijk vermeld dat de data gedeeld mogen worden binnen de groep. Bovendien hebben experts (Penetrum) vastgesteld dat meer dan 30 % van de verbindingen die Tiktok maakt naar IP adressen in China gaan. Volgens dezelfde experts worden de Tiktok data opgeslagen op servers van de Chinese internetprovider Alibaba die goede banden heeft met de Chinese overheid, en zou Tiktok zich bezondigen aan verregaande tracking van gebruikers. Kortom, die gebruikers mogen niet dezelfde bescherming van hun privégegevens verwachten als wat ze gewoon zijn binnen de EU.

Hierbij willen we de aandacht vestigen op twee Chinese wetten die van toepassing zijn op ByteDance en dus ook op de gegevens die via TikTok verzameld worden. Ten eerste is er de Chinese cybersecurity wet die netwerkoperatoren verplicht om samen te werken met Chinese politie- en veiligheidsdiensten. Op vraag van de veiligheidsdiensten dienen deze bedrijven volledige toegang te geven tot hun data. Er is ook een verplichting tot een niet nader gespecifieerde "technische ondersteuning". Ten tweede is er de "*intelligence law*" die de relatie tussen de veiligheidsdiensten en de Chinese maatschappij regelt. Deze verplicht organen, organisaties en burgers om de nodige ondersteuning, assistentie en samenwerking te voorzien aan de veiligheidsdiensten. Ze geeft deze diensten ook het recht om zichzelf toegang te verschaffen tot alle "relevante" niet-publieke plaatsen en bronnen. En daar informatie te verzamelen. Wat is hierbij relevant? Onder andere het publiceren of verspreiden van boodschappen die de staatsveiligheid in gevaar brengen en van gefabriceerde of gemanipuleerde feiten. Begrippen die heel breed geïnterpreteerd kunnen worden door een regime met een bijzondere invulling van principes zoals mensenrechten, privacy, vrije meningsuiting of de scheiding tussen recht en staat.".

[8] Vraag nr. 55-2-000049 van volksvertegenwoordiger Michael Freilich van 13 april 2021 aan de vice-eersteminister en minister van Justitie en Noordzee Vincent Van Quickenborne.

C'est toutefois surtout la mise en garde lancée par le ministre dans sa réponse à la question parlementaire précitée qui lève tout doute à ce sujet:

"Les éléments mentionnés ci-dessus appellent toutefois à une vigilance accrue. C'est pourquoi il est recommandé de ne pas installer d'applications qui ne sont pas nécessaires sur des appareils à usage professionnel, ou qui contiennent des informations sensibles. Ce conseil vaut certainement pour les applications chinoises comme TikTok.".

Nous estimons que les conseils de ce type sont bien trop peu contraignants et craignons de lourdes conséquences ainsi qu'une perte d'indépendance stratégique et économique en l'absence d'intervention rapide et adéquate. Étant donné que la mise en garde du ministre visait surtout les "*appareils à usage professionnel, ou qui contiennent des informations sensibles*", la présente résolution vise également ces catégories.

Contre-mesures

Nous estimons, pour toutes les raisons exposées plus haut, qu'il est temps que la Belgique entreprenne des actions afin de contrer autant que possible les cybermenaces et les activités d'espionnage des acteurs étrangers.

Het is echter vooral de waarschuwing van de minister in zijn antwoord op de parlementaire vraag die niets aan de verbeelding overlaat:

"De elementen die hierboven worden vermeld zorgen er voor dat een verhoogde waakzaamheid geboden is. Daarom is het aan te raden om op apparaten voor professioneel gebruik, of waarop gevoelige informatie staat, geen apps te installeren die niet noodzakelijk zijn. Dit advies is zeker van toepassing op Chinese apps zoals TikTok.".

