DOC 55 **1263/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

11 mai 2020

PROPOSITION DE RÉSOLUTION

relative au déploiement de la 5G

(déposée par Mme Vanessa Matz et consorts)

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

11 mei 2020

VOORSTEL VAN RESOLUTIE

over de uitrol van 5G

(ingediend door mevrouw Vanessa Matz 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*
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 definitieve 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,

La 5G est la cinquième génération de standards pour réseau mobile. Elle permet un Internet mobile ultra rapide avec notamment des vitesses de téléchargement décuplées, l'envoi de données à haut débit ainsi qu'une meilleure stabilité de connexion. Alors que la 4G se concentre essentiellement sur les terminaux mobiles, elle ouvre la voie à la connexion d'une pléthore d'appareils distincts. L'idée est ainsi de permettre la mise en place d'un écosystème d'objets connectés cadrant parfaitement avec le principe d'une *smart city*, notamment.

La 5G est considérée comme le moteur d'une quatrième révolution industrielle. En effet, celle-ci représenterait un potentiel énorme en termes économiques avec la création de nouveaux marchés et donc de nouveaux emplois. En ce qui concerne la mobilité, la 5G permettrait une meilleure gestion du trafic ou l'utilisation de véhicules connectés et autonomes. Dans le domaine de la santé, il y aurait notamment la possibilité d'entreprendre des opérations chirurgicales à distance sans risque de coupure de connexion ou encore de procéder à la télémédecine pour les personnes éprouvant des difficultés à se déplacer ou dans les zones rurales dépourvues de praticiens en suffisance. Enfin, en matière de services, la 5G pourrait conduire à une gestion plus intelligente de l'énergie, à un contrôle à distance d'appareils industriels ou à un développement de machines autonomes. Plus globalement, c'est le bénéfice collectif de l'intelligence artificielle qui s'en trouverait élargi.

La 5G est particulièrement complexe et doit être abordée sous plusieurs angles: l'angle technique, l'angle géopolitique, l'angle économique, l'angle social et l'angle de la santé publique. L'aspect sécuritaire doit être totalement séparé de l'aspect géopolitique, mais ne doit pas pour autant être négligé.

À la grande différence de la 4G, le développement de la 5G aura pour effet de transformer le secteur des télécommunications en un fournisseur de services essentiels pour de nombreux secteurs de la société.

Pour pouvoir mettre en place et utiliser cette 5G via une augmentation du volume de données et de la capacité de transmission, un rehaussement des normes d'émission d'ondes électromagnétiques pour les antennes GSM est impératif dans certaines régions. Ledit rehaussement des normes d'émission inquiète bon nombre de citoyens et d'acteurs de la société civile.

TOELICHTING

DAMES EN HEREN,

5G is de standaard van de vijfde generatie voor mobiele netwerken. Deze technologie maakt ultrasnel mobiel internet mogelijk, met onder meer veel grotere downloadsnelheden, het versturen van gegevens met grote snelheid en een betere stabiliteit van de verbinding. Terwijl 4G hoofdzakelijk bestemd is voor mobiele toestellen, biedt 5G de mogelijkheid heel veel diverse toestellen op het internet aan te sluiten. De bedoeling is een ecosysteem van geconnecteerde voorwerpen uit te bouwen dat onder andere perfect aansluit bij het principe van een *smart city*.

5G wordt beschouwd als de motor voor een vierde industriële revolutie. Die zou een enorm economisch potentieel inhouden waarbij nieuwe markten en dus nieuwe banen zouden worden geschapen. Inzake mobiliteit zou 5G een beter verkeersbeheer of het gebruik van geconnecteerde en autonome voertuigen mogelijk maken. In de gezondheidszorg zouden chirurgische ingrepen op afstand kunnen worden uitgevoerd, zonder het risico te lopen dat de internetverbinding wordt onderbroken, en zou telegeneeskunde mogelijk worden voor mensen die zich moeilijk kunnen verplaatsen of die in landelijke gebieden wonen waar een gebrek is aan artsen. Op het vlak van de dienstverlening zou 5G ten slotte een intelligenter energiebeheer mogelijk kunnen maken, alsook de controle van industriële toestellen op afstand of de ontwikkeling van autonome machines. In ruimere zin zou 5G de collectieve baten van artificiële intelligentie nog vergroten.

5G is een bijzonder complexe technologie en moet vanuit verschillende invalshoeken worden benaderd; er is niet alleen het technische aspect, maar ook het geopolitieke, het economische, het maatschappelijke en dat van de volksgezondheid. Het veiligheidsaspect staat volledig los van het geopolitieke aspect, maar mag niet worden veronachtzaamd.

Het grote verschil met 4G bestaat erin dat de uitrol van 5G ertoe zal leiden dat de telecomsector zal uitgroeien tot een levensnoodzakelijke dienstverlener voor tal van maatschappelijke sectoren.

Om die 5G-technologie te kunnen uitrollen en er gebruik van te kunnen maken via een verhoogd gegevensvolume en een grotere transmissiecapaciteit, moeten de elektromagnetische stralingsnormen voor de gsm-antennes in bepaalde gebieden onvermijdelijk worden verhoogd. Veel burgers en actoren uit het middenveld maken zich zorgen over die verhoging van de stralingsnormen. Ze

Ceux-ci pointent d'éventuelles répercussions des nouvelles normes sur notre santé. Pour ces personnes, il est très difficile d'évaluer suffisamment à l'avance les effets sanitaires d'un déploiement massif et à grande échelle de la technologie 5G, lequel déploiement multiplierait de manière importante notre exposition aux ondes électromagnétiques. En date du 1er mai 2020, une carte blanche signée par 434 médecins et 900 professionnels de la santé demande aux décideurs politiques de faire respecter le principe de précaution et souligne que l'exposition aux rayonnements électromagnétiques de radiofréquences et de micro-ondes n'a cessé d'augmenter ces dernières décennies.

A ce propos, et même si le Centre international de recherche sur le cancer (CIRC) – structure rattachée à l'Organisation mondiale de la Santé (OMS) – a classé en 2011 les champs de radiofréquences électromagnétiques dans la catégorie des phénomènes comme "étant peut-être cancérigènes", la littérature scientifique majoritaire actuelle n'a pas établi de lien de causalité démontrant une quelconque nocivité des ondes. Dans ce contexte, l'OMS – via des organismes scientifiques indépendants – a fixé une norme d'émission de 41,2 volts par mètre, laquelle norme offre une marge de sécurité importante pour palier à tout risque provenant de toute incertitude, aussi minime soit-elle.

Lors d'une audition en commission de l'Économie, le 11 décembre 2019, M. Miguel De Bruycker, directeur du Centre pour la Cybersécurité de Belgique (CCB) citait ceci: "La technologie 5G apporte de nouvelles améliorations et possibilités, en matière de sécurité, mais nous place également face à de nouveaux défis à cet égard. La nouvelle architecture et la virtualisation améliorent la flexibilité mais accroissent aussi la complexité et la dépendance des logiciels et des mises à jour des logiciels dans le réseau. Tout opérateur de réseau sera davantage dépendant de ses fournisseurs et des gestionnaires de réseau externes en raison de l'augmentation de la complexité. Les menaces à l'égard de la disponibilité, de la confidentialité et de l'intégrité du réseau 5G et des informations envoyées pourraient dès lors être plus difficiles à éviter et à détecter.

L'augmentation de la complexité et de la dépendance des logiciels signifie aussi qu'il sera de plus en plus important d'opter pour des fournisseurs qui prennent très au sérieux le développement, les tests et les correctifs des logiciels. Le nombre croissant de possibilités d'attaques peut aussi influer sur le choix des fournisseurs.

