DOC 54 **1591/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

18 januari 2016

VOORSTEL VAN RESOLUTIE

betreffende de opvoering van de strijd tegen het radicalisme op internet

(ingediend door mevrouw Vanessa Matz en de heren Georges Dallemagne en Benoît Lugen)

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

18 janvier 2016

PROPOSITION DE RÉSOLUTION

visant à renforcer la lutte contre le radicalisme sur Internet

(déposée par Mme Vanessa Matz et MM. Georges Dallemagne et Benoît Lutgen)

N-VA	:	*Nieuw-Vlaamse Alliantie*
PS	:	*Parti Socialiste*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
Open Vld	:	*Open Vlaamse liberalen en democraten*
sp.a	:	*socialistische partij anders*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
cdH	:	*centre démocrate Humaniste*
VB	:	*Vlaams Belang*
PTB-GO!	:	*Parti du Travail de Belgique – Gauche d'Ouverture*
DéFI	:	*Démocrate Fédéraliste Indépendant*
PP	:	*Parti Populaire*

Afkortingen bij de nummering van de publicaties:

DOC 54 0000/000:	*Parlementair document van de 54e zittingsperiode + basisnummer en volgnummer*
QRVA:	*Schriftelijke Vragen en Antwoorden*
CRIV:	*Voorlopige versie van het Integraal Verslag*
CRABV:	*Beknopt Verslag*
CRIV:	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN:	*Plenum*
COM:	*Commissievergadering*
MOT:	*Moties tot besluit van interpellaties (beigekleurig papier)*

Abréviations dans la numérotation des publications:

DOC 54 0000/000:	*Document parlementaire de la 54e législature, suivi du n° de base et du n° consécutif*
QRVA:	*Questions et Réponses écrites*
CRIV:	*Version Provisoire du Compte Rendu intégral*
CRABV:	*Compte Rendu Analytique*
CRIV:	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN:	*Séance plénière*
COM:	*Réunion de commission*
MOT:	*Motions déposées en conclusion d'interpellations (papier beige)*

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

Bestellingen:
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.dekamer.be
e-mail : publicaties@dekamer.be

De publicaties worden uitsluitend gedrukt op FSC gecertificeerd papier

Publications officielles éditées par la Chambre des représentants

Commandes:
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.lachambre.be
courriel : publications@lachambre.be

Les publications sont imprimées exclusivement sur du papier certifié FSC

TOELICHTING

DAMES EN HEREN,

De informatie- en communicatietechnologie overheerst onze moderne samenleving. Een wereld zonder internet is vandaag haast ondenkbaar. Het is moeilijk of zelfs onmogelijk geworden het te stellen zonder internet en zonder de vele mogelijkheden en informatiebronnen die het biedt. Jammer genoeg hebben die technologieën niet alleen voordelen. Het internet is ook een plek waar men allerhande misstanden en excessen vindt.

De terroristische groeperingen halen voordeel uit de technologische vooruitgang om jongeren te benaderen via andere kanalen, meer bepaald de sociale netwerken, de videokanalen en de internetfora. Zij verspreiden hun propaganda breder, sneller en doeltreffender dan ooit. Internet is het radicaliseringskanaal bij uitstek en het nieuwe wingebied van de terroristen. In 91 % van de gevallen blijken de terroristen overigens te werk te zijn gegaan via het internet[1].

De computernetwerken maken een individuele benadering mogelijk. Men zou kunnen spreken van "binnenhuisradicalisering". De internetgebruikers kunnen binnen de beslotenheid van hun woning toegang krijgen tot extreme inhoud, terwijl geradicaliseerde personen makkelijk contact kunnen leggen met mensen die vatbaar zijn voor radicalisering. Vooral de leeftijdsgroep 15-21 jaar blijkt voor dergelijke ideeën open te staan: die is namelijk goed voor 63 % van de kandidaat-jihadstrijders[2].

De terroristische dreiging heeft zodoende geleidelijk andere vormen aangenomen en gaat voortaan uit van kleinere groepen, cellen en eenlingen die in Europa wonen en die vrijer en onvoorspelbaarder opereren. Zij worden niet of nauwelijks aangestuurd door een welbepaalde organisatie, maar bereiden op eigen houtje aanvallen voor, wat preventie en detectie veel moeilijker maakt.

Terrorisme en gewelddadig radicalisme vormen ernstige bedreigingen voor onze veiligheid, voor de democratische waarden en voor de rechten en vrijheden van onze burgers. Niet alleen kosten die aanslagen mensenlevens en veroorzaken ze materiële schade, ze zaaien ook tweedracht tussen de gemeenschappen en leiden tot steeds extremere opinies in de samenleving.

1 D. Bouzarsur, "*Le profil des djihadistes français*".
2 *Idem*.

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

Les technologies de l'information et de la communication dominent nos sociétés modernes. Un monde sans réseau est aujourd'hui quasiment inimaginable. Il est devenu difficile, voire impossible, de se passer d'Internet et des nombreuses possibilités et sources d'information qu'il présente. Malheureusement, ces technologies ne comportent pas que des avantages. Internet est également un lieu où abus et excès en tout genre se rencontrent.

