DE MINISTER VAN BINNENLANDSE ZAKEN, INSTITUTIONELE HERVORMINGEN EN DEMOCRATISCHE VERNIEUWING

LA MINISTRE DE L'INTERIEUR, DES REFORMES INSTITUTIONNELLES ET DU RENOUVEAU DEMOCRATIQUE

Département : 12
Departement :

Document : 55 2022202318307

Réponse à la question parlementaire écrite n° 1640 du 04/01/2023, de monsieur DEPOORTERE, Député, concernant la « Lutte contre la cybercriminalité – Évolution et fréquence ».

L'honorable membre trouvera ci-après la réponse aux questions posées.

La Banque de données nationale générale (BNG) est une base de données policières dans laquelle sont enregistrés les faits sur base de procès-verbaux résultant des missions de police judiciaire et administrative. Elle permet de réaliser des comptages sur différentes variables statistiques telles que le nombre de faits enregistrés, les modus operandi, les objets utilisés lors de l'infraction, les moyens de transport utilisés, les destinations de lieu, etc.

Les données ci-dessous font toujours référence aux délits enregistrés par les services de police pour les années complètes de 2017 à 2021, ainsi que pour le premier semestre de 2022, au niveau national, tels qu'ils sont enregistrés dans la BNG sur la base des procès-verbaux.
Ces données proviennent de la banque de données clôturée à la date du 18 novembre 2022.

1-2.
S'agissant du terme « cybercriminalité », celui-ci peut tout d'abord concerner la criminalité informatique pure, laquelle recouvre les attaques contre la sécurité d'un système ou l'intégrité des données stockées dans un système informatique.

Antwoord op de schriftelijke parlementaire vraag nr. 1640 van mijnheer DEPOORTERE, Volksvertegenwoordiger van 04/01/2023, betreffende de "Bestrijding van cybercriminaliteit - Evolutie en voorkomen".

Het geachte lid vindt hieronder het antwoord op de gestelde vragen.

De Algemene Nationale Gegevensbank (ANG) is een politiedatabank waarin feiten geregistreerd worden op basis van processen-verbaal die voortvloeien uit de missies van de gerechtelijke en bestuurlijke politie. Zij laat toe om tellingen uit te voeren op verschillende statistische variabelen, zoals het aantal geregistreerde feiten, de modus operandi, de voorwerpen gehanteerd bij het misdrijf, de gebruikte vervoermiddelen, de bestemmingen-plaats, enz.

De onderstaande gegevens betreffen steeds de door de politiediensten geregistreerde misdrijven voor de volledige jaren 2017 tot en met 2021, alsook voor het eerste semester van 2022, op het nationale niveau, zoals geregistreerd in de ANG op basis van de processen-verbaal.
Deze gegevens zijn afkomstig uit de databankafsluiting van 18 november 2022.

1-2.
Inzake het begrip "Cybercrime" kan ten eerste de pure informaticacriminaliteit worden weerhouden. Deze term omvat de aanslagen op de veiligheid van een systeem of de integriteit van de in een informaticasysteem opgeslagen gegevens.

La loi sur la criminalité informatique comprend 4 infractions (faux en informatique, fraude informatique, hacking et sabotage), où le hacking et le sabotage, pris ensemble, sont aussi appelés « cyberattaques ».

De wet op de informaticacriminaliteit omvat 4 inbreuken (valsheid in informatica, informaticabedrog, hacking en sabotage), waarbij de derde (hacking) en de vierde (sabotage) ook wel eens gezamenlijk benoemd worden als “cyberaanvallen”.

Outre les infractions à la loi sur la criminalité informatique pures, des infractions de droit commun peuvent également être commises par le biais de moyens ICT. La plupart de ces infractions sont des délits de fraude, notamment les escroqueries commises via internet. Il peut s'agir entre autres de : fraude dans la vente ou l’achat en ligne (par exemple un bien qui n’est pas livré après un achat en ligne), fausse loterie, fraude à l’émotion (fausse charité ou fraude à l’amitié), fraude à l’identité (vol et abus), etc.