(…) En guise de réponse en matière de cybersécurité aux risques de sécurité que pourrait présenter le passage à la technologie 5G, le CCB a développé un guide de la

wijzen erop dat de nieuwe normen schadelijke gevolgen voor de gezondheid kunnen hebben. Ze zijn van oordeel dat het heel moeilijk is om tijdig in te schatten welke gevolgen een grootschalige uitrol van de 5G-technologie zal hebben voor de gezondheid omdat die uitrol tot een veel grotere blootstelling aan elektromagnetische golven zou leiden. In een open brief van 1 mei 2020 hebben 434 artsen en 900 gezondheidzorgbeoefenaars de beleidsmakers opgeroepen het voorzorgsbeginsel in acht te nemen. Ze benadrukten daarbij dat de blootstelling aan elektromagnetische straling van radiofrequenties en van microgolven de voorbije decennia voortdurend is toegenomen.

Hoewel het Internationaal Agentschap voor Kankeronderzoek – dat deel uitmaakt van de Wereldgezondheidsorganisatie (WGO) – de elektromagnetische radiofrequentievelden in 2011 heeft gecategoriseerd als verschijnselen die misschien kankerverwekkend zijn, is in de meeste huidige wetenschappelijke literatuur geen sprake van een causaal verband op grond waarvan enig schadelijk gevolg van de golven kan worden bewezen. In die context heeft de WGO via onafhankelijke wetenschappelijke organisaties een stralingsnorm vastgelegd van 41,2 volt per meter. Aangezien die norm een grote veiligheidsmarge biedt, kan elk risico dat uit om het even welke onzekerheid voorvloeit, worden ondervangen.

Tijdens een hoorzitting in de commissie Economie, Consumentenbescherming en Digitale agenda op 30 januari 2020 heeft de heer Miguel de Bruycker, directeur van het Centrum voor Cybersecurity België (CCB), het volgende verklaard: "De 5G-technologie brengt nieuwe veiligheidsverbeteringen en -mogelijkheden maar introduceert eveneens nieuwe veiligheidsuitdagingen. De nieuwe architectuur en de virtualisatie zorgen voor een grotere flexibiliteit maar eveneens voor extra complexiteit en afhankelijkheid van de software en van de software-updates in het netwerk. Een netwerkoperator zal meer afhankelijk worden van zijn leveranciers en externe netwerkbeheerders omwille van de toename van de complexiteit. De dreigingen ten opzichte van de beschikbaarheid, de vertrouwelijkheid en de integriteit van het 5G-netwerk en van de verstuurde informatie kunnen hierdoor moeilijker te vermijden en te detecteren zijn.

De grotere complexiteit en afhankelijkheid van de software betekent eveneens het toenemend belang om voor leveranciers te kiezen die de softwareontwikkeling, -testing en -*patching* zeer ernstig nemen. Ook het toenemend aantal aanvalsmogelijkheden kan de keuze van de leveranciers beïnvloeden.

(…) Als *cybersecurity*-antwoord op deze veiligheidsrisico's die het overgaan naar 5G-technologie met zich mee zouden kunnen brengen heeft het CCB een supply

chaîne d'approvisionnement (*supply chain guideline)* pour les réseaux TIC qui soutiennent des services essentiels. Ce guide porte aussi bien sur la sécurité de la chaîne d'approvisionnement que sur la sécurité du cycle de vie à l'égard de la gestion de systèmes dans ce type de réseaux. Les mesures proposées par le CCB doivent permettre d'atteindre un même niveau de sécurité tout au long du cycle de vie du système, de la prospection du marché en vue de l'achat à la mise hors service finale en passant par l'installation, la configuration et l'utilisation. La rédaction de ce guide est presque terminée et sa publication est prévue pour bientôt"

De plus, le groupe de coopération NIS, Network and Information Systems, de l'Union européenne, a publié, après consultation des États membres, le rapport intitulé "Évaluation coordonnée par l'Union européenne des risques liés à la cybersécurité des réseaux 5G" et a élaboré une boîte à outils mise à la disposition des États membres depuis le 31 décembre 2019. La Commission européenne et l'Agence ENISA (Agence européenne de la cybersécurité) ont également entrepris les démarches nécessaires pour créer, sur la base du règlement relatif à la cybersécurité, un cadre de certification et encourager les États membres à accorder la priorité à l'élaboration d'un schéma de certification pour les réseaux et les appareils 5G.

Toujours lors de la commission de l'Économie du 11 décembre 2019, dans son exposé introductif, M. Jaak Raes, administrateur général de la Sûreté de l'État (VSSE) disait ceci: "L'espionnage passe également par une combinaison de ressources humaines et de moyens techniques. Pour citer un exemple récent près de chez nous, l'orateur fait référence à un fabricant néerlandais de machines à puce. Des employés du fabricant ont piraté le réseau de l'entreprise pour voler des documents. Ils ont ensuite vendu la technologie à une entreprise concurrente. L'espionnage technique par l'utilisation abusive de l'infrastructure 5G offrira des possibilités sans précédent. Dès lors qu'une partie de l'intelligence des réseaux se situera dans le réseau radioélectrique, il y aura une multiplication des points d'accès possibles. Il s'agit d'un problème potentiel en termes de protection des données des autorités publiques et des secrets d'affaires, de la vie privée et des infrastructures critiques.

La perte d'indépendance stratégique et économique dans le secteur des télécoms constitue un danger au moins aussi important pour la Belgique, mais aussi pour d'autres États membres de l'Union européenne et pour l'UE en général. Il s'agit d'une infrastructure critique qui, avec le déploiement de la 5G, fournira un service crucial à nombre d'autres secteurs stratégiques. La dépendance stratégique signifie que pour tous les secteurs dépendant

chain guideline ontwikkeld voor ICT-netwerken die essentiële diensten ondersteunen. Deze richtlijn omhelst zowel de supply chain als de life cycle veiligheidsaspecten voor het beheer van systemen in dergelijke netwerken. De maatregelen die het CCB voorstelt moeten zorgen voor een gelijk niveau van beveiliging over de ganse levenscyclus van het systeem, van marktprospectie over aankoop, installatie en configuratie, tot het gebruik en de uiteindelijke buitengebruikstelling van het systeem. Deze *supply chain guideline* is bijna volledig opgesteld en zal binnenkort worden gepubliceerd.".

Bovendien heeft de heer de Bruycker erop gewezen dat de *NIS (Network and Information Systems) Cooperation Group* van de Europese Unie na consultatie van de lidstaten het *EU coordinated risk assessment of the cybersecurity of 5G networks* heeft gepubliceerd en een *toolbox* heeft uitgewerkt die sinds 31 december 2019 ter beschikking is van de lidstaten. Tot slot heeft hij aangegeven dat de Europese Commissie en het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) eveneens de nodige stappen hebben gezet om op basis van de cyberveiligheidsverordening een certificeringskader uit te werken en de lidstaten aan te moedigen om prioriteit te geven aan een certificeringsregeling voor 5G-netwerken en -apparatuur.

Tijdens dezelfde hoorzitting van de commissie Economie, Consumentenbescherming en Digitale agenda van 30 januari 2020 heeft de heer Jaak Raes, administrateur-generaal van de Veiligheid van de Staat (VSSE), het volgende aangestipt: "Of het gebeurt via een combinatie van menselijke en technische middelen. Om een recent voorbeeld dicht bij huis aan te halen, verwijst de spreker naar een Nederlandse chipmachinefabrikant. Werknemers van de fabrikant hackten het bedrijfsnetwerk om documenten te stelen. Vervolgens verkochten ze de technologie aan een concurrerende firma. Technische spionage middels misbruik van 5G-infrastructuur zal ongeziene mogelijkheden bieden. Omdat een deel van de intelligentie van de netwerken in het radionetwerk zal zitten, komt er een verveelvoudiging van het aantal mogelijke toegangspunten. Dit is potentieel een probleem in termen van bescherming van overheidsgegevens en bedrijfsgeheimen, de persoonlijke levenssfeer en de kritieke infrastructuur.