Les groupes terroristes tirent parti des progrès technologiques pour trouver de nouvelles façons d'approcher les jeunes en utilisant les réseaux sociaux, les canaux vidéo et les discussions en ligne. Ils diffusent leur propagande plus largement, plus rapidement et plus efficacement qu'auparavant. Internet est le canal par excellence de radicalisation et le nouveau mode de recrutement des terroristes. Il est d'ailleurs privilégié par ces derniers dans 91 % des cas[1].

Les réseaux informatiques permettent une individualisation de l'offre. On parle de "radicalisation en chambre". Les utilisateurs peuvent accéder à des contenus extrêmes dans l'intimité de leur domicile et les personnes radicalisées peuvent communiquer aisément avec des personnes qui présentent un risque de radicalisation. La tranche des 15-21 ans est la plus touchée, ils représentent 63 % des candidats au djihad[2].

La menace terroriste a, de ce fait, évolué et provient désormais aussi de plus petits groupes, de cellules et d'individus isolés, établis en Europe et qui fonctionnent de façon plus libre et plus imprévisible. Pas ou peu dirigés par une organisation précise, ils préparent des attaques de manière autonome, ce qui rend la prévention et la détection plus difficiles.

Le terrorisme et la radicalisation violente constituent des menaces sérieuses pour notre sécurité, pour les valeurs démocratiques et pour les droits et libertés de nos citoyens. Ils n'entraînent pas seulement pertes en vies humaines et dégâts matériels; ils sèment également le germe de la division entre les communautés, suscitant des opinions de plus en plus extrêmes dans la société.

1 D. Bouzarsur, "Le profil des djihadistes français".
2 *Idem*.

Om daaraan het hoofd te bieden, draagt de Staat de verantwoordelijkheid om doeltreffend op te treden, doch zonder de vrijheden van zijn burgers in te perken. Wij moeten deze strijd voeren en tegelijkertijd waken over de fundamentele rechten die ten grondslag liggen aan onze democratische samenleving. Op grond van het evenredigheidsbeginsel is een juist evenwicht nodig tussen de met een repressief optreden gepaard gaande vereisten en de inachtneming van de fundamentele rechten en vrijheden, zoals het recht om zonder inmenging een mening te koesteren, het recht op vrijheid van meningsuiting (inclusief de vrijheid om opzoekingen te doen, informatie en ideeën te vergaren en ze door te spelen), alsmede het recht op eerbiediging van het privéleven.

De klassieke repressietechnieken volstaan niet om de ontwikkeling van de radicaliseringstrends het hoofd te bieden. Om een en ander te voorkomen en te bestrijden, is een omvattender aanpak nodig.

Dit voorstel van resolutie behelst precies een pleidooi om de strijd tegen het radicalisme op internet op te voeren. Volgens de indieners moet een en ander zijn beslag krijgen op drie niveaus: toezicht en opsporing, de verwijdering van "illegale inhoud" en de uitbouw van een tegendiscours.

I. **Een aangescherpte opsporing en monitoring met het oog op een doeltreffend toezichtsbeleid**

Het toezicht is een essentieel element om toekomstige terroristische handelingen te voorkomen en de verspreiding van terroristische propaganda tegen te gaan.

De indieners van dit voorstel van resolutie zijn van mening dat de opsporing en het toezicht moeten worden aangescherpt. Het komt erop aan te voorzien in een grotere nationale capaciteit om terrorisme te voorkomen, zich tegen terrorisme te beschermen en de gevolgen ervan op te vangen, meer bepaald door de informatie op het internet beter te verzamelen en te analyseren.

De financiële en structurele middelen waarover de met de cyberveiligheid belaste instanties beschikken, volstaan hoegenaamd niet om de veiligheid van onze cyberruimte te garanderen en om een volwaardige strategie te ontwikkelen waarmee de cybercriminelen doeltreffend kunnen worden bestreden.

De indieners betreuren in het bijzonder dat het zoveel tijd vergt vóór het Centrum voor Cybersecurity België een feit is. Het koninklijk besluit waarbij dit centrum

Pour y faire face, l'État a la responsabilité de mener une action efficace sans toutefois limiter les libertés de ses citoyens. Nous devons mener cette lutte en préservant les droits fondamentaux qui fondent notre société démocratique. En vertu du principe de proportionnalité, un juste équilibre est nécessaire entre les intérêts de l'action répressive et le respect des droits et libertés fondamentales, tels que le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées, ainsi que le droit au respect de la vie privée.

Les techniques traditionnelles de répression sont insuffisantes pour faire face à l'évolution des tendances en matière de radicalisation. Une approche plus large est nécessaire pour prévenir ce phénomène et le combattre.

La présente proposition de résolution a précisément pour objet de renforcer la lutte contre le radicalisme sur Internet. Les auteurs considèrent que les actions doivent être menées sur trois plans: la surveillance et la détection, le retrait des "contenus illégaux" et l'organisation d'un contre-discours.

I. **Renforcer la détection et le monitoring pour une politique de surveillance efficace**

La surveillance constitue un élément essentiel pour prévenir de futurs actes terroristes et empêcher la diffusion de la propagande terroriste.

Les auteurs de la présente proposition de résolution estiment que la détection et la surveillance doivent être renforcées. Il est nécessaire de consolider la capacité, au niveau national, à prévenir le terrorisme, s'en protéger et remédier à ce phénomène y compris en améliorant la collecte et l'analyse d'informations sur Internet.

