

opdracht om verder onderzoek te verrichten en een fenomeenanalyse uit te voeren? Dat is uiteindelijk toch ook een van de prioriteiten uit uw Nationaal Veiligheidsplan.

**02.03 Daniel Senesael (PS):** Monsieur le président, madame la ministre, vous n'êtes pas sans savoir que le ChWapi, le Centre hospitalier de Wallonie picarde de Tournai, a subi, le dimanche 17 janvier 2021, une cyberattaque de grande ampleur ayant entraîné l'impossibilité d'accès à 80 des 300 serveurs permettant le bon fonctionnement des services du centre hospitalier et dont la résolution a nécessité de nombreux jours.

La crise sanitaire que nous connaissons actuellement rend les centres hospitaliers et les laboratoires particulièrement vulnérables à ce genre d'attaques, d'une part, en raison de la pression subie par ces établissements et du recours au télétravail, et d'autre part, en raison de l'intérêt grandissant des pirates informatiques pour la collection et la vente d'informations relatives aux recherches sur le covid-19 et sur ses vaccins.

Madame la ministre, dès le lundi 18 janvier 2021, des membres de la Computer Crime Unit de la police fédérale (FCCU) se sont rendus à Tournai en vue d'apporter leur soutien aux services informatiques du ChWapi. Pouvons-nous recevoir des informations au sujet des procédures liées au suivi de ce type d'attaques par la FCCU?

Il nous est parvenu que des cyberattaques plus ou moins conséquentes sont fréquemment observées – et la plupart du temps maîtrisées – par les services informatiques des centres hospitaliers belges. La FCCU a-t-elle dû intervenir dans d'autres hôpitaux ou laboratoires depuis le début de la crise sanitaire?

Pouvons-nous obtenir des informations au sujet de l'attention portée par la FCCU à l'égard de ce type de phénomène – lequel, étant survenu à Tournai, est susceptible de se reproduire ailleurs dans notre pays?

**02.04 Julie Chanson (Ecolo-Groen):** Madame la ministre, en complément aux questions de mes collègues, je reviens simplement sur votre note de politique générale, dans laquelle vous aviez fait allusion à l'investissement dans des profils spécialisés et dans l'augmentation du quorum annuel d'inspecteurs en chef spécialisés pour lutter contre cette cybercriminalité à laquelle nous venons de faire allusion. J'en viens directement à ma question.

À ce jour, combien d'inspecteurs en chef spécialisés prévoyez-vous d'engager? Vers quels chiffres pouvons-nous tendre ou espérer tendre en 2021 quant à ce recrutement? Quand ces effectifs supplémentaires pourront-ils être engagés? En savez-vous davantage aujourd'hui sur la manière dont ce recrutement pourra se dérouler?

**02.05 Minister Annelies Verlinden:** Mijnheer Freilich, Telegram is geen onbekend gegeven voor onze politiediensten. Verschillende van dergelijke geëncrypteerde communicatiekanalen zijn immers erg aantrekkelijk voor criminelen. Telegramgebruikers kunnen versleutelde en zichzelf vernietigende berichten uitwisselen. Bovendien gebruikt Telegram een zelfontwikkeld cryptografisch protocol met een dubbele authenticatie, in combinatie met een wachtwoord. Daardoor is toegang tot de gegevens bijzonder moeilijk.

Binnen de federale politie beschikt de centrale directie van de bestrijding van de zware en georganiseerde criminaliteit (DJSOC) over een cel Internetrecherche, die online allerlei illegale inhoud opspoort, onder meer met betrekking tot propaganda voor terrorisme, radicalisme en gewelddadig extremisme. Zo nodig neemt die cel contact op met de verschillende internetplatformen, met het verzoek de illegale inhoud zelf te verwijderen.

De cel speurt ook naar onderzoekselementen op het internet ten voordele van de gehele geïntegreerde politie en haar partners. Dat gebeurt in het kader van alle gerechtelijke dossiers. Op dit moment bestaat de cel uit 20 personen en is ze in het kader van haar opzoekwerk naar illegale inhoud ook aanwezig op Telegram.

Telegramaccounts zijn gelinkt aan telefoonnummers die geverifieerd worden met een sms. Hoewel de toegang voor het grote publiek gemakkelijk is, moeten de politiediensten zich aan de wetgeving houden, onder meer aan de wet op de bijzondere opsporingsmethoden (BOM). Uw vraag over de verwijdering van Telegram uit de Apple App Store en Google Play valt echter niet binnen mijn bevoegdheid.

Mijnheer Moyaers, internetcriminaliteit en veiligheid zijn niet alleen mijn bevoegdheid, maar ook van de minister van Justitie en van de premier, onder wiens bevoegdheid het Centrum voor Cybersecurity België (CCB) valt. Om

fenomenen zoals identiteitsfraude, phishing, oplichting, grooming en afpersing aan te pakken, moet worden ingezet op een ketengerichte aanpak, gaande van preventie tot opvolging, vervolging en nazorg. Een sterke politie-aanwezigheid op het internet maakt daar ook deel van uit. In mijn beleidsverklaring gaf ik al aan dat ik de operationele diensten rond cybercriminaliteit wil versterken met de juiste profielen, expertise en technologie.