Een minstens even belangrijk gevaar (voor België, maar ook voor andere EU-lidstaten en de EU als geheel) is het verlies van strategische en economische onafhankelijkheid in de telecomsector. Dit is een kritieke infrastructuur die met de uitrol van 5G in een cruciale dienstverlening zal voorzien voor tal van andere strategische sectoren. Strategische afhankelijkheid houdt in dat voor alle sectoren die van 5G afhankelijk zijn als het

de la 5G, il existe, pour ainsi dire, un bouton marche/arrêt dans un pays tiers. Certains pays où sont établis des producteurs de 5G ont déjà prouvé qu'ils adoptaient une cyberpolitique très agressive.

Un problème lié à cette dépendance stratégique est celui de l'ingérence. Cela consiste à utiliser des mécanismes d'influence abusifs pour exercer des pressions sur des processus décisionnels souverains. L'orateur fait référence, par exemple, aux cas dans lesquels une entreprise menace de retirer des investissements si un pays se montre trop critique à l'égard de questions considérées comme relevant des affaires intérieures (par exemple, les droits de l'homme) dans le pays du fournisseur, ou si des prêts bon marché sont utilisés pour exercer des pressions politiques sur des pays.

Dans un souci d'exhaustivité, il convient également d'accorder, en ce qui concerne la sécurité dans le contexte de la 5G, une attention spécifique aux interceptions légales. Les services de sécurité et de renseignement disposent de moyens qui leur permettent, moyennant le respect des critères légaux et un contrôle, d'intercepter, dans certains cas, des communications ou des métadonnées. C'est un instrument très important dans la lutte contre le terrorisme. Il s'agit en outre d'un dispositif qui est très strictement contrôlé. Avant de pouvoir procéder à des écoutes téléphoniques, les services de renseignement doivent introduire une demande auprès de la commission BIM (Bijzondere Inlichtingenmethoden – Méthodes particulières de recherche) compétente, composée de trois magistrats indépendants (un ancien juge d'instruction, un ancien magistrat du parquet et un ancien juge du siège) qui passent l'enquête au crible. Dans certains cas exceptionnels uniquement, les services de renseignement seront autorisés à procéder à des interceptions légales. Cette autorisation ne sera accordée que lorsque les services concernés peuvent prouver que les informations dont ils ont besoin ne peuvent être obtenues d'aucune autre manière et que l'opération s'inscrit dans le cadre de menaces bien définies.

Lors de la commission de l'Économie du 11 décembre 2019, Claude Van de Voorde, lieutenant-général du Service général du Renseignement et de la Sécurité (SGRS) citait: "En ce qui concerne la sécurisation des réseaux 5G, le Conseil de l'Union européenne a adopté une série de conclusions le 3 décembre 2019. Ces conclusions partent notamment du principe que lors de l'élaboration du profil de risque d'un fournisseur, il faut également tenir compte de facteurs non techniques et faire en sorte que des éléments qui revêtent une importance cruciale pour la sécurité nationale ne soient accessibles qu'à des parties dignes de confiance. Sur la scène internationale encore, l'OTAN, dans sa communication, attire aujourd'hui l'attention sur la problématique

ware een aan/uit-knop in een derde land staat. Er zijn landen met 5G-producenten die reeds bewezen hebben er een zeer agressieve cyberpolitiek op na te houden.

Een probleem dat met deze strategische afhankelijkheid verband houdt, is inmenging. Dit gaat om het gebruiken van oneigenlijke beïnvloedingsmechanismen om druk uit te oefenen op soevereine beslissingsprocessen. De spreker verwijst hier bijvoorbeeld naar gevallen waarin wordt gedreigd met het terugtrekken van investeringen indien een land zich te kritisch opstelt met betrekking tot zaken die in het land van de leverancier als interne aangelegenheden worden beschouwd (bijvoorbeeld mensenrechten), of goedkope leningen gebruikt om landen politiek onder druk te zetten.

Voor de volledigheid moeten we hier, wat veiligheid in de 5G-context betreft, ook een specifiek punt vermelden omtrent legale intercepties of wettelijke onderscheppingen (*lawful intercepts*). Inlichtingen- en veiligheidsdiensten hebben middelen ter beschikking om, met inachtneming van de wettelijke criteria en controle, in bepaalde gevallen communicatie of metadata te onderscheppen. Dit is een belangrijk middel in de strijd tegen het terrorisme. Het is bovendien een middel dat bijzonder streng wordt gecontroleerd. Alvorens over te kunnen gaan tot een telefoontap moeten de inlichtingendiensten een aanvraag indienen bij de bevoegde BIM-commissie (Bijzondere Inlichtingenmethoden) die bestaat uit drie onafhankelijke magistraten (een oud-onderzoeksrechter, een oud-parketmagistraat een voormalig rechter van de zetel) die het onderzoek onder de loep nemen. Slechts in uitzonderlijke gevallen zullen de inlichtingendiensten de toelating krijgen om lawful intercepts uit te voeren. Deze toelating zal slechts verleend worden wanneer de betrokken diensten kunnen aantonen dat de informatie die deze diensten nodig hebben op geen enkel andere wijze te verkrijgen is en kadert in een aantal welomschreven dreigingen.".

Nog tijdens de vergadering van de commissie Economie, Consumentenbescherming en Digitale agenda van 30 januari 2020 heeft de heer Claude Van de Voorde, luitenant-generaal van de Algemene Dienst Inlichting en Veiligheid (ADIV) het volgende meegedeeld: "Wat het beveiligen van 5G-netwerken betreft heeft de Raad van de EU op 3 december 2019 conclusies aangenomen. De conclusies van de Raad bevatten onder meer de stelling dat bij het opstellen van het risicoprofiel van een leverancier ook rekening moet worden gehouden met niet-technische factoren, en dat onderdelen die van cruciaal belang zijn voor de nationale veiligheid alleen van betrouwbare partijen mogen komen. Nog op het internationale toneel vestigt de NAVO nu in haar communicatie

de la sécurité des réseaux 5G. Le fait que l'OTAN se prononce sur la technologie des télécommunications est une donnée nouvelle, qui souligne l'importance du déploiement et de l'impact de la 5G.

La question qui se pose souvent de prouver l'existence d'une porte dérobée (backdoor) ou d'un flagrant délit réduit la problématique relative à la sécurité de la 5G à une matière technique qui devrait pouvoir être solutionnée post factum, après que l'abus a été constaté. L'impact de la télécommunication 5G sur l'ensemble de la société nous contraint toutefois à adopter une approche préventive. Si nous confions le déploiement de nos réseaux 5G à des entreprises géostratégiquement problématiques, il ne faut en fait même plus se demander s'il y a une faille technique quelque part. À ce moment-là, les pouvoirs publics ont déjà accepté de se décharger de toute l'architecture de leur maison numérique, de la conception à la construction de toutes les pièces, y compris le placement des portes et la pose des verrous. La 5G est tellement cruciale dans la société de demain que les pouvoirs publics doivent d'abord s'assurer que l'architecte et l'entrepreneur qu'ils ont choisis pour leurs citoyens sont des partenaires fiables."