Les moyens financiers et structurels dont disposent les instances chargées de la cybersécurité sont largement insuffisants pour assurer la sécurité de notre cyberespace ainsi que pour développer une véritable stratégie à même de lutter efficacement contre les cybercriminels.

Les auteurs déplorent en particulier le temps nécessaire à la mise en place du centre de cybersécurité national. Si l'arrêté royal créant le centre a été adopté

werd opgericht, dateert van 10 oktober 2014[3] maar het centrum is nog steeds niet operationeel.

Tijdens de parlementaire besprekingen heeft de regering een budget aangekondigd van ongeveer 8 miljoen euro voor de indienstneming van bijkomend personeel, plus extra investeringen op het vlak van opsporing en bescherming, waaronder de oprichting van het Centrum voor Cybersecurity België[4]. Het blijkt echter dat in 2015 slechts 900 000 euro beschikbaar zal zijn voor de lancering van het centrum[5]. Dat bedrag is ruimschoots onvoldoende.

De indieners vinden dat het budget van 8 miljoen euro dringend moet worden vrijgemaakt om het Centrum voor Cybersecurity operationeel te maken. Er zijn daartoe krachtige en doeltreffende beslissingen nodig. In dit verband werd overigens een specifiek voorstel van resolutie ingediend[6].

De oprichting van het Centrum voor Cybersecurity zal echter niet volstaan om radicalisering en terroristische propagandavoering via het internet een halt toe te roepen.

De recente besparingen waartoe de regering heeft beslist, beknotten de slagkracht van de instanties die ter zake moeten optreden. De indieners hekelen de besparingen in essentiële sectoren zoals de politie (- 9,6 % van het totale budget in 2015), het gerecht (- 13 % van het totale budget in 2015), de Veiligheid van de Staat (- 9,8 % tussen 2013 en 2015 voor de personeelsuitgaven en - 26 % tussen 2015 en 2019 voor de investeringsuitgaven) en het Coördinatieorgaan voor de dreigingsanalyse (- 29 % tussen 2015 en 2019 voor de personeelsuitgaven)[7].

De indieners vragen méér personele en technische middelen voor de verschillende diensten die belast zijn met de controle op het internet en met risicoanalyse en -opsporing. Om gespecialiseerde profielen te kunnen aantrekken, zijn investeringen nodig die het mogelijk maken de dreiging doeltreffend aan te pakken.

3 Koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België, *Belgisch Staatsblad,* 21 november 2014.

4 Beleidsverklaring van de eerste minister, 14 november 2014, DOC 54-0020/015.

5 CRABV 54-COM/051, Beknopt verslag – Commissie voor de Binnenlandse Zaken, de Algemene Zaken en het Openbaar Ambt, Antwoord van de eerste minister op de vraag van de heer G. Dallemagne (nr. 984) en de heer P. Buysrogge (nr. 1093), 13 januari 2015, blz. 8.

6 G. DALLEMAGNE, Voorstel van resolutie over de aanscherping van de cyberveiligheid in België, 16 september 2014, DOC 54-0257/001.

7 Ontwerp van algemene uitgavenbegroting 2015, 13 november 2014, DOC 54 0496/001-002.

le 10 octobre 2014[3], ce dernier n'est toujours pas opérationnel.

Dans le cadre des débats parlementaires, le gouvernement a annoncé un budget d'environ 8 millions d'euros pour l'engagement de personnel supplémentaire ainsi que des investissements additionnels sur le plan de la détection et de la protection, dont la création du centre belge de cybersécurité[4]. Il semble cependant que seul 900 000 euros seront disponibles en 2015 pour le lancement du centre.[5] Ce montant est largement insuffisant.

Les auteurs considèrent qu'il est urgent de dégager le budget de 8 millions d'euros et de rendre opérationnel le centre de cybersécurité. Il est impératif de prendre des décisions fortes et efficaces dans ce domaine. Une proposition de résolution spécifique a d'ailleurs été déposée à cet égard.[6]

La seule création du centre de cybersécurité ne sera cependant pas suffisante pour répondre à la problématique de la radicalisation et de la propagande terroriste sur Internet.

Les récentes économies décidées par le gouvernement mettent à mal l'action des autorités en la matière. Les auteurs dénoncent les économies réalisées dans des services essentiels, à savoir la police (- 9,6 % du budget total en 2015), la justice (- 13 % du budget total en 2015), la sûreté de l'État (- 9,8 % entre 2013 et 2015 pour les dépenses relatives au personnel et - 26 % entre 2015 et 2019 pour les dépenses en investissement) et l'Organe de coordination pour l'analyse de la menace (- 29 % entre 2015 et 2019 pour les dépenses en personnel).[7]

Les auteurs demandent l'augmentation des moyens humains et techniques au sein des différents services chargés de la surveillance d'Internet ainsi que de l'analyse et de la détection des risques. Le recrutement de profils spécialisés demande des investissements à la hauteur de la menace.

3 Arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité en Belgique, *M.B.*, 21 novembre 2014.

4 Exposé d'orientation politique du premier ministre, 14 novembre 2014, DOC 54-20/015.

5 CRABV 54-COM/051, Compte rendu analytique – Commission de l'Intérieur, des Affaires générales et de la Fonction publique, Réponse du premier ministre à la question de M. G. Dallemagne (n° 984) et M. P. Buysrogge (n° 1093), 13 janvier 2015, p. 8.