Naast pure inbreuken op de informaticawet kunnen ook gemeenrechtelijke misdrijven gepleegd worden door middel van ICT. Het merendeel van deze feiten zijn bedrogsmisdrijven, namelijk de oplichtingen die via internet worden gepleegd. Zo kan het onder meer gaan om: fraude bij online kopen en verkopen (bijvoorbeeld iets online kopen dat nooit geleverd wordt), valse loterij, emotiefraude (valse liefdadigheid of vriendschapsfraude), identiteitsfraude (diefstal en misbruik), ...

Le premier tableau en annexe reprend le nombre de faits enregistrés par les services de police en matière de « Criminalité informatique », suivant une répartition par type d'infraction, tels qu'ils sont enregistrés dans la BNG sur la base des procès-verbaux.

De eerste tabel in bijlage bevat het aantal door de politiediensten feiten inzake “Informaticacriminaliteit” met een onderverdeling naar type misdrijf, zoals geregistreerd in de ANG op basis van de processen-verbaal.

Le deuxième tableau en annexe reprend le nombre de faits enregistrés par les services de police en matière de « Fraude par internet ».

De tweede tabel in bijlage bevat het aantal door de politiediensten feiten inzake “Oplichting via internet”.

Tabel 1: aantal geregistreerde feiten inzake "Informaticacriminaliteit"
Tableau 1: nombre de faits enregistrés en matière de « Criminalité informatique »

	2017	2018	2019	2020	2021	SEM 1 - 2022
Informaticabedrog / Fraude informatique	17.645	20.217	28.594	35.337	39.716	23.858
Hacking	2.643	3.660	4.264	5.561	4.646	2.626
Valsheid in informatica / Faux en informatique	806	1.256	1.737	3.387	3.677	1.882
Sabotage	511	514	501	411	401	196
Totaal / Total	**21.605**	**25.647**	**35.096**	**44.696**	**48.440**	**28.562**

Bron: Federale Politie / Source: Police fédérale

Tabel 2: aantal geregistreerde feiten inzake "Oplichting via internet"
Tableau 2: nombre de faits enregistrés en matière de « Fraude par internet »

	2017	2018	2019	2020	2021	SEM 1 - 2022
Internetfraude / Fraude par internet	14.174	19.264	26.062	37.043	38.940	19.489

Bron: Federale Politie / Source: Police fédérale

3.
Le troisième tableau en annexe fournit un aperçu des modus operandi les plus enregistrés en matière de « Criminalité informatique » (top 10).

Le quatrième tableau en annexe fournit un aperçu des modus operandi les plus enregistrés en matière de « fraude par internet » (top 10).

Il faut noter que le champ « modus operandi » ne doit être complété que de manière facultative dans les systèmes d'enregistrement des services de police. Plusieurs modus operandi peuvent également être mentionnés pour le même fait.

3.
De derde tabel in bijlage bevat een overzicht van de meest geregistreerde modus operandi betreffende "Informaticacriminaliteit" (top 10).

De vierde tabel in bijlage bevat een overzicht van de meest geregistreerde modus operandi betreffende "Oplichting via internet" (top 10).

Ik wens er u op te wijzen dat het veld inzake de "modus operandi" facultatief in te vullen is in de vattingssystemen van de politiediensten. Bij éénzelfde feit kunnen ook meerdere modus operandi worden aangeduid.

Tabel 3: aantal geregistreerde modus operandi inzake "Informaticacriminaliteit" (top 10)
Tableau 3: nombre de modus operandi enregistrés en matière de « Criminalité informatique » (top 10)

		2017	2018	2019	2020	2021	SEM 1 - 2022
Gebruikte communicatiewijze / Moyen de communication utilisé	Internet (e-mail, chatroom, etc.)	1.536	2.688	3.822	6.932	8.438	4.712
Informatica- en telecommunicatiecriminaliteit / Criminalité en informatique et télécommunications	Phishing	495	1.419	2.725	8.598	9.536	5.074
Informatica- en telecommunicatiecriminaliteit / Criminalité en informatique et télécommunications	Online banking	792	1.553	2.507	5.014	4.961	2.815
Gebruikte communicatiewijze / Moyen de communication utilisé	Radiofonie - telefonie (sms, mms, wap, ...) / Radiophonie - téléphonie (sms, mms, wap, etc.)	395	830	1.506	5.234	5.627	2.731
Informatica- en telecommunicatiecriminaliteit / Criminalité en informatique et télécommunications	Hacking extern / Hacking externe	1.546	2.112	2.437	3.746	3.679	1.981