Wij vinden zo'n advies veel te vrijblijvend en zijn bevreesd om de zware gevolgen, het verlies aan strategische onafhankelijkheid en economische veiligheid als er niet snel en adequaat wordt opgetreden. Aangezien de waarschuwing van de minister in de eerste plaats gericht is op "apparaten voor professioneel gebruik, of waarop gevoelige informatie staat", zijn ook dat de categorieën waarop deze resolutie focust.

Tegenmaatregelen

Om al deze redenen wordt het tijd dat ook in ons land actie wordt ondernomen om cyberdreigingen en spionage door buitenlandse actoren zoveel als mogelijk tegen te houden.

Michael FREILICH (N-VA)
Joy DONNÉ (N-VA)
Theo FRANCKEN (N-VA)

PROPOSITION DE RÉSOLUTION

La Chambre des représentants,

A. vu la croissance exponentielle de la cybercriminalité observée ces dernières décennies;

B. vu l'infiltration persistante au sein du Service public fédéral Intérieur;

C. considérant que les pays développés ont de plus en plus souvent recours à des cyberstratégies offensives passant par une manipulation active des réseaux ou des infrastructures critiques dans le but de collecter des informations ou à des fins de sabotage;

D. vu l'ampleur des dégâts que les cyberattaques menées en Europe ont provoqués jusqu'à présent;

E. considérant que les réseaux à usage privé ou professionnel sont généralement moins bien sécurisés que les réseaux de certaines institutions;

F. considérant que les appareils privés des membres du personnel constituent souvent des cibles intéressantes;

G. considérant que les États-Unis d'Amérique ont établi une liste rouge d'entreprises qui seraient liées à une armée étrangère;

H. considérant que, dans sa boîte à outils 5G, l'Union européenne recommande de ne pas confier la gestion de l'infrastructure critique 5G à des fournisseurs "à risque";

I. considérant que plusieurs États membres de l'Union ont déjà adopté des législations en vue de protéger leur infrastructure critique 5G contre certains fournisseurs;

J. vu les déclarations du ministre néerlandais de la Justice et de la Sécurité, du directeur du FBI et du vice-premier ministre et de M. Vincent Van Quickenborne, ministre de la Justice et de la Mer du Nord;

K. vu l'ingérence de certains gouvernements étrangers dans le monde économique, d'ailleurs établie juridiquement, et considérant que ces entreprises étrangères n'ont dès lors pratiquement pas d'autre choix que d'espionner;

L. vu la possibilité théorique que les appareils fabriqués par Xiaomi, Oppo et OnePlus, par exemple, et les informations qu'ils traitent soient utilisés à des fins d'espionnage pour le gouvernement chinois;

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. gelet op de exponentiële groei van cybercriminaliteit de afgelopen decennia;

B. rekening houdende met de langdurige infiltratie binnen de federale overheidsdienst Binnenlandse Zaken;

C. overwegende dat ontwikkelde landen steeds meer gebruik maken van offensieve cyberstrategieën, waarbij ze overgaan tot actieve manipulatie van netwerken of kritieke infrastructuur met als doel het vergaren van informatie of sabotage;

D. gelet op de zware schade van cyberaanvallen die reeds hebben plaatsgevonden in Europa;

E. gezien netwerken die privé of professioneel worden gebruikt, vaak minder goed beveiligd zijn dan de netwerken van bepaalde instituties;

F. gezien privé toestellen van personeelsleden vaak interessante doelwitten zijn;

G. overwegende dat de Verenigde Staten van Amerika gebruik maken van een zwarte lijst met ondernemingen die banden zouden hebben met het buitenlandse legers;

H. overwegende dat de 5G-toolbox van de Europese Unie aanraadt om de kritieke 5G infrastructuur niet in handen te geven van risicovolle leveranciers;

I. rekening houdende met de verschillende EU lidstaten die reeds wetgeving hebben aangenomen om hun kritieke 5G infrastructuur te beschermen tegen bepaalde leveranciers;

J. gelet op de uitspraken van het Nederlandse ministerie van Justitie en Veiligheid, het hoofd van de FBI en Belgisch vice-eersteminister en minister van Justitie en Noordzee Vincent Van Quickenborne;