6 G. Dallemagne, Proposition de résolution visant à renforcer la cybersécurité en Belgique, 16 septembre 2014, DOC 54-257/001.

7 Projet du budget général des dépenses pour l'année budgétaire 2015, 13 novembre 2014, DOC 54 496/001-002.

II. **De juridische en technische mogelijkheden uitbouwen en verbeteren, met het oog op de verwijdering van illegale inhoud die terrorisme verheerlijkt**

Net als de "klassieke" media functioneert het internet niet in een juridisch vacuüm, maar is het onderworpen aan de beginselen van een rechtsstaat. Aangezien de internetactoren bij het uitoefenen van hun activiteiten op fysiek grondgebied gevestigd zijn, zijn krachtens het territorialiteitsbeginsel de op dat grondgebied vigerende rechtsregels van toepassing. Wat illegaal is offline, is dat ook online.

Het begrip "illegale inhoud" heeft betrekking op een voor de gehele bevolking verboden inhoud, ongeacht de gebruikte drager. Deze inhoudscategorie omvat onder meer de extreme vormen van geweld en het aanzetten tot haat of discriminatie. Er bestaat in het Belgische recht een geheel van regels dat het gebruik en de verspreiding van dergelijke boodschappen beperkt.

Zo is het krachtens artikel 140*bis* van het Strafwetboek strafbaar een boodschap te verspreiden of op enigerlei andere wijze ter beschikking te stellen van het publiek, met de bedoeling aan te zetten tot het plegen van een terroristisch misdrijf (terroristische propaganda).

De wetten ter bestrijding van racisme[8] en discriminatie[9] stellen het volgende strafbaar: aanzetten tot discriminatie, segregatie, haat of geweld tegen personen of groepen op grond van bepaalde kenmerken (nationaliteit, vermeend ras, huidskleur, afkomst, nationale of etnische herkomst, godsdienst of levensbeschouwing enzovoort).

Onder "aanzetten" moet worden verstaan elke verbale of non-verbale communicatie die anderen ertoe aanzet, stimuleert, aanmoedigt en oproept een bepaald gedrag aan te nemen, of dat gedrag aan te wakkeren, te versterken, te veroorzaken of uit te lokken. Het is echter niet noodzakelijk dat die aanzetting automatisch een reactie tot gevolg heeft, om verboden te zijn.

Het is wél noodzakelijk het frauduleuze gebruik van de informaticasystemen, de sociale netwerken en het internet in het algemeen te voorkomen, door ervoor te zorgen dat dergelijk gedrag strafbaar wordt gesteld. De indieners menen dat de procedures voor het verwijderen van illegale inhoud efficiënter moeten worden, evenals

8 Wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden, *Belgisch Staatsblad*, 8 augustus 1981.

9 Wet van 10 mei 2007 ter bestrijding van bepaalde vormen van discriminatie, *Belgisch Staatsblad,* 30 mei 2007.

II. **Renforcer et améliorer les possibilités juridiques et techniques permettant le retrait des contenus illégaux faisant l'apologie du terrorisme**

Internet, comme les médias classiques, opère dans un État de droit. Il ne se situe pas dans un vide juridique. Ses acteurs agissent à partir d'un territoire physique et par conséquent, en vertu du principe de territorialité, ce sont les règles juridiques en vigueur sur ce territoire qui seront d'application. Ce qui est illégal hors ligne reste illégal en ligne.

Le terme "contenu illégal" vise un contenu interdit à l'ensemble de la population, quel que soit le support utilisé. Cette catégorie de contenu englobe, entre autres, les formes extrêmes de violence et d'incitation à la haine ou à la discrimination. Il existe en droit belge un ensemble de règles qui limitent l'utilisation et la diffusion de ce type de messages. Ainsi,

— l'article 140*bis* du Code pénal érige en infraction la diffusion ou la mise à disposition du public de toute autre manière d'un message avec l'intention d'inciter à la commission d'une infraction terroriste (propagande terroriste);

— les lois anti-racisme[8] et anti-discrimination[9] érigent en infraction l'incitation à la discrimination, à la ségrégation, à la haine ou à la violence à l'encontre de personnes ou de groupes sur la base de certaines caractéristiques (la nationalité, la prétendue race, la couleur de peau, l'ascendance, l'origine nationale ou ethnique, la conviction religieuse ou philosophique, *etc.*).

L'incitation vise toute communication verbale ou non verbale qui incite à, stimule, attise, encourage, accentue, provoque, pousse ou appelle d'autres personnes à adopter un certain comportement. Il n'est cependant pas nécessaire que cette incitation entraîne d'office une réaction pour être interdite.

Il est nécessaire de prévenir l'usage frauduleux des systèmes informatiques, des réseaux sociaux et de l'Internet en général, en assurant l'incrimination de ces comportements. Les auteurs sont d'avis qu'il faut rendre plus efficaces les procédures de retrait des contenus illégaux ainsi que les enquêtes et la collecte de preuves

8 Loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme ou la xénophobie, *M.B.*, 8 août 1981.

9 Loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination, *M.B.*, 30 mai 2007.

de onderzoeken en het verzamelen van elektronische bewijzen die betrekking hebben op dergelijke informaticagelieerde misdrijven.

Hoewel de Staat en de internetproviders geval per geval samenwerken om illegale inhoud te verwijderen, is dat geen eenvoudige taak, aangezien veel internetsites buiten België gevestigd zijn.