1 overwonnen materiële hindernis / gebouw - 1 obstacle matériel franchi / bâtiment	Code / paswoord - Code / mot de passe	771	997	1.374	931	950	460
Informatica- en telecommunicatiecriminaliteit / Criminalité en informatique et télécommunications	Shouldersurfing	1.449	1.275	1.483	611	356	165
Informatica- en telecommunicatiecriminaliteit / Criminalité en informatique et télécommunications	Hacking e-mail account / Hacking compte e-mail	575	819	851	691	601	290
Informatica- en telecommunicatiecriminaliteit / Criminalité en informatique et télécommunications	Contactloos betalen / Paiement sans contact				6	1.541	2.147
Informatica- en telecommunicatiecriminaliteit / Criminalité en informatique et télécommunications	Maakt een valse account aan / Crée un faux compte	4	139	527	944	1.170	643

Bron: Federale Politie / Source: Police fédérale

Tabel 4: aantal geregistreerde modus operandi inzake "Oplichting via internet" (top 10)
Tableau 4: nombre de modus operandi enregistrés en matière de « Fraude par internet » (top 10)

		2017	2018	2019	2020	2021	SEM 1 - 2022
Gebruikte communicatiewijze / Moyen de communication utilisé	Internet (e-mail, chatroom, ...)	5.207	7.327	9.540	13.259	14.304	6.788
Gebruikte communicatiewijze / Moyen de communication utilisé	Radiofonie - telefonie (sms, mms, wap, ...) / Radiophonie - téléphonie (sms, mms, wap, etc.)	822	1.611	2.665	5.667	6.712	3.352
Oplichting - domein / Escroqueries - domaines	Niet-levering. Volledig of gedeeltelijk betaalde goed / Non-livraison de biens payés en tout ou en partie	2.088	2.355	3.254	5.151	4.567	1.985
Oplichting - middelen / Escroqueries - moyens	Handelt vanuit het buitenland richting België / Agit depuis étranger vers Belgique	1.515	1.977	2.257	2.479	2.587	1.068
Oplichting - middelen / Escroqueries - moyens	Gebruikt valse hoedanigheid (titel/functie/werk, …) / Utilise fausse qualité (titre/fonction/emploi, etc.)	618	1.161	1.379	2.374	2.237	1.067
Misleidende handeling door valse hoedanigheid/naam Subterfuges par fausse qualité ou nom	Inzake bestaande identiteit / Concerne identité existante	732	984	1.172	1.999	2.164	979
Oplichting - middelen / Escroqueries - moyens	Ensceneert een vals evenement / Met en scène faux événement	508	605	785	1.265	1.554	912
Oplichting - middelen / Escroqueries - moyens	Oefent herhaaldelijk druk uit op het slachtoffer / Agit à plusieurs reprises sur victime	446	588	817	1.072	1.504	810
Gebruikte communicatiewijze / Moyen de communication utilisé	Schriftelijke mededeling / Communication écrite	279	519	657	1.089	1.574	855
Oplichting - middelen / Escroqueries - moyens	Handelt inv rechts-/nat. Pers. znd zijn medeweten / Agit au nom d'une pers. morale/physique à son insu	361	504	658	1.097	1.400	873

Bron: Federale Politie / Source: Police fédérale

4.

Les tableaux 5, 6 et 7 reprennent le nombre de suspects uniques enregistrés par la police liés dans la BNG aux infractions en matière de « Criminalité informatique », suivant une répartition par :

4.

De tabellen 5, 6 en 7 bevatten het aantal unieke door de politie geregistreerde verdachten, die in de ANG gekoppeld zijn aan de feiten inzake “Informaticacriminaliteit” met een opdeling naar:

- geslacht;

- genre;
- groupe d'âge;
- groupe de nationalité (belge, UE, non-UE).

Les tableaux 8, 9 et 10 reprennent le nombre de suspects uniques enregistrés par la police liés dans la BNG aux infractions en matière de « fraude par internet », suivant une répartition par:

- genre;
- groupe d'âge;
- groupe de nationalité (belge, UE, non-UE).

- leeftijdsgroep;
- nationaliteitsgroep (Belg, EU, niet-EU).

De tabellen 8,9 en 10 bevatten het aantal unieke door de politie geregistreerde verdachten, die in de ANG gekoppeld zijn aan de feiten inzake “Oplichting via internet” met een opdeling naar:

- geslacht;
- leeftijdsgroep;
- nationaliteitsgroep (Belg, EU, niet-EU).