Lors de la commission de l'Économie précitée, dans son exposé introductif, Mme Christiane Höhn, conseillère principale auprès du Coordinateur de l'Union européenne pour la lutte contre le terrorisme, soulignait que: "le coordinateur de l'Union européenne pour la lutte contre le terrorisme n'est pas associé aux travaux sur les aspects techniques de la cybersécurité.

Le coordinateur est en revanche associé aux travaux sur la problématique des écoutes légales, comme les écoutes téléphoniques. Au printemps dernier, le coordinateur de l'Union européenne pour la lutte contre le terrorisme a tiré la sonnette d'alarme, à la demande de la police fédérale allemande. Cette dernière était extrêmement préoccupée par cette problématique et plaidait pour une approche globale au niveau européen afin de pouvoir préserver les possibilités existant actuellement en matière d'interceptions légales. Les techniques d'écoute actuelles sont compromises par le déploiement de la technologie 5G et il sera beaucoup plus difficile, voire impossible de les mettre en œuvre à l'avenir."

(…) "Les difficultés liées aux interceptions légales trouvent principalement leur origine dans le cryptage des messages de communication. Certains messages font l'objet d'un chiffrement de bout en bout, ce qui rend l'accès aux données extrêmement difficile, voire impossible. Le cryptage des messages d'information est déjà une réalité à l'heure actuelle, mais son ampleur s'accentuera à l'avenir. Une autre difficulté concerne le cryptage du numéro d'identité internationale d'abonné mobile (IMSI),

de aandacht op de 5G-veiligheidsproblematiek. Dat de NAVO zich uitspreekt over telecommunicatietechnologie is een nieuw gegeven dat mee het belang onderlijnt van de uitbouw en de impact van 5G.

De vaak gestelde vraag naar bewijzen van een backdoor of een smoking gun reduceert de probleemstelling omtrent de veiligheid van 5G tot een technische zaak die post factum, na de vaststelling van een misbruik, zou moeten kunnen worden opgelost. De impact van 5G-telecom op de gehele maatschappij noopt ons evenwel tot een preventieve aanpak. Indien we geostrategisch problematische bedrijven onze 5G-netwerken laten uitbouwen, moeten we ons eigenlijk zelfs niet meer afvragen of ergens een technisch achterdeurtje bestaat. Op dat moment heeft de overheid reeds aanvaard dat zij de gehele architectuur van haar digitale woning uit handen geeft, van het ontwerpen en bouwen van alle kamers ervan, tot het plaatsen van deuren en het voorzien van de sloten. 5G wordt dermate cruciaal in de toekomstige samenleving, dat de overheid er zich in eerste instantie moet van vergewissen dat de architect en de aannemer die zij dit voor haar onderdanen laat uitbouwen, betrouwbare partners zijn.".

Tijdens dezelfde vergadering van de voormelde commissie heeft mevrouw Christiane Höhn, hoofdadviseur van de EU-coördinator voor terrorismebestrijding, er in haar inleidende uiteenzetting op gewezen dat "de EU-coördinator voor terrorismebestrijding niet betrokken is bij de technische aspecten betreffende de cyberveiligheid.

Hij is echter wel betrokken bij de problematiek van de wettelijke afluisterpraktijken zoals telefoontaps. Tijdens het afgelopen voorjaar heeft de EU-coördinator voor terrorismebestrijding aan de alarmbel getrokken, op vraag van de Duitse federale politie. Die laatste maakte zich grote zorgen over dit onderwerp en pleitte voor een globale aanpak op het niveau van de EU teneinde de huidige mogelijkheden inzake lawful intercepts te kunnen vrijwaren. De huidige afluistertechnieken staan door de uitrol van de 5G-technologie onder druk en zullen veel moeizamer of zelfs helemaal niet meer kunnen worden uitgevoerd.

(…) De moeilijkheden inzake lawful intercepts situeren zich in de eerste plaats op het vlak van het versleutelen van de communicatieboodschappen. Zo zal er onder andere meer end-to-end encryption plaatsvinden, waardoor er weinig tot geen toegang zal zijn tot de gegevens. Thans bestaat er ook al versleuteling van informatieboodschappen, maar de omvang van de versleuteling zal in de toekomst veel groter worden. Een andere complicatie betreft de versleuteling van het

qui ne permettra plus d'accéder au numéro unique du propriétaire du GSM. Il ne sera ainsi plus possible de localiser un utilisateur du réseau mobile et de l'identifier lorsqu'il passe un appel, ce qui rendra impossible toute écoute téléphonique et bloquera l'accès à toute une série de métadonnées générées par les écoutes.

Par ailleurs, l'architecture des réseaux 5G constitue un défi important pour ce qui est de la problématique des interceptions légales. Les réseaux 5G seront, à l'avenir, beaucoup plus fragmentés et, partant, beaucoup moins centralisés que le réseau 4G actuel. Les informations ne transiteront plus par les nœuds d'information centraux du réseau, auxquels les dispositifs d'écoute sont connectés à l'heure actuelle. De plus, le réseau se virtualisera et certaines de ses fonctions ou de ses composantes pourront par exemple se situer à l'étranger, ce qui signifie que les services de sécurité nationale n'y auront plus accès.

De surcroît, il existe également un risque de division du réseau, qui empêchera de générer une copie exhaustive permettant de réaliser une éventuelle interception légale. Il sera également plus difficile de garantir la confidentialité d'éventuelles écoutes téléphoniques. Il se pourrait ainsi que la personne mise sur écoute en soit consciente, sans pour autant que les services de sécurité concernés le sachent.

Enfin, l'oratrice s'attarde sur les mesures qui peuvent être prises pour préserver les interceptions légales. Tout d'abord, les parlements nationaux des différents États membres de l'UE ont un rôle particulièrement important à jouer à cet égard. Ils doivent de toute urgence fixer un cadre et des conditions juridiques afin de garantir aussi le recours aux interceptions légales sur le réseau 5G. Le Code des communications électroniques européen permet désormais de répondre aux demandes d'écoutes téléphoniques des services de sécurité nationale, en obligeant notamment les opérateurs de téléphonie mobile à fournir un certain nombre de services.

Afin de relever les défis posés par le réseau 5G, les différents services de police européens ont proposé des mesures supplémentaires. Ils demandent par exemple que les opérateurs mobiles soient officiellement enregistrés. Ils demandent aussi que ces opérateurs fournissent une copie exhaustive et décryptée des informations demandées et structurent leur réseau de manière à ce qu'il soit possible d'en localiser les utilisateurs. En outre, ils souhaiteraient que les opérateurs coopèrent à la mise en œuvre de certaines mesures, comme l'installation d'intercepteurs d'IMSI. L'oratrice souligne l'importance

IMSI-nummer (international mobile subscriber identity), waardoor het niet meer mogelijk zal zijn om toegang te hebben tot het unieke nummer van de gsm-houder. Hierdoor verdwijnt de mogelijkheid om een gebruiker van het mobiele netwerk te lokaliseren en te herkennen bij het maken van een oproep, met als gevolg dat er niet langer telefoontaps.

Bovendien is de architectuur van de 5G-netwerken een belangrijke uitdaging betreffende de problematiek van *lawful intercepts*. De 5G-netwerken zullen in de toekomst veel meer gefragmenteerd zijn en dus veel minder gecentraliseerd dan het huidige 4G-netwerk. De informatie zal niet meer langs centrale informatieknopen passeren binnen het netwerk waaraan thans de afluisterapparatuur wordt gekoppeld. Daarnaast zal er zich een virtualisering van het netwerk voordoen, waarbij er functies of onderdelen van dat netwerk zich bijvoorbeeld in het buitenland kunnen bevinden, waardoor de nationale veiligheidsdiensten er geen toegang meer toe hebben.