De definitie van de strafbare feiten verschilt immers van land tot land en bijgevolg is het, zelfs indien de wetgeving van een land inhoud als illegaal beschouwt, mogelijk dat de auteur of de leverancier ervan zich buiten het bereik van de rechterlijke macht van dat land bevindt als hij opereert vanuit een land waar die inhoud als legaal wordt beschouwd. Bijgevolg kan moeilijk worden opgetreden tegen racistische, discriminerende of terroristische propaganda die van op buitenlandse websites wordt verspreid.

Gezien het grensoverschrijdende en internationale karakter van het internet is het van essentieel belang dat de lidstaten samenwerken, met name door bepaalde gemeenschappelijke minimumnormen in hun strafwetgeving te omschrijven. Derhalve verzoeken de indieners om de ratificatie van het aanvullend protocol bij het Verdrag van de Raad van Europa in verband met *cybercrime*[10]. Het protocol voorziet in een harmonisering van het materieel strafrecht bij de bestrijding van racisme en vreemdelingenhaat op het internet en in een betere internationale samenwerking ter zake.

Er moet ook worden gezorgd voor een nauwere samenwerking tussen de Staat en de belangrijkste internetactoren, opdat illegale inhoud wordt verwijderd.

Elke *webhost* heeft zijn eigen algemene gebruiksvoorwaarden, waarin hij de verboden inhoud omschrijft die kan worden verwijderd. De omvang van de online geplaatste inhoud is evenwel zo groot dat die bedrijven niet bij machte zijn alle illegale inhoud op te sporen. Voor de Staat is hier een rol weggelegd om de *webhosts* te helpen de illegale inhoud te identificeren.

Zo heeft het Verenigd Koninkrijk binnen Scotland Yard een specifieke cel opgericht die ermee belast is bedrijven als Google, Facebook en Twitter te wijzen op inhoud die volgens haar in strijd is met de gebruiksvoorwaarden van die bedrijven zelf en die daarom van het net zou moeten worden gehaald. Via die meldingsmethode zou 93 % van de aangegeven inhoud worden verwijderd,

[10] Aanvullend protocol bij het verdrag inzake cybercrime van de Raad van Europa ondertekend, dat betrekking heeft op het strafbaar stellen van racistische of xenofobe handelingen die met gebruik van computernetwerken worden gesteld, Straatsburg, 28 januari 2003.

électroniques portant sur de telles infractions liées aux systèmes informatiques.

L'État et les fournisseurs de services coopèrent sur une base *ad hoc* pour supprimer les contenus illégaux, mais cette tâche n'est pas simple car de nombreux sites Internet sont hébergés en dehors de la Belgique.

En effet, la définition des infractions varie d'un pays à l'autre et par conséquent, même si la législation d'un pays considère un contenu comme illégal, il se peut que l'auteur ou le fournisseur de celui-ci soit hors d'atteinte du pouvoir judiciaire de ce pays s'il agit à partir d'un pays où ce contenu est considéré comme légal. Il est, par conséquent, difficile d'intervenir contre la propagande raciste, discriminatoire ou terroriste diffusée depuis des sites étrangers.

Vu le caractère transfrontalier et international d'Internet, il est essentiel que les États collaborent, notamment en définissant certaines normes communes minimales dans leur législation pénale. À ce titre, les auteurs demandent la ratification du protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité.[10] Le protocole prévoit une harmonisation du droit pénal matériel dans la lutte contre le racisme et la xénophobie sur Internet ainsi que l'amélioration de la coopération internationale dans ce domaine.

La collaboration entre l'État et les acteurs clés de l'Internet doit, par ailleurs, être accrue pour assurer le retrait du contenu illégal.

Chaque hébergeur de site a ses propres conditions générales d'utilisation dans lesquelles il définit le contenu interdit susceptible être retiré. Ces compagnies ne sont cependant pas en mesure de détecter l'ensemble des contenus illégaux tant le volume est important. L'État a ici un rôle à jouer afin d'aider les hébergeurs de sites à identifier le contenu illégal.

Ainsi, le Royaume-Uni a créé une cellule spécifique au sein de Scotland Yard chargée de signaler auprès des sociétés telles que Google, Facebook, Twitter … les contenus qu'elle estime en contradiction avec les chartes d'utilisation de ces compagnies mêmes et qui devraient faire l'objet d'un retrait. A la suite de ces démarches, 93 % du contenu signalé serait retiré,

[10] Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, Strasbourg, 28 janvier 2003.

terwijl in het kader van dezelfde procedure slechts 33 % van de door gewone gebruikers aangegeven illegale inhoud zou worden verwijderd.

De indieners van dit voorstel van resolutie vinden dat het voorbeeld van het Verenigd Koninkrijk navolging verdient en dat België zich zou moeten toerusten met een bijzondere eenheid die als opdracht heeft illegale inhoud die van het net zou moeten worden gehaald, te melden aan de internetproviders. Die eenheid zou kunnen worden opgericht binnen de diensten die bevoegd zijn voor het toezicht op en de verwijdering van illegale inhoud op het internet, te weten het toekomstige Centrum voor Cybersecurity België, de *Federal Computer Crime Unit* of nog de Veiligheid van de Staat.