Tabel 5: aantal geregistreerde unieke gekende verdachten inzake "Informaticacriminaliteit" - per geslacht
Tableau 5: nombre de suspects uniques identifiés enregistrés en matière de « Criminalité informatique » - par genre

	2017	2018	2019	2020	2021	SEM 1 - 2022
Mannen / Hommes	836	1.251	1.625	2.366	2.168	1.011
Vrouwen / Femmes	345	520	695	921	885	360

Bron: Federale Politie / Source: Police fédérale

Tabel 6: aantal geregistreerde unieke gekende verdachten inzake "Informaticacriminaliteit" - per leeftijdscategorie
Tableau 6: nombre de suspects uniques identifiés enregistrés en matière de « Criminalité informatique » - par groupe d'âge

	2017	2018	2019	2020	2021	SEM 1 - 2022
-18 jaar/ans	109	172	211	259	226	113
18 - 29 jaar/ans	519	890	1.278	1.784	1.604	655
30 -39 jaar/ans	290	361	414	611	609	270
40 - 49 jaar/ans	161	223	260	395	346	202
50 - 64 jaar/ans	104	121	148	224	247	117
65+	8	11	27	47	45	27

Bron: Federale Politie / Source: Police fédérale

Tabel 7: aantal geregistreerde unieke gekende verdachten inzake "Informaticacriminaliteit" - per nationaliteitsgroep
Tableau 7: nombre de suspects uniques identifiés enregistrés en matière de « Criminalité informatique » - par groupe de nationalité

2017	2018	2019	2020	2021	SEM 1 - 2022

Belg / Belge	797	1.290	1.722	2.325	2.202	973
EU (niet België) / UE (non-Belgique)	216	243	345	618	444	220
Europa (niet EU) / Europe (Non-UE)	48	63	56	56	62	27
Andere / Autre	127	179	215	313	366	164

Bron: Federale Politie / Source: Police fédérale

Tabel 8: aantal geregistreerde unieke gekende verdachten inzake "Oplichting via internet" - per geslacht
Tableau 8: nombre de suspects uniques identifiés enregistrés en matière de « Fraude par internet » - par genre

	2017	2018	2019	2020	2021	SEM 1 - 2022
Mannen / Hommes	494	903	1.047	2.243	2.336	823
Vrouwen / Femmes	249	351	505	957	1.123	383

Bron: Federale Politie / Source: Police fédérale

Tabel 9: aantal geregistreerde unieke gekende verdachten inzake "Oplichting via internet" - per leeftijdscategorie
Tableau 9: nombre de suspects uniques identifiés enregistrés en matière de « Fraude par internet » - par groupe d'âge

	2017	2018	2019	2020	2021	SEM 1 - 2022
-18 jaar/ans	27	66	85	121	97	41
18 - 29 jaar/ans	349	697	906	1.910	2.062	677
30 -39 jaar/ans	182	223	266	547	594	216
40 - 49 jaar/ans	111	151	184	348	377	133
50 - 64 jaar/ans	74	110	107	242	276	104
65+	9	27	26	66	92	43

Bron: Federale Politie / Source: Police fédérale

Tabel 10: aantal geregistreerde unieke gekende verdachten inzake "Oplichting via internet" - per nationaliteitsgroep
Tableau 10: nombre de suspects uniques identifiés enregistrés en matière de « Fraude par internet » - par groupe de nationalité

	2017	2018	2019	2020	2021	SEM 1 - 2022
Belg / Belge	559	912	1.190	2.130	2.520	857
EU (niet België) / UE (non-Belgique)	106	213	237	706	545	233
Europa (niet EU) / Europe (Non-UE)	13	15	12	46	47	15
Andere / Autre	72	133	129	348	378	109

Bron: Federale Politie / Source: Police fédérale

5.
Il n’est pas possible, sur base des variables disponibles dans la BNG, de déterminer le total des dommages sociaux causés par les cybercriminels.

5.
Op basis van de in de ANG beschikbare variabelen is het niet mogelijk om de totale maatschappelijke schade die werd berokkend door cybercriminelen te bepalen.