Collègue Chanson, chaque année, la police judiciaire fédérale recrute et engage des inspecteurs principaux spécialisés. En 2021, elle engagera 90 collaborateurs pour l'ensemble des spécialités. L'appel aux candidats externes sera lancé dans le courant du mois de mars. Parallèlement à ces engagements de collaborateurs opérationnels, la PJF investit également dans des profils de cadre administratif et logistique spécialisé (ingénieurs, programmeurs, etc.). Il s'agit des collaborateurs avec des profils hautement spécialisés qui seront recrutés dans le courant de 2021.

Monsieur Senesael, le soutien apporté dans le cadre de la cyberattaque contre l'Hôpital ChWapi à Tournai fait partie de la Quick Reaction Force (QRF). Cette équipe ad hoc, composée d'employés de différentes Computer Crime Units fédérale et régionales, qui ont les compétences nécessaires pour enquêter sur la cybercriminalité dans les environnements de réseaux complexes, peut être déployée lors d'incidents de cybercriminalité grave. Il convient, toutefois, de noter que la QRF est responsable des premières opérations policières urgentes en vue de sauvegarder autant que possible les preuves nécessaires. Aider l'opérateur concerné à arrêter l'attaque, à restaurer les systèmes infectés, à corriger les vulnérabilités ou à restaurer le fonctionnement normal des systèmes n'est pas du ressort de la QRF.

D'autres partenaires de la chaîne de cybersécurité comme la Crisis Emergency Response Team (CERT) effectue de telles tâches et peut assister l'exploitant avec des mesures correctives et/ou préventives. Le suivi des cyberincidents graves fait partie du cyberplan d'urgence du Centre de cybersécurité de Belgique. En fonction de la classification d'un cyberincident, ce plan fournit un certain nombre de mécanismes pour coordonner la coopération et l'échange d'informations entre les différents partenaires de la chaîne de cybersécurité. Le soutien QRF n'est pas une procédure standard mais un mécanisme qui peut être activé pour fournir les capacités policières

spécialisées nécessaires, en cas de besoin. Cela ne signifie pas que les incidents que vous citez ne peuvent pas faire l'objet d'une enquête judiciaire menée par la police judiciaire fédérale compétente de l'arrondissement.

Dans l'état actuel des recherches, il est trop tôt pour tirer des conclusions générales ou faire des recommandations détaillées. Il va sans dire que toutes les conclusions pertinentes qui pourraient être utilisées pour accroître la cybersécurité sont partagées avec les parties prenantes. Cette diffusion des informations sera généralement effectuée par la CERT. Dans l'ensemble, nous n'avons aucune indication selon laquelle les établissements médicaux seront désormais plus susceptibles d'être la cible de cyberattaques que d'autres secteurs. Néanmoins, la prévention, c'est-à-dire l'investissement dans la cybersécurité et le maintien des systèmes informatiques à jour, est cruciale pour éviter de devenir des proies faciles pour des cybercriminels.

**02.06** **Michael Freilich** (N-VA): Mijnheer de voorzitter, mevrouw de minister, het is inderdaad juist dat het op Telegram geëncrypteerde berichten betreft, waar men heel moeilijk binnen kan. Ik heb het echter over de chatgroepen, de chatboxen. Die zijn open voor iedereen. De politie zou daar, op vraag van een procureur des Konings - zo heb ik begrepen - mogen ingaan op vragen als "ik zit nu in die straat en heb drugs, wie kan mij belevaren?" Men kan daar zeker iets gaan doen. Ik verneem dat 20 mensen dat opvolgen. Dat lijkt veel, maar dat zijn er slechts 2 per provincie. Als men weet dat voor heel de provincie Antwerpen waar wekelijks duizenden van die berichten zijn, slechts 2 mensen dat moeten opvolgen, dan stel ik mij daar vragen bij.

Ik verwacht toch wel een engagement van u, en ik heb dat niet gehoord. Ik verwacht een engagement dat u erkent dat er een probleem is. Ik begrijp ook dat u een voorbereide tekst krijgt van uw kabinet en die moet voorlezen. Ik hoop dat u zich bewust bent van de problematiek, of ik u daarvan nu bewust maak, en zegt dat u daarvan een prioriteit gaat maken. De problematiek is er, is heel erg en verplaatst zich helemaal naar het internet.

Ik heb begrepen dat de reguliere criminaliteit vandaag fors gezakt is door corona. Heel veel mensen zijn thuis, wat betekent dat het aantal woninginbraken gedaald is. Een andere voorbeeld, het aantal winkeldiefstallen is ook gedaald. Criminaliteit verplaatst zich nu echter naar het internet.