De indieners zijn voorstander van de oprichting van dergelijke cellen in alle lidstaten van de Europese Unie. De werking van de verschillende nationale cellen zou worden gecoördineerd onder leiding van Europol en uiteindelijk zou daar een Europese cel kunnen worden opgericht die met die missies is belast[11].

Ten slotte vinden de indieners dat de anonimiteit beter moet worden omkaderd en dat de capaciteit om discriminerende, haatdragende en illegale inhoud te vervolgen, moet worden opgevoerd.

Verscholen achter hun computer voelen de surfers zich veilig, want ze denken dat het onmogelijk is hen te ontmaskeren. Ze kunnen onterecht het gevoel hebben straffeloos beledigende of hatelijke woorden te mogen gebruiken of laakbare handelingen op het internet te mogen plegen.

De indieners wensen dat, in samenwerking met het Parlement en ICT-deskundigen, snel een uitgebreid onderzoek op het getouw wordt gezet om na te gaan welke regeling kan worden ontwikkeld om mensen die berichten of andere inhoud op het internet zetten, te verplichten zich te identificeren.

III. **Diensten en initiatieven ontplooien die dergelijke retoriek moeten tegengaan**

Het internet kan voor de overheid ook een middel zijn om de retoriek van terroristische en/of jihadistische organisaties te weerleggen. De strijd tegen extremistische propaganda gaat verder dan een louter verbod of de verwijdering van illegale inhoud. De verspreiding van positieve en doelgerichte berichten op zo'n schaal dat kwetsbare en risicovolle surfers er gemakkelijk toegang

[11] Voorstel van resolutie over het Europees beleid tegen radicalisme en terrorisme (DOC 54 0915/001).

tandis que seul 33 % du contenu illégal signalé par les utilisateurs *lambda* serait retiré dans le cadre de la même procédure.

À l'instar de ce qui existe au Royaume-Uni, les auteurs de la présente proposition estiment que la Belgique devrait se doter d'une unité spéciale qui serait chargée de signaler auprès des fournisseurs d'Internet les contenus illégaux qui devraient être retirés. Cette unité pourrait être créée au sein des services compétents en matière de surveillance et de retrait du contenu illégal sur Internet, à savoir le futur centre de cybersécurité, la *Federal Computer Crime Unit* ou encore la Sûreté de l'État.

Les auteurs sont favorables au développement de telles cellules auprès de l'ensemble des États membres de l'Union européenne. L'action des différentes cellules nationales serait coordonnée sous l'autorité d'Europol et à terme, une cellule européenne chargée de ces missions pourrait être créée au sein même d'Europol[11].

Enfin, les auteurs sont d'avis que l'anonymat doit être mieux encadré et que la capacité de poursuivre les propos discriminatoires, haineux et les contenus illégaux doit être renforcée.

Cachés derrière leur ordinateur, les internautes se sentent à l'abri, imaginant qu'il est impossible de les confondre. Ils peuvent développer à tort un sentiment d'impunité lorsqu'ils tiennent des propos insultants, haineux ou commettent des faits répréhensibles sur Internet.

Les auteurs souhaitent qu'une étude approfondie soit rapidement lancée, en collaboration avec le Parlement et les spécialistes des technologies de l'information et de la communication, afin d'étudier les possibilités de développer un système obligeant les personnes laissant des messages ou tout autre contenu sur Internet à s'identifier.

III. **Déployer les services et initiatives chargées des contre-discours**

Internet peut également servir d'outil aux autorités pour contrecarrer le discours des organisations terroristes et/ou djihadistes. La lutte contre la propagande extrémiste va au-delà de la simple interdiction ou suppression des contenus illégaux. La diffusion de messages positifs et soigneusement ciblés de façon suffisamment large pour que les internautes vulnérables

[11] Proposition de résolution relative à la politique européenne de lutte contre le radicalisme et le terrorisme.

toe hebben, mag niet over het hoofd worden gezien in verband met het preventiebeleid.

In welke bewoordingen en via welke distributiekanalen een en ander concreet gestalte moet krijgen, behoort zorgvuldig te worden bestudeerd. Het uitgangspunt moet een communicatiestrategie zijn die een echte analyse van het verschijnsel radicalisering inhoudt (benadering vanuit onder andere sociologisch, psychologisch, religieus en educatief oogpunt).

Begin 2015 heeft de Europese Unie België gevraagd een eenheid op te richten die, in samenwerking met het Verenigd Koninkrijk, communicatiestrategieën helpt ontwikkelen om de werving van jihadisten via het internet te voorkomen.

De indieners van dit voorstel van resolutie steunen die initiatieven, die moeten worden voortgezet en een verspreiding op grotere schaal verdienen. Zij moeten meer in het bijzonder eenvormig worden gemaakt en uitgebreid tot alle lidstaten van de Europese Unie, op basis van een Europese strategie voorzien van een tegendiscours.

et à risques puissent y accéder facilement devrait être prise en considération dans la politique de prévention.

Les discours et les canaux de diffusion doivent être soigneusement étudiés. Ils doivent se baser sur une stratégie de communication qui intègre une réelle analyse du phénomène de radicalisation (approche sociologique, psychologique, religieuse, éducative, *etc.*).

Début 2015, l'Union européenne a chargé la Belgique de mettre en place une unité d'aide à l'élaboration de stratégies de communication, en collaboration avec le Royaume-Uni, afin de prévenir le recrutement de djihadistes par Internet.