6.
La lutte contre la cybercriminalité *stricto sensu* est, en principe, une tâche des forces de la police dans le cadre de l'exercice de leurs missions de police judiciaire, guidées par le Ministère Public. Toutefois, lorsque la lutte contre la cybercriminalité est envisagée dans une dimension plus large, et donc que les aspects de prévention et de réparation sont également pris en compte, d'autres services et ministères entrent en jeu, qui sont également compétents dans ces domaines. Nous pensons ici, entre autres, au Centre pour la Cybersécurité (CCB), la Défense (SGRS), la Sûreté de l’Etat (VSSE), l’OCAM, la Justice, l’IBPT, le SPF Economie ou encore les Régions pour ce qui concerne leurs compétences propres.

6.
Het bestrijden van cybercriminaliteit *stricto sensu* is in beginsel een opdracht voor de politiediensten in het kader van het uitvoeren van hun taken van gerechtelijke politie, daarbij aangestuurd door het Openbaar Ministerie. Wanneer de strijd tegen cybercriminaliteit echter in een ruimere dimensie wordt bekeken, en dus ook aspecten van preventie en remediëring in beschouwing worden genomen, komen er nog andere diensten en ministeries in het vizier, die ook bevoegd zijn op deze domeinen. We denken hierbij onder meer aan het Centrum voor Cybersecurity België (CCB), Defensie (ADIV), Staatsveiligheid (VSSE), het OCAD, Justitie, het BIPT, de FOD Economie of nog de Gewesten voor zover dat dit hun eigen bevoegdheden betreft.

7.
Le CCB joue un rôle de coordination et d'accompagnement de la plate-forme de consultation stratégique à laquelle nous participons avec nos services partenaires. Pour la gestion des cybercrises, le centre de crise remplit un rôle crucial de coordination.

7.
Het CCB vervult een coördinerende, alleszins voor wat betreft het strategische overlegplatform waarbij we samen met onze partnerdiensten betrokken zijn. Voor het beheren van cybercrisissen vervult het crisiscentrum een cruciale coördinerende rol.

8.
Il existe actuellement de nombreuses initiatives contre les différentes formes de cybercriminalité. Cela nécessite une approche mixte, permettant de déployer les forces de chaque acteur. Il est important qu'un acteur joue un rôle central et de coordination. En Belgique, il s'agit du CCB pour la cybercriminalité sensu stricto, qui relève de la compétence du Premier ministre. Mes services jouent un rôle de soutien dans ce domaine. Par exemple, la Direction Générale Sécurité et Prévention (DGSP) veille à ce que

8.
Momenteel lopen er heel wat initiatieven tegen diverse vormen van cybercriminaliteit. Er is daarbij een gemengde aanpak nodig, waardoor op de sterktes van iedere actor kan ingezet worden. Het is belangrijk dat één actor daarbij de coördinerende en centrale rol op zich neemt. In België is dit het CCB voor cybercrime sensu stricto, dat onder de bevoegdheid valt van de eerste minister. Mijn diensten spelen daarbij een ondersteunende rol. Zo zorgt de Algemene Directie Veiligheid en Preventie (ADVP) ervoor dat de informatie van het CCB nog beter bekend

les informations du CCB soient encore mieux connues sur le terrain et sensibilise par ailleurs les autorités locales à prévenir et agir, en concertation avec le CCB.

raakt op het terrein en sensibiliseert zij de lokale overheden om acties te ondernemen, in onderling overleg met het CCB.

9.
Tout comme derrière la cybercriminalité elle-même se cache un écosystème de services criminels, il est clair que pour lutter contre la cybercriminalité, la coopération (internationale et des partenariats public-privé) est également une importante clé du succès - et ce tant dans des dossiers concrets que dans le développement de partenariats généraux ou le transfert de connaissances.
En Belgique, la *Cybersecurity Coalition* (CSC) joue un rôle important dans ce domaine.
Il s'agit d'un partenariat unique dans lequel des acteurs du monde universitaire, des organismes publics et du secteur privé unissent leurs forces dans la lutte contre la cybercriminalité. Actuellement, plus de 100 organisations en sont des membres actifs.
En outre, la DGSP est en contact régulier avec Febelfin. C'est ainsi qu'un partenariat public-privé est mis en pratique.