Bovendien bestaat ook het risico dat het netwerk kan opgedeeld worden, waardoor er geen volledige kopie mogelijk is die een eventuele lawful intercept kan realiseren. Het zal ook moeilijker worden om de vertrouwelijkheid van eventuele telefoontaps te garanderen. Hierdoor zal het kunnen gebeuren dat de persoon die afgeluisterd wordt weet heeft van dit feit, zonder dat de betrokken veiligheidsdiensten hiervan op de hoogte zijn.".

Tot slot is mevrouw Höhn in haar uiteenzetting nader ingegaan op de maatregelen die kunnen worden genomen om lawful intercepts te waarborgen. Ze heeft daarbij het volgende verklaard: "Vooreerst is er een bijzonder belangrijke rol weggelegd voor de nationale parlementen van de verschillende EU-lidstaten. Zij moeten dringend de voorwaarden creëren en wettelijk verankeren teneinde de toepassing van lawful intercepts ook in het kader van het 5G-netwerk te verzekeren. Het Europees wetboek voor elektronische communicatie verschaft thans de mogelijkheid om tegemoet te komen aan de vragen tot telefoontaps van de nationale veiligheidsdiensten, waarbij de mobiele operatoren verplicht zijn om een aantal diensten te leveren.

Om het hoofd te bieden aan de uitdagingen in het kader van het 5G-netwerk hebben de verschillende Europese politiediensten bijkomende maatregelen voorgesteld. Zo vragen zij dat de mobiele operatoren officieel geregistreerd zijn. Zij moeten een volledige en ontsleutelde kopie bezorgen van de gevraagde informatie en het netwerk op die manier structureren dat het mogelijk is om de gebruikers van het netwerk te lokaliseren. Bovendien verlangen zij dat de operatoren samenwerken om bepaalde maatregelen zoals de installatie van de IMSI catcher te realiseren. De spreekster benadrukt dat

de parvenir à une approche coordonnée. La sécurité intérieure constitue une compétence exclusivement nationale, ce qui accroît le risque de fragmentation de la législation à cet égard. Elle plaide dès lors pour une concertation structurelle entre les États membres de l'UE afin d'éviter une telle fragmentation."

Actuellement, les services de renseignement ne font que rendre des avis et ne prennent aucune décision quant au choix du fournisseur. Les services de renseignement recommandent vivement de rechercher un partenaire fiable et de prendre des mesures d'atténuation pour limiter les risques de sécurité. Il est recommandé à cet égard de faire appel à plusieurs fournisseurs pour un réseau 5G donné, ce qui permettra d'atténuer les répercussions d'une éventuelle manipulation et de réduire sensiblement le risque de formation d'un monopole. C'est pourquoi il est important de prévoir une étape cruciale qui permet au gouvernement de rester maître et acteur quant au choix des opérateurs et des fournisseurs.

Face à cette menace pour la sûreté nationale, la France notamment a pris des dispositions afin de répondre à cette menace. La faiblesse considérée pourrait résulter d'un défaut de conception, volontaire ou non, d'erreurs de configuration dans leur déploiement par les opérateurs ou de leurs sous-traitants dans le cadre de la maintenance et de l'administration de ces équipements.

De telles faiblesses pourraient être exploitées à des fins d'espionnage, d'interruption du fonctionnement ou d'attaque informatique dirigée contre des services utilisant le réseau.

La France prévoit donc que préalablement à toute activité d'exploitation de certains équipements radioélectriques, les opérateurs doivent adresser une demande d'autorisation au premier ministre. Celui-ci se prononcera dans un délai de deux mois à compter de la réception du dossier complet de demande. La liste des équipements concernés sera publiée et mise à jour par le premier ministre. Ce dernier déterminera s'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale, en se basant sur les critères définis dans la loi et notamment au regard des garanties que présente l'équipement pour l'intégrité, la sécurité et la continuité de l'exploitation des réseaux et services de communications électroniques.

Nous proposons dans cette proposition de résolution que le gouvernement belge joue également un rôle de contrôle et délivre préalablement une autorisation. Ce contrôle doit également se faire par le Parlement au

het belangrijk is om tot een gecoördineerde aanpak te komen. De interne veiligheid is een uitsluitend nationale bevoegdheid. Hierdoor is er een verhoogd risico op fragmentatie van de wetgeving ter zake. Zij pleit dan ook voor structureel overleg tussen de EU-lidstaten teneinde zulke versnippering te vermijden.".

Thans doen de inlichtingendiensten niet meer dan adviezen verstrekken en nemen ze geen enkele beslissing inzake de keuze van de leverancier. De inlichtingendiensten raden ten stelligste aan om uit te kijken naar een betrouwbare partner en om inzake veiligheid risicobeperkende maatregelen te nemen. In dat verband wordt aanbevolen om voor een bepaald 5G-netwerk een beroep te doen op meerdere leveranciers om de weerslag van een eventuele manipulatie te reduceren en om het risico op monopolievorming aanzienlijk te verminderen. Daarom is het belangrijk om te voorzien in een beslissende stap die de regering in de mogelijkheid stelt voor de keuze van de operatoren en de leveranciers het heft in handen te houden.

Ten aanzien van die dreiging voor de nationale veiligheid heeft onder meer Frankrijk maatregelen getroffen om ze aan te pakken. De bedoelde kwetsbaarheid zou het gevolg kunnen zijn van een al dan niet vrijwillige designfout of van configuratiefouten bij de uitrol door de operatoren of hun onderaannemers in het raam van het onderhoud en het beheer van die apparatuur.

Dergelijke kwetsbaarheden kunnen worden benut om te spioneren, om de werking te onderbreken of om een computeraanval uit te voeren op de diensten die het netwerk gebruiken.

In Frankrijk is dus bepaald dat de operatoren van bepaalde radio-elektrische apparatuur voorafgaand aan elke vorm van exploitatie een vergunningsaanvraag moeten indienen bij de eerste minister, die binnen twee maanden na ontvangst van het volledige aanvraagdossier een beslissing zal nemen. De eerste minister zal de lijst met de betrokken apparatuur bekendmaken en bijwerken. Hij zal bepalen of er een ernstig risico bestaat dat de defensiebelangen en de nationale veiligheid kunnen worden geschaad, op grond van de in de wet bepaalde criteria en onder meer rekening houdend met de door de apparatuur geboden garanties voor de integriteit, de veiligheid en de continuïteit van de exploitatie van de elektronische-communicatienetwerken en -diensten.

In dit voorstel van resolutie wordt ook de Belgische regering verzocht een rol te spelen inzake controle en vooraf een vergunning te verlenen. Die controle zou ook door het Parlement moeten worden uitgevoerd,

travers d'une commission spéciale chargée d'analyser, de rendre des avis, de valider, de proposer.

Récemment, le mercredi 1er avril 2020, Proximus annonçait lancer une 5G *light* en Belgique avec comme couverture initiale une trentaine de communes à travers le pays. Une opération prématurée sachant toutes les incertitudes qui règnent tant en matière d'effets sur la santé, qu'en matière de sécurité ou encore vu le manque de balises pour un cadre international.

La Région de Bruxelles-Capitale n'est pas directement concernée par l'opération en raison de ses normes d'émission d'ondes plus strictes que la Région flamande et la Région wallonne. Néanmoins, plusieurs communes voisines de la Région bruxelloise sont impliquées comme Zaventem, Leeuw-Saint-Pierre, Hal ou Overijse[1]. Dans ces circonstances, des zones couvertes par cette 5G light débordent sur le territoire de la Région bruxelloise, particulièrement dans la zone Sud avec notamment Uccle et Forest, deux communes qui ont récemment demandé un moratoire de ce déploiement.