Les auteurs soutiennent ces initiatives qui doivent êtres poursuivies et déployées plus largement. Elles devraient, notamment, être étendues et uniformisées à l'ensemble des États membres de l'Union européenne sur la base d'une stratégie européenne de contre-discours.

Vanessa MATZ (cdH)
Georges DALLEMAGNE (cdH)
Benoît LUTGEN (cdH)

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. gelet op het belang van de informatie- en communicatietechnologie in onze moderne samenleving;

B. gelet op de evolutie van de terreurdreiging en de moeilijkheden die ermee gepaard gaan inzake preventie en opsporing;

C. gelet op het gebruik van de nieuwe technologieën door de terroristische en extremistische groeperingen en, als gevolg daarvan, de bredere, snellere en efficiëntere verspreiding van de jihadistische propaganda;

D. gelet op de risico's die de terreuraanslagen vormen voor de maatschappelijke cohesie, doordat ze verdeeldheid tussen de gemeenschappen zaaien en almaar extremere opinies in de samenleving doen ontstaan;

E. overwegende dat de traditionele technieken om op de radicalisering vat te krijgen, niet volstaan om de evoluerende trends op dat vlak tegen te gaan;

F. gelet op de verantwoordelijkheid van de Staat om het verschijnsel terrorisme op nationaal niveau te voorkomen en er doeltreffend op te reageren, ook op het internet;

G. overwegende dat de bestrijding van het radicalisme op internet moet worden gevoerd met inachtneming van het evenredigheidsbeginsel, zonder inperking van de individuele vrijheden en met behoud van de fundamentele rechten waarop onze samenleving is gestoeld;

H. gelet op het regeerakkoord, dat cyberveiligheid en de bestrijding van radicalisme als prioriteiten beschouwt;

I. gelet op de budgettaire besparingen van de regering in de diensten die belast zijn met veiligheid en justitie;

J. overwegende dat het noodzakelijk is het frauduleuze gebruik van de informaticasystemen, de sociale netwerken en het internet in het algemeen te voorkomen, door ervoor te zorgen dat illegaal gedrag strafbaar wordt gesteld;

K. gelet op het grensoverschrijdende en internationale karakter van het internet en de problemen die het internet doet rijzen op het vlak van bestraffing en procedures;

PROPOSITION DE RÉSOLUTION

La Chambre des représentants,

A. considérant l'importance des technologies de l'information et de la communication dans nos sociétés modernes;

B. considérant l'évolution de la menace terroriste et les difficultés qu'elle suscite en matière de prévention et de détection;

C. considérant l'utilisation des nouvelles technologies par les groupes terroristes et les extrémistes et, de ce fait, la diffusion plus large, plus rapide et plus efficace de la propagande djihadiste;

D. considérant les risques que les attaques terroristes font peser sur la cohésion sociale en semant le germe de la division entre les communautés, suscitant des opinions de plus en plus extrêmes dans la société;

E. considérant que les techniques traditionnelles de répression sont insuffisantes pour faire face à l'évolution des tendances en matière de radicalisation;

F. considérant la responsabilité incombant à l'État de prévenir et répondre efficacement, au niveau national, au phénomène du terrorisme, y compris sur Internet;

G. considérant que la lutte contre le radicalisme sur Internet doit être menée dans le respect du principe de proportionnalité, sans limiter les libertés individuelles et en préservant les droits fondamentaux qui fondent notre société;

H. considérant l'accord de gouvernement en ce qu'il définit la cybersécurité et la lutte contre le radicalisme comme une priorité;

I. considérant les économies budgétaires réalisées par le gouvernement dans les services chargés de la sécurité et de la justice;

J. considérant la nécessité de prévenir l'usage frauduleux des systèmes informatiques, des réseaux sociaux et de l'Internet en général, en assurant l'incrimination des comportements illégaux;

K. considérant le caractère transfrontalier et international d'Internet et les difficultés qu'il suscite sur les plans répressif et procédural;

L. overwegende dat samenwerking tussen Staten en samenwerking met de informatie- en communicatiebedrijven uit de privésector essentieel zijn om doeltreffend te kunnen optreden;

M. gelet op het gevoel van straffeloosheid dat de surfers kunnen krijgen;

N. overwegende dat de strijd tegen extremistische propaganda verder gaat dan een louter verbod of de verwijdering van illegale inhoud;

O. gelet op het belang van de verspreiding van positieve en doelgerichte berichten aan kwetsbare surfers die vatbaar zijn voor radicalisering;

VERZOEKT DE FEDERALE REGERING:

1. een gecentraliseerde en geïntegreerde benadering inzake veiligheid uit te werken, voorzien van een wettelijk kader dat een doeltreffend optreden mogelijk maakt dat tegen de bedreiging is opgewassen maar tegelijk aandacht heeft voor onze fundamentele rechten en vrijheden;

2. sterker in te zetten op opsporing en controle om toekomstige terroristische acties te voorkomen en de verspreiding van extremistische propaganda te verhinderen;

3. sneller werk te maken van de oprichting van het Centrum voor Cybersecurity België, zodat de samenleving beter kan worden verdedigd tegen de cyberdreiging en zodat expertise wordt opgebouwd in verband met cyberveiligheid;

4. binnen het Centrum voor Cybersecurity België in de nodige technische en personele middelen te voorzien om een efficiënte en aan de uitdagingen inzake cyberveiligheid aangepaste strategie te kunnen uitstippelen;