9.
Net zoals achter de cybercriminaliteit zelf een ecosysteem van criminele dienstverlening schuilgaat, is het duidelijk dat voor het bestrijden van cybercriminaliteit (internationale en privaat-publieke) samenwerking eveneens een belangrijke sleutel vormt om succes te kunnen boeken – en dit zowel in concrete dossiers als in het uitwerken van algemene samenwerkingsverbanden of kennisoverdracht.
In België vervult de *Cybersecurity Coalition* (CSC) een belangrijke rol op dit vlak. Deze coalitie is een uniek partnerschap waarbij spelers uit de academische wereld, openbare instanties en de private sector de krachten bundelen in de strijd tegen cybercriminaliteit. Momenteel zijn meer dan 100 organisaties actief lid. Daarnaast heeft de ADVP regelmatig contact met Febelfin. Op die manier wordt een publiek-private samenwerking in de praktijk gebracht.

10.
Cette question parlementaire ne relève pas de mes compétences mais de la compétence du Premier ministre dont dépend le Centre for Cyber Security Belgium (CCB).

10.
Deze parlementaire vraag valt niet onder mijn bevoegdheden maar behoort tot die van de Eerste minister, aan wie het Centre for Cyber Security Belgium (CCB) rapporteert.

En ce qui concerne la prévention dans le cadre d'une approche axée sur la chaîne, plusieurs actions et mesures préventives pour lutter contre la criminalité en ligne ont déjà été prises par mes services ces dernières années:
1) Le développement et la publication d'une boîte à outils 'inspiration prévention cyber' contenant des informations pour les autorités locales souhaitant initier des actions autour de la prévention contre les arnaques en ligne. Cela inclut également de nombreuses pratiques locales inspirantes.

Wat betreft preventie binnen de ketengerichte politionele aanpak zijn er de afgelopen jaren door mijn diensten al verschillende acties en preventieve maatregelen genomen om online criminaliteit tegen te gaan:

1) De ontwikkeling en publicatie van een toolbox 'cyberinspiratie' met informatie voor lokale overheden die acties wensen te starten rond preventie tegen online oplichting. Daarin komen ook tal van inspirerende lokale praktijken aan bod.

2) La coopération avec des organisations telles que CCB, IEFH, Child Focus et Febelfin sera développée davantage.

3) Les autorités locales seront encouragées à prendre également des mesures contre la cybercriminalité. Ainsi, les communes peuvent également utiliser les ressources qu'elles obtiennent grâce au *Plan Stratégique de Sécurité et de Prévention* pour mieux protéger leurs citoyens contre les formes en ligne de criminalité. D'ici 2021, 15 communes l'auront déjà intégré dans leur plan.

4) Les escroqueries en ligne sont incluses dans les sessions d'information et les formations en cours d'emploi destinées aux conseillers en prévention vols. Par exemple, un webinaire sur les risques liés aux appareils intelligents a été organisé.

5) En octobre 2022, la sécurité des appareils connectés était au centre de la campagne BeSafe@Home. Quelques conseils de base que chaque citoyen peut appliquer y ont été communiqués.

6) Plusieurs pages relatives à la cybercriminalité sont apparues sur le site Web de BeSafe en 2022. Les citoyens peuvent notamment y trouver des informations sur les délits en ligne, tels que la diffusion non consensuelle d'images intimes, les logiciels de harcèlement, les discours haineux et les escroqueries (www.besafe.be).

11.
En effet, la notion de cybercriminalité peut être comprise dans un sens restreint (infractions qui ont pour objet l'outil informatique – faux et fraude en informatique, hacking, sabotage), mais aussi dans un sens large (comprenant également les situations dans lesquelles le moyen informatique est utilisé de façon prépondérante pour commettre une autre infraction – p.ex. l'escroquerie par internet, le

2) De samenwerking met organisaties zoals CCB, IGVM, Child Focus en Febelfin wordt verder uitgebouwd

3) Lokale overheden worden aangemoedigd om zich ook in te zetten tegen cybercriminaliteit. Zo kunnen de gemeenten de middelen die ze verkrijgen via het *Strategische Veiligheids- en Preventieplan*, ook inzetten om hun burgers beter te beschermen tegen digitale vormen van criminaliteit. In 2021 integreerden al 15 gemeenten dit in hun plan.

4) Online oplichting wordt mee opgenomen in de infosessies en bijscholingen voor de diefstalpreventieadviseurs, zo werd bijvoorbeeld een webinar over de risico's van slimme toestellen georganiseerd.