En Wallonie, Proximus a annoncé en date du lundi 20 avril 2020 avoir suspendu provisoirement le déploiement de sa 5G light dans plusieurs communes concernées par ce lancement: Ottignies-Louvain-la-Neuve, Châtelet, Namur, Tournai ou Arlon. Il apparaît cependant que cette suspension ne touche pas la Flandre et donc indirectement Bruxelles puisque les possibles émissions de 5G light qui se produiraient sur le territoire de la Région bruxelloise proviendraient de communes voisines flamandes.

En parallèle, le 31 janvier, l'Institut belge des services postaux et des télécommunications (IBPT) avait proposé d'octroyer des droits d'utilisation provisoires pour les réseaux 5G pour permettre le déploiement de cette technologie malgré le blocage politique. Le 24 mars, l'IBPT a précisé que 5 sociétés étaient prises en compte pour l'octroi d'une licence 5G provisoire: Cegeka, Entropia, Orange, Proximus et Telenet.

Dans ce contexte où la clarté et la transparence ne règnent pas à l'heure actuelle, où l'incertitude plane quant à la sécurité et au contexte géopolitique, il semble essentiel de rappeler, à travers l'adoption de cette proposition de résolution, la réflexion générale et les principes fondamentaux qui doivent baliser un éventuel déploiement de la 5G en Belgique.

door toedoen van een bijzondere commissie die ermee zou worden belast te analyseren, adviezen te geven, te valideren en voorstellen te doen.

Onlangs, op woensdag 1 april 2020, heeft Proximus aangekondigd dat het in België een 5G *light* zou lanceren, eerst in een dertigtal gemeenten verspreid over het land. Dat was voorbarig, gezien de vele onzekerheden inzake zowel de gevolgen voor de gezondheid als de veiligheid en het ontbreken van krijtlijnen voor een internationaal kader.

Het Brussels Hoofdstedelijk Gewest is daar niet rechtstreeks bij betrokken omdat het strengere stralingsnormen hanteert dan het Vlaams Gewest en het Waals Gewest. Meerdere aan het Brussels Hoofdstedelijk Gewest grenzende gemeenten zijn echter wel betrokken, onder meer Zaventem, Sint-Pieters-Leeuw of Overijse[1]. In die omstandigheden reikt de dekking van dat 5G-light-netwerk tot op het grondgebied van het Brussels Hoofdstedelijk Gewest, in het bijzonder het zuidelijk deel ervan, waar zich onder meer Ukkel en Vorst bevinden, twee gemeenten die onlangs een moratorium op die uitrol hebben gevraagd.

Wat Wallonië betreft, heeft Proximus op 20 april 2020 aangekondigd in een aantal gemeenten waar het 5G-light-netwerk zou worden opgestart (Ottignies-Louvain-la-Neuve, Châtelet, Namen, Doornik en Aarlen), de uitrol voorlopig te hebben opgeschort. Het ziet er echter naar uit dat die opschorting niet van toepassing is in Vlaanderen en onrechtstreeks dus ook niet in Brussel, aangezien op het grondgebied van het Brussels Hoofdstedelijk Gewest mogelijk vanuit de Vlaamse buurgemeenten afkomstige 5G-light-straling zou kunnen voorkomen.

Tegelijk heeft op 31 januari het Belgisch instituut voor postdiensten en telecommunicatie (BIPT) voorgesteld voorlopige gebruiksrechten voor de 5G-netwerken toe te kennen, teneinde de uitrol van die technologie mogelijk te maken, ondanks de blokkering op politiek niveau. Op 24 maart heeft het BIPT aangegeven dat vijf bedrijven in aanmerking kwamen voor de toekenning van een voorlopige 5G-licentie, namelijk Cegeka, Entropia, Orange, Proximus en Telenet.

Aangezien er momenteel een gebrek aan duidelijkheid en transparantie heerst en er veel onzekerheid bestaat aangaande de veiligheid en de geopolitieke context, lijkt het van wezenlijk belang om via de aanneming van dit voorstel van resolutie te wijzen op de algemene overwegingen en op de fundamentele beginselen die aan een eventuele uitrol van het 5G-netwerk in België ten grondslag moeten liggen.

1 Carte: *https://bx1.be/news/proximus-lance-la-5g-dans-plus-de-30-communes-dont-certaines-autour-de-bruxelles/*

1 Kaart: *https://bx1.be/news/proximus-lance-la-5g-dans-plus-de-30-communes-dont-certaines-autour-de-bruxelles/*.

Nous demandons notamment la suspension de toutes les décisions prises par l'IBPT concernant les projets d'octroi de droits d'utilisation provisoires début 2020 et que celles-ci soient conditionnées à des études d'impact, des concertations et des enquêtes publiques. Nous chargeons le gouvernement de réaliser toutes les études d'impacts nécessaires, les analyses de sécurité et la consultation au préalable à toute décision d'octroi de licence ou d'autorisation pour toute activité d'exploitation.

Il est à noter qu'au-delà de l'aspect sanitaire et sécuritaire, il existe d'autres problématiques qui inquiètent l'opinion publique pour ce qui est de la 5G: la question des éventuelles répercussions sur l'environnement, la question des personnes hyper-sensibles aux ondes, l'accentuation fort probable d'une fracture numérique ou encore la question d'une société hyperconnectée au bord du burn-out.

De indieners vragen daarom onder andere dat alle in het begin van 2020 door het BIPT genomen beslissingen aangaande de plannen voor de toekenning van voorlopige gebruiksrechten worden opgeschort en dat zij onderworpen worden aan de voorwaarde dat effectbeoordelingen worden uitgevoerd en dat overleg en openbare onderzoeken plaatsvinden. Voorts wordt de regering verzocht om vóór elke beslissing tot toekenning van een licentie of tot verlening van een vergunning voor om het even welke uitbatingsactiviteit alle nodige effectbeoordelingen en veiligheidsanalyses uit te voeren, alsook de nodige raadplegingen te houden.

Er moet worden aangestipt dat, naast de gezondheids- en veiligheidsaspecten, ook andere vraagstukken in verband met 5G de publieke opinie zorgen baren, namelijk de eventuele weerslag op het milieu, de situatie van de mensen die uiterst gevoelig zijn voor straling, het feit dat de digitale kloof heel waarschijnlijk groter zal worden en het probleem van een hypergeconnecteerde samenleving waar burn-out lonkt.

PROPOSITION DE RÉSOLUTION

La chambre des representants:

A. considérant que la 5G aura pour effet de transformer le secteur des télécommunications en fournisseurs de services essentiels pour de nombreux secteurs de la société, à la différence de la 4G;

B. considérant que, pour la mise en place de la 5G, un rehaussement des normes d'émission d'ondes électromagnétiques pour les antennes GSM sera impératif dans certaines régions et que celui-ci inquiète un grand nombre d'acteurs de la société civile tant en matière de santé que d'environnement;

C. considérant la difficulté voire l'impossibilité d'évaluer objectivement les effets sanitaires d'un déploiement massif à grande échelle de la 5G;

D. considérant toutefois la légitimité des interrogations en matière de santé et d'impact environnemental liées au déploiement potentiel de la 5G et la nécessité d'y apporter des réponses;

E. considérant que la nouvelle architecture et la virtualisation accroissent la complexité et la dépendance concernant les logiciels et leurs mises à jour dans le réseau et que tout opérateur de réseau sera davantage dépendant de ses fournisseurs et des gestionnaires de réseau externes;

F. considérant les menaces à l'égard de la disponibilité, de la confidentialité et de l'intégrité du réseau 5G;

G. considérant l'importance d'opter pour des fournisseurs qui prennent au sérieux le développement, les tests et les correctifs des logiciels et d'imposer ces critères dans le choix des fournisseurs;