5. bijkomende technische en personele middelen ter beschikking te stellen van de diensten die belast zijn met risicoanalyse en -opsporing, waaronder de Veiligheid van de Staat, de Algemene Dienst Inlichting en Veiligheid (ADIV) en het Orgaan voor de Coördinatie en de Analyse van de Dreiging (OCAD);

6. de *Computer Crime Units* binnen de centrale directie (FCCU) en de regionale directies (RCCU) van de federale gerechtelijke politie te versterken wat het aantal personeelsleden en hun specialisatie betreft, en deze eenheden beter en moderner materiaal ter beschikking te stellen;

L. considérant que la collaboration entre États ainsi que la collaboration avec le secteur privé de l'information et de la communication sont essentielles pour mener une action efficace;

M. considérant le sentiment d'impunité qui peut se manifester chez des internautes;

N. considérant que la lutte contre la propagande extrémiste va au-delà de la simple interdiction ou suppression des contenus illégaux;

O. considérant l'importance de la diffusion de messages positifs et soigneusement ciblés à l'attention des internautes vulnérables et sensibles à la radicalisation;

DEMANDE AU GOUVERNEMENT FÉDÉRAL:

1. de développer une approche centralisée et intégrée en matière de sécurité, dotée d'un cadre légal qui permette une action efficace à la mesure de la menace, mais aussi soucieuse de nos droits et libertés fondamentaux;

2. de renforcer la détection et la surveillance pour prévenir de futurs actes terroristes et empêcher la diffusion de la propagande extrémiste;

3. d'accélérer la mise en place du Centre pour la cybersécurité en Belgique afin d'augmenter la capacité de défense de la société contre la cybermenace et de développer l'expertise sur la cybersécurité;

4. de prévoir, au sein du Centre pour la cybersécurité en Belgique, les moyens techniques et humains indispensables à la mise en place d'une stratégie efficace et à la hauteur des enjeux de cybersécurité;

5. de renforcer les moyens techniques et humains mis à disposition des services chargés de l'analyse et de la détection des risques, parmi lesquels la Sûreté de l'État, le Service Général du Renseignement et de la Sécurité (SGRS) et l'Organe de coordination pour l'analyse de la menace (OCAM);

6. de renforcer les *Computer Crime Units* au sein de la direction centrale (FCCU) et des directions déconcentrées (RCCU) de la police judiciaire fédérale, le nombre de ses effectifs et leur spécialisation ainsi que la qualité et la modernité du matériel mis à leur disposition;

7. de juridische en technische mogelijkheden om illegale inhoud van het internet te verwijderen, te evalueren en te verbeteren;

8. de samenwerking tussen Staten in het kader van strafbare feiten in verband met computersystemen te versterken;

9. het door de Raad van Europa op 28 januari 2003 aangenomen *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* te bekrachtigen;

10. nauwere contacten te smeden met de belangrijkste spelers van het internet, ook in Europees en internationaal verband, om de intrekking van problematische inhoud mogelijk te maken;

11. binnen de diensten bevoegd voor de controle op en de intrekking van illegale inhoud op het internet een speciale eenheid op te richten die ermee belast is de internetproviders te wijzen op illegale inhoud die op grond van hun algemene gebruiksvoorwaarden zou moeten worden verwijderd;

12. aan het bestaan van deze speciale eenheid bekendheid te geven via de oprichting van een infopunt ten behoeve van de bevolking;

13. samen met het Parlement en de specialisten op het vlak van informatie- en communicatietechnologie een grondige studie te verrichten naar de mogelijkheden om bakens uit te zetten wat de anonimiteit op het internet betreft;

14. de diensten die belast zijn met het organiseren van een tegendiscours verder uit te bouwen en de initiatieven ter zake voort te zetten;

15. een Europese communicatiestrategie te ontwikkelen om de rekrutering van jihadisten via het internet te voorkomen.

20 november 2015

7. d'évaluer et d'améliorer les possibilités juridiques et techniques permettant de retirer les contenus illégaux sur Internet;

8. de renforcer la collaboration entre États dans le cadre des infractions pénales liées aux systèmes informatiques;

9. de ratifier le Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste ou xénophobe commis par le biais de systèmes informatiques du 28 janvier 2003;

10. de développer les contacts avec les acteurs clés de l'Internet, y compris au niveau européen et international, pour assurer le retrait du contenu problématique;

11. de créer une unité spéciale, au sein des services compétents en matière de surveillance et de retrait du contenu illégal sur Internet, chargée de signaler auprès des fournisseurs d'accès à Internet les contenus illégaux qui devraient être retirés sur la base de leurs conditions générales d'utilisation;

12. de promouvoir l'existence de cette unité spéciale par la création d'un point de contact à destination de la population;

13. de mener une étude approfondie, en collaboration avec le Parlement et les spécialistes de technologies de l'information et de la communication, afin d'évaluer les possibilités d'encadrer l'anonymat sur Internet;

14. de poursuivre et de déployer les services et initiatives chargées des contre-discours;

15. de développer une stratégie européenne de communication afin de prévenir le recrutement de djihadistes sur Internet.

20 novembre 2015

Vanessa MATZ (cdH)
Georges DALLEMAGNE (cdH)
Benoît LUTGEN (cdH)

Centrale drukkerij – Imprimerie centrale