K. gelet op de vermenging van de bepaalde buitenlandse Overheden met hun bedrijfsleven, welke ook juridisch is vastgelegd, waardoor deze buitenlandse bedrijven bijna niet anders kunnen dan mee te werken aan spionage;

L. gelet op de theoretische mogelijkheid dat apparaten van bijvoorbeeld Xiaomi, Oppo en OnePlus en de informatie die ze verwerken gebruikt worden voor Chinese spionage;

M. vu la 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 (loi NIS);

N. vu les exposés présentés en commission de l'Intérieur de la Chambre des représentants le mardi 22 juin 2021 par plusieurs orateurs au cours des auditions consacrées aux cyberattaques visant les systèmes IT de l'État et des services publics,

Demande au gouvernement fédéral:

1. d'obliger la VSSE, l'OCAM et le SGRS à établir une liste des fournisseurs étrangers de produits informatiques pouvant être considérés comme des fournisseurs à haut risque;

2. de prononcer l'interdiction d'utiliser les produits de ces fournisseurs à haut risque, en concertation avec les entités fédérées, dans les services publics fédéraux et régionaux, l'armée, les entreprises visées par la loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (loi NIS), ainsi que dans les entreprises ayant accès aux réseaux informatiques et aux données des services publics et entreprises précités;

3. de permettre aux membres du personnel des entreprises ou des secteurs visés au 2 de déposer leurs appareils privés dans un espace sécurisé et séparé durant leurs heures de travail;

4. de demander aux entreprises et aux organismes visés de dresser au plus vite un inventaire des produits informatiques figurant sur la liste des fournisseurs à haut risque;

5. de permettre la consultation publique de la liste des fournisseurs à haut risque afin que les consommateurs non visés par l'interdiction précitée puissent également prendre connaissance des risques potentiels de ces appareils;

6. de rendre compte à la Chambre des représentants, dans un délai d'un an, des avancées de la mise en œuvre de la présente résolution.

1er juillet 2021

M. gelet op de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (NIS-wet);

N. gelet op de uiteenzetting van verschillende sprekers tijdens de hoorzittingen in de commissie Binnenlandse Zaken van de Kamer van volksvertegenwoordigers over de "cyberaanvallen op het IT-systeem van de Staat en de overheidsdiensten" op dinsdag 22 juni 2021,

Verzoekt de federale regering:

1. de VSSE, OCAD en ADIV op te leggen om een lijst samen te stellen van buitenlandse leveranciers van digitale producten die als hoog-risicoleveranciers kunnen worden omschreven;

2. in samenspraak met de deelstaten een verbod in te stellen voor de federale en regionale overheidsdiensten, het leger, bedrijven opgenomen in de Netwerk- en Informatiebeveiligingswet (NIS-wet) evenals bedrijven die toegang hebben tot het computer- en datanetwerk van voornoemde, om gebruik te maken van deze producten geleverd door hoog risico leveranciers;

3. aan de personeelsleden van de in verzoek 2 vernoemde bedrijven of sectoren de mogelijkheid te voorzien om privétoestellen tijdens de werkuren in bewaring te geven in een veilige en afgesloten ruimte;

4. de bedrijven en instellingen die in aanmerking komen zo snel mogelijk een inventaris te laten opmaken van reeds bestaande digitale producten die op de lijst voorkomen van de hoogrisicoleveranciers;

5. de lijst van hoogrisicoleveranciers publiekelijk consulteerbaar te maken, opdat ook consumenten die niet onder het verbod vallen, kennis kunnen nemen van de mogelijke risico's verbonden aan dergelijke apparaten;

6. na één jaar terug te koppelen naar de Kamer van volksvertegenwoordigers over de vooruitgang van deze resolutie.

1 juli 2021

Michael FREILICH (N-VA)
Joy DONNÉ (N-VA)
Theo FRANCKEN (N-VA)

Imprimerie centrale – Centrale drukkerij