H. considérant que le CCB (Centre pour la Cybercriminalité de Belgique) prépare un guide qui porte aussi bien sur la sécurité de la chaîne d'approvisionnement que sur la sécurité du cycle de vie à l'égard de la gestion de systèmes dans ce type de réseau;

I. considérant que l'Union européenne a publié le 31 décembre 2019 une boîte à outils pour les États, certes non contraignante mais dont il faut tenir compte pour la sécurité de l'État;

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. wijst erop dat met 5G, anders dan met 4G, de telecomsector voor tal van maatschappelijke sectoren een levensnoodzakelijke dienstverlener zal worden;

B. merkt op dat voor de uitrol van 5G de elektromagnetische-stralingsnormen voor de gsm-masten in bepaalde gebieden zullen moeten worden verhoogd en dat zulks tot bezorgdheid leidt bij veel middenveldactoren zowel op het vlak van milieu als inzake de gezondheid;

C. stipt aan dat het moeilijk of zelfs onmogelijk is de gezondheidsgevolgen van een massale uitrol van 5G objectief te evalueren;

D. vindt de vragen in verband met de gezondheid en met de milieu-impact die met de mogelijke uitrol van 5G gepaard gaan, volstrekt legitiem en stelt dat daarop antwoorden moeten worden aangereikt;

E. geeft aan dat de nieuwe architectuur en de virtualisatie leiden tot een grotere complexiteit en afhankelijkheid van software en van software-updates in het netwerk, en dat elke netwerkoperator almaar meer afhankelijk zal worden van zijn leveranciers en van de externe netwerkbeheerders;

F. vestigt de aandacht op de dreigingen ten opzichte van de beschikbaarheid, de vertrouwelijkheid en de integriteit van het 5G-netwerk;

G. acht het belangrijk dat wordt gekozen voor leveranciers die de softwareontwikkeling, *-testing* en *-patching* ernstig nemen, en dat bij de keuze van de leveranciers de verplichting zal gelden met die criteria rekening te houden;

H. geeft aan dat het Centrum voor Cybersecurity België (CCB) een leidraad uitwerkt die betrekking heeft op de veiligheidsaspecten van zowel de *supply chain* als de *life cycle* voor het beheer van systemen in dergelijke netwerken;

I. merkt op dat de Europese Unie op 31 december 2019 ten behoeve van de lidstaten een *toolbox* heeft uitgebracht, die weliswaar niet verplicht is, maar waarmee voor de veiligheid van de Staat rekening moet worden gehouden;

J. considérant que la Commission européenne et ENISA (Agence européenne de la cybersécurité) sont en train de créer un cadre de sécurité sur la base du règlement relatif à la cybersécurité et encourageront les États membres à accorder la priorité à l'élaboration d'un schéma de certification pour les réseaux et applications de la 5G mais que celui-ci n'est pas encore prêt;

K. considérant que l'espionnage technique par l'utilisation abusive de l'infrastructure tirera profit de possibilités sans précédent si aucune balise et aucun cadre légal ne sont mis en place pour améliorer la protection des données des autorités publiques et des secrets d'affaires, de la vie privée et des infrastructures critiques;

L. considérant la perte d'indépendance stratégique et économique qui signifie que, pour tous les secteurs dépendant de la 5G, il existe, pour ainsi dire, un bouton marche/arrêt dans un pays tiers et certains ont déjà prouvé qu'ils adoptaient une cyberpolitique agressive;

M. considérant que, lié à cette dépendance stratégique, en découle un problème d'ingérence qui consiste à utiliser des mécanismes d'influence abusifs pour exercer des pressions sur des processus décisionnels souverains;

N. considérant que la situation géostratégique des entreprises auxquelles le déploiement de la 5G est confié est aussi, voire plus, importante que les failles techniques et qu'il est donc crucial pour l'État de choisir des partenaires fiables;

O. considérant que, avec le déploiement de la 5G, les techniques d'écoute actuelles dont dispose la police fédérale sont compromises et qu'il sera beaucoup plus difficile, voire impossible, de les mettre en œuvre à l'avenir compte tenu de l'architecture du réseau 5G;

P. considérant que les difficultés liées aux interceptions légales trouvent leur origine dans le cryptage des messages de communication et le cryptage du numéro d'identité international d'abonné mobile, ce qui pose de grandes difficultés en matière de sécurité et singulièrement dans la lutte contre le terrorisme;

Q. considérant qu'il faut établir un cadre légal en amont afin de développer les outils nécessaires aux services de police pour garantir la sécurité;

R. considérant que les services de renseignement recommandent vivement de rechercher un partenaire fiable et de faire appel à plusieurs fournisseurs pour un

J. wijst erop dat de Europese Commissie en het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) momenteel een veiligheidskader uitwerken op basis van de cyberveiligheidsverordening en dat ze de lidstaten ertoe zullen aanmoedigen prioriteit te geven aan een certificeringsregeling voor 5G-netwerken en -apparatuur, maar dat die laatste nog niet klaar is;

K. wijst erop dat technische spionage middels misbruik van de infrastructuur van ongeziene mogelijkheden zal profiteren indien geen enkele afbakening noch enig wettelijk kader wordt opgezet voor een betere bescherming van de overheidsgegevens, de bedrijfsgeheimen, de persoonlijke levenssfeer en de kritieke infrastructuur;

L. wijst op het verlies van strategische en economische onafhankelijkheid, wat betekent dat voor alle van 5G afhankelijke sectoren als het ware een aan/uit-knop in een derde land staat, en attendeert erop dat sommige landen al hebben bewezen er een zeer agressief cyberbeleid op na te houden;

M. wijst erop dat, gerelateerd aan die strategische afhankelijkheid, uit een en ander een inmengingsprobleem voortvloeit, dat bestaat in de aanwending van oneigenlijke beïnvloedingsmechanismen om druk uit te oefenen op soevereine beslissingsprocessen;

N. wijst erop dat de geostrategische situatie van de ondernemingen die tot taak krijgen 5G uit te rollen al even belangrijk of zelfs belangrijker is dan de technische zwakheden, en dat het voor de Staat dus van cruciaal belang is dat hij betrouwbare partners kiest;

O. wijst erop dat met de uitrol van 5G de huidige afluistertechnieken waarover de federale politie beschikt in het gedrang komen en dat ze, gelet op de architectuur van het 5G-netwerk, in de toekomst veel moeizamer of zelfs helemaal niet meer zullen kunnen worden uitgevoerd;

P. wijst erop dat de moeilijkheden inzake *lawful intercepts* terug te voeren zijn op de versleuteling van de communicatieboodschappen en op de versleuteling van het IMSI-abonneenummer (waarbij IMSI staat voor *International Mobile Subscriber Identity*, te weten het identiteitsnummer ten behoeve van internationale mobiliteit) en dat dit ernstige veiligheidsmoeilijkheden doet rijzen, inzonderheid in de strijd tegen terrorisme;

Q. wijst erop dat eerst een wettelijk kader moet worden opgezet, met de bedoeling de voor de politie benodigde middelen te ontwikkelen om de veiligheid te waarborgen;

R. wijst erop dat de inlichtingendiensten ten stelligste aanraden om uit te kijken naar een betrouwbare partner en om voor een 5G-netwerk een beroep te doen op

réseau 5G afin de réduire le risque de formation d'un monopole;

S. considérant que l'initiative unilatérale de Proximus pour le lancement de sa 5G *light* est prématuré compte tenu de l'absence de cadre légal et de balises pour le déploiement de la 5G;

T. considérant que la problématique de la 5G est d'intérêt public et concerne les intérêts essentiels des citoyens;

U. considérant que, pour pallier le problème causé par l'absence de gouvernement fédéral de plein exercice (et l'absence d'accord avec les Communautés), l'IBPT a invité les opérateurs à se porter candidats à des droits d'utilisation provisoires pour un déploiement initial de la 5G en Belgique dans la bande 3600-3800 MHz et que, en plein confinement dans le cadre de la crise sanitaire de la pandémie du COVID-19, il a annoncé une consultation publique devant s'achever le 21 avril 2020 et ensuite la prise des décisions individuelles d'octroi des licences provisoires pour le déploiement de la 5G en rapport avec les cinq candidatures valablement reçues;

V. considérant le Règlement de la Chambre des représentants, en son chapitre VIII, section 5, article 39, qui permet la création d'une commission spéciale.