5) In oktober 2022 stond de beveiliging van slimme toestellen centraal bij de BeSafe@Home-actie. Daarin werden enkele basistips meegedeeld die iedere burger kan toepassen.

6) Op de website van BeSafe verschenen in 2022 verschillende pagina's die verband houden met cybercriminaliteit. Zo kunnen burgers daar onder meer informatie vinden over online misdrijven, zoals de niet-consensuele verspreiding van intieme beelden, stalkerware, haatspraak en oplichting (www.besafe.be) .

11.
Het begrip cybercriminaliteit kan in de enge zin worden opgevat (strafbare feiten die het informaticasysteem als voorwerp hebben, zoals valsheid in informatica, informaticabedrog, hacking en sabotage), maar ook in de ruime zin (waaronder ook situaties vallen waarin informatica als middel wordt gebruikt voor het plegen van andere misdrijven, zoals internetfraude, phishing). Cybercriminaliteit in enge zin wordt in principe door de Federale

phishing). La cybercriminalité au sens restreint est plus généralement investiguée par la Police judiciaire fédérale, en particulier les Computer Crime Units (CCU) présents dans chaque direction déconcentrée de la police judiciaire fédérale.

Les infractions dites de cybercriminalité au sens large peuvent faire l'objet d'une enquête tant au niveau de la Police Locale que de la Police Judiciaire Fédérale, en fonction des paramètres du dossier (conforme à la répartition des compétences comme préscrit dans la COL 2/2002). Dans ces cas, les CCU apportent toutefois un appui spécialisé pour le recherche des éléments de preuve sur les supports digitaux.

Les CCU comptent actuellement environ 275 collaborateurs, dont 36 au niveau de la Federal Computer Crime Unit (DJSOC/FCCU), consacrés tant à l'enquête en cybercrime qu'à l'appui pour l'exploitation de supports informatiques, quel que soit le phénomène concerné (sans compter la recherche internet). Dans de nombreuses unités, ces collaborateurs sont amenés à exécuter plusieurs types de tâches.

Il est donc difficile de donner un chiffre précis du nombre d'enquêteurs spécifiquement orientés vers l'enquête cyber, mais on estime généralement qu'environ 18% de la capacité des RCCU/FCCU est consacrée aux dossiers d'enquêtes dans le domaine de la cybercriminalité au sens strict.

Pour la FCCU, c'est environ 50% des membres du personnel qui sont directement actifs dans la lutte contre la cybercriminalité.

Pour les autres services dépendant d'autres départements, je vous invite à poser la question aux Ministres concernés.

gerechtelijke politie aangepakt, in het bijzonder door de Computer Crime Units (CCU's) in elk van de gedeconcentreerde directies van de Federale Gerechtelijke Politie.

De zogenaamde cybercriminaliteit in de ruime zin kan door zowel de Lokale politie als de Federale Gerechtelijke Politie worden onderzocht, afhankelijk van de parameters van de zaak (verdeling van de bevoegdheden zoals bepaald in de COL 2/2002). In deze gevallen bieden de CCU's echter gespecialiseerde ondersteuning bij het zoeken naar bewijsmateriaal op digitale media.

De CCU's tellen momenteel ongeveer 275 medewerkers, waarvan 36 werkzaam in de Federal Computer Crime Unit (DJSOC/FCCU), die zich toeleggen op het onderzoeken van cybercriminaliteit en het ondersteunen van de exploitatie van informaticadragers, ongeacht het betreffende fenomeen (internetrecherche niet meegerekend). In veel eenheden worden deze personeelsleden geacht verschillende soorten taken verrichten.

Het is dan ook moeilijk een precies cijfer te geven voor het aantal rechercheurs dat zich specifiek bezighoudt met cyberonderzoeken, maar algemeen wordt geschat dat ongeveer 18% van de capaciteit van de RCCU/FCCU wordt besteed aan onderzoeksdossiers in het domein van cybercriminaliteit in de strikte zin.

Voor de FCCU gaat het om ongeveer 50% van het personeel dat direct actief is in de strijd tegen cybercriminaliteit.

Voor de andere diensten die afhankelijk zijn van andere departementen, nodig ik u uit de betrokken ministers te bevragen.

Annelies VERLINDEN