Ik hoop dat wij van u en heel de regering daar stappen kunnen verwachten. U zegt dat bij Apple of Google gaan pleiten niet uw bevoegdheid is. Dat kan zo zijn, maar u hebt wel een collega-minister die u zomaar een vraag kunt stellen. Voor mij is het veel moeilijker. Dan moet ik weer vier weken wachten tot mijn vraag aan de orde komt. Het gaat wel degelijk om criminaliteit in België. En dat is wel uw bevoegdheid. Als dat engagement er is, ben ik zeker dat u daarvoor het nodige kunt doen.

**02.07 Bert Moyaers** (sp.a): Mijnheer de voorzitter, mevrouw de minister, zoals collega Freilich zegt, de criminaliteit heeft zich wel degelijk verplaatst, zeker tijdens de coronacrisis en cybercriminaliteit is niet meer weg te denken. Het is nu eenmaal een veel gemakkelijkere manier om veel grotere bedragen te kunnen stelen. Als er straks nog tijd voor is, zullen we het debat hierover misschien nog voortzetten, maar ik voel toch steeds meer de vraag rijzen om over te gaan tot schaalvergroting. Grotere politiezones met meer specialisatie in huis, en waarbij ook federale gerechtelijke politie nauw betrokken wordt, zijn volgens mij toch een oplossing.

Het is goed dat u de operationele diensten wilt versterken met de nodige expertise, zoals u had aangekondigd in uw beleidsnota, maar er is toch haast bij. Op dat gebied zie ik echter weinig licht aan het einde van de tunnel. Er zijn momenteel zo veel gedupeerden die hun spaargeld via criminele circuits naar het buitenland zien verdwijnen, wat uiteindelijk ook onze economie in gevaar brengt. Van mijn eigen politiezone kreeg ik bijvoorbeeld enkele weken terug nog te horen dat ze noodgedwongen, in overleg met het openbaar ministerie, nog slechts in enkele beperkte gevallen onderzoek kunnen doen naar cybercriminaliteit.

De schaalvergroting zal wellicht niet voor vandaag of morgen zijn, maar ik wil toch aandringen om op korte termijn, via de federale politie, een fenomeenanalyse te laten uitvoeren, ongeacht of dat nu met een versterkte operationele dienst is, die u zonet aankondigde, dan wel met de expertise die we vandaag al in huis hebben. Er zijn immers meer dan voldoende gegevens voorhanden om via de lokale politiediensten. Het gaat uiteindelijk toch om een prioriteit uit ons Nationaal Veiligheidsplan.

**02.08 Daniel Senesael** (PS): Madame la ministre, je vous remercie pour vos éléments de réponse qui ont retenu mon attention sur deux points.

D'abord, l'enquête judiciaire est en cours et ses conclusions pourront être utilisées à bon escient pour augmenter la sécurité des serveurs utilisés pour le bon fonctionnement du centre hospitalier. J'espère évidemment que ces conclusions iront dans le sens que vous soulignez.

Ensuite, vous dites que la prévention reste cruciale pour éviter le renouvellement de tels incidents. Je peux partager votre point de vue, mais il reste néanmoins nécessaire, voire primordial, de remonter la chaîne pour découvrir et, surtout, poursuivre les auteurs de ces cyberattaques qui mettent en péril la gestion de nos centres hospitaliers et celui du CHwapi de Tournai en particulier.

**02.09 Julie Chanson** (Ecolo-Groen): Madame la ministre, je vous remercie pour vos réponses. Je me réjouis de vous entendre dire que l'appel à recrutement commencera dès le mois prochain. C'est appréciable, vu l'urgence de la situation.

*L'incident est clos.*

*Het incident is gesloten.*

**03 Débat d'actualité sur le régime de fin de carrière pour le personnel opérationnel de la police intégrée (NAPAP) et questions jointes de - Vanessa Matz à Annelies Verlinden (Intérieur et Réformes institutionnelles) sur "La non-inscription du subsidie NAPAP dans le budget des zones de police et ses implications" (55013063C)**

- **Julie Chanson à Annelies Verlinden (Intérieur et Réformes institutionnelles) sur "Les subsidies NAPAP au sein des budgets de police 2021" (55013384C)**

- **Koen Metsu à Annelies Verlinden (Intérieur et Réformes institutionnelles) sur "La situation en ce qui concerne le régime NAPAP" (55013630C)**

- **Caroline Taquin à Annelies Verlinden (Intérieur et Réformes institutionnelles) sur "Le budget 2021 et le financement de la NAPAP pour les zones de police" (55013723C)**

- **Daniel Senesael à Annelies Verlinden (Intérieur et Réformes institutionnelles) sur "Le financement de la NAPAP en 2021" (55014026C)**

**03 Actualiteitsdebat over het eindeloopbaanstelsel voor de operationele personeelsleden van de geïntegreerde politie (NAVAP) en toegevoegde vragen van**

- **Vanessa Matz aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen) over "De gevolgen van het niet inschrijven van de NAVAP-subsidies in de begroting van de politiezones" (55013063C)**