Demande au gouvernement fédéral:

1. de réaliser si nécessaire et de mettre à disposition les études basées sur des critères objectifs sanitaires, environnementaux et de sécurité nationale afin d'analyser l'impact de la 5G préalablement à toute décision d'octroi de licence ou d'activité d'exploitation;

2. d'assurer le devoir évident, d'une part, de transparence quant aux résultats de ces études et à l'état des lieux des contacts avec les différents acteurs du dossier et, d'autre part, d'une communication claire des intentions de l'exécutif;

3. de fournir toutes les informations utiles à une "commission spéciale" qui serait créée par la Chambre des représentants et chargée, concernant le déploiement de la 5G sur le territoire, les demandes d'autorisation de toute activité d'exploitation d'équipements radioélectriques et

meerdere leveranciers teneinde het risico op monopolievorming te verminderen;

S. wijst erop dat het eenzijdige initiatief van Proximus om een 5G *light*-netwerk te lanceren voorbarig is, gelet op het ontbreken van een wettelijk kader en van afbakenende maatregelen voor de uitrol van 5G;

T. wijst erop dat het 5G-vraagstuk van openbaar belang is en betrekking heeft op voor de burger essentiële belangen;

U. wijst erop dat het Belgisch instituut voor postdiensten en telecommunicatie (BIPT), om het probleem te ondervangen dat ons land geen federale regering met volheid van bevoegdheden heeft (en er dus ter zake ook geen overeenkomst bestaat met de gemeenschappen), de operatoren ertoe heeft opgeroepen zich kandidaat te stellen voor het verkrijgen van voorlopige gebruiksrechten met het oog op de introductie van 5G in de 3600-3800 MHz-band in België, alsook dat het BIPT, in volle *lockdown* als gevolg van de door het COVID-19-virus veroorzaakte gezondheidscrisis, een openbare raadpleging heeft aangekondigd met als einddatum 21 april 2020, gevolgd door individuele besluiten over de toekenning van voorlopige licenties voor de uitrol van 5G ten gunste van de vijf ontvankelijke kandidaturen;

V. wijst op het Reglement van de Kamer van volksvertegenwoordigers, hoofdstuk VIII, afdeling 5, artikel 39, dat het mogelijk maakt een bijzondere commissie op te richten;

Verzoekt de federale regering:

1. indien nodig de nodige onderzoeken uit te voeren op grond van objectieve criteria inzake gezondheid, milieu en nationale veiligheid en ze ter beschikking te stellen, teneinde de impact van 5G te analyseren voordat enige beslissing wordt genomen inzake de toekenning van een exploitatievergunning of inzake het opstarten van een exploitatieactiviteit;

2. de voor de hand liggende plicht na te komen inzake eensdeels de transparantie aangaande de resultaten van die onderzoeken en de stand van zaken omtrent de contacten met de diverse actoren in het dossier, en anderdeels een duidelijke communicatie over de voornemens van de regering;

3. alle nuttige inlichtingen te verstrekken aan een bijzondere commissie die zou worden opgericht door de Kamer van volksvertegenwoordigers en die, met betrekking tot de uitrol van 5G op het Belgisch grondgebied, de vergunningsaanvragen inzake enigerlei activiteit op

d'octroi de licences, préalablement aux décisions qui seront prises par le gouvernement fédéral:

a. d'analyser et d'évaluer les demandes;

b. de rendre des avis;

c. de faire des propositions;

d. d'assurer la concertation avec les régions, les intervenants du monde académique ou encore la société civile;

4. de suspendre toutes les décisions prises par l'IBPT concernant les projets d'octroi de droits d'utilisation provisoires début 2020 et de conditionner celles-ci à des études d'impact, des analyses de sécurité, des concertations et des enquêtes publiques;

5. de prévoir, préalablement à toute activité d'exploitation d'équipements radioélectriques et de toute licence, la nécessité d'une demande d'autorisation de la part des opérateurs au gouvernement fédéral; celle-ci ne pourra être accordée qu'après la réalisation d'études d'impact, d'analyses et de consultations; le gouvernement fédéral pourra ainsi s'assurer de la sûreté et de la sécurité de l'État et garder le contrôle quant au choix de partenaires fiables; cette liste des équipements autorisés devra être publiée et mise à jour régulièrement;

6. d'établir un cadre légal répondant aux besoins exprimés par les différents services de police européens;

7. de prendre les mesures nécessaires pour continuer à permettre les interceptions légales avant de déployer la 5G sur notre territoire et ainsi donner à la police fédérale les outils nécessaires à notre sécurité et en particulier dans la lutte contre le terrorisme;

8. de réglementer le déploiement de la 5G en tenant compte des diverses recommandations faites notamment par l'Union européenne.

11 mai 2020

Vanessa MATZ (cdH)
Maxime PREVOT (cdH)
Josy ARENS (cdH)

het vlak van de exploitatie van radioapparatuur en de toekenning van licenties, voordat de federale regering beslissingen neemt, ermee zou worden belast:

a. de aanvragen te onderzoeken en te beoordelen;

b. adviezen uit te brengen;

c. voorstellen te formuleren;

d. te overleggen met de gewesten, de actoren van de academische wereld en het middenveld;

4. alle beslissingen op te schorten die het BIPT begin 2020 heeft genomen inzake de toekenningsplannen van voorlopige gebruiksrechten en deze beslissingen te onderwerpen aan de voorwaarde dat effectbeoordelingen en veiligheidsanalyses worden uitgevoerd en dat overleg en de openbare raadplegingen plaatsvinden;

5. te bepalen dat de operatoren bij de federale regering een vergunningsaanvraag moeten indienen voordat zij van start gaan met enige activiteit omtrent de exploitatie van radioapparatuur en voordat enige licentie wordt toegekend; die vergunning kan pas worden verleend na de uitvoering van effectbeoordelingen, analyses en raadplegingen; aldus kan de federale regering zich vergewissen van de veiligheid en van de veiligheid van de Staat en kan ze erop toezien dat betrouwbare partners worden gekozen; deze lijst van de toegestane apparatuur moet worden bekendgemaakt en geregeld bij de tijd worden gebracht;

6. te voorzien in een wettelijk raamwerk dat tegemoetkomt aan de noden van de diverse Europese politiediensten;

7. voordat het 5G-netwerk op ons grondgebied wordt uitgerold de vereiste maatregelen te nemen zodat de wettelijke intercepties mogelijk blijven en aldus aan de federale politie de instrumenten te verschaffen die nodig zijn voor onze veiligheid en in het bijzonder voor de bestrijding van terrorisme;

8. de uitrol van 5G te reglementeren met inachtneming van de diverse aanbevelingen die onder meer door de Europese Unie werden geformuleerd.

11 mei 2020

Imprimerie centrale – Centrale drukkerij