DOC 55 **3323/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

20 avril 2023

LE CYBER COMMAND DE LA DÉFENSE

Audition

Rapport

fait au nom de la commission
de la Défense nationale
par
MM. **Samuel Cogolati** et **Michael Freilich**

Sommaire Pages

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

20 april 2023

HET CYBER COMMAND VAN DEFENSIE

Hoorzitting

Verslag

namens de commissie
voor Landsverdediging
uitgebracht door
de heren **Samuel Cogolati** en **Michael Freilich**

Inhoud Blz.

09381

Composition de la commission à la date de dépôt du rapport/
Samenstelling van de commissie op de datum van indiening van het verslag
Président/Voorzitter: Peter Buysrogge

A. — Titulaires / Vaste leden:		**B. — Suppléants / Plaatsvervangers:**
N-VA	Peter Buysrogge, Theo Francken, Darya Safai	Björn Anseeuw, Mieke Claes, Michael Freilich, Frieda Gijbels
Ecolo-Groen	Julie Chanson, Wouter De Vriendt, Guillaume Defossé	Kim Buyst, Samuel Cogolati, Barbara Creemers
PS	Hugues Bayet, André Flahaut, Christophe Lacroix	Malik Ben Achour, Hervé Rigot, Sophie Thémont, Özlem Özen
VB	Steven Creyelman, Annick Ponthier	Pieter De Spiegeleer, Joris De Vriendt, Ellen Samyn
MR	Christophe Bombled, Denis Ducarme	Daniel Bacquelaine, Philippe Pivin, Caroline Taquin
cd&v	Hendrik Bogaert	Wouter Beke, Nawal Farih
PVDA-PTB	Maria Vindevoghel	Roberto D'Amico, Steven De Vuyst
Open Vld	Jasper Pillen	Tim Vandenput, Marianne Verhaert
Vooruit	Kris Verduyckt	Melissa Depraetere, Vicky Reynaert

C. — Membre sans voix délibérative / Niet-stemgerechtigd lid:

Les Engagés	Georges Dallemagne

N-VA	:	*Nieuw-Vlaamse Alliantie*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
PS	:	*Parti Socialiste*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
cd&v	:	*Christen-Democratisch en Vlaams*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Open Vld	:	*Open Vlaamse liberalen en democraten*
Vooruit	:	*Vooruit*
Les Engagés	:	*Les Engagés*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant – Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de nummering 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 vertaalde beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénière*	*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)*

MESDAMES, MESSIEURS,

Votre commission a procédé, le 1er mars 2023, à un échange de vues avec le général-major Michel Van Strythem au sujet du *Cyber Command* de la Défense.

A. **Exposé introductif du général-major Michel Van Strythem**

Le processus qui a conduit à la mise en place d'un *Cyber Command*, inauguré le 19 octobre 2022, a débuté en 2010 au sein du SGRS. Le cyberespace constitue un cinquième domaine opérationnel en plus de la terre, de la mer, de l'air et de l'espace. On peut considérer que le cyber est composé de deux "écosystèmes", un civil et un militaire.

De quoi se compose le cyberespace?

— Un niveau physique comprenant des émetteurs, des récepteurs et des canaux de transmission (satellites, câbles de fibres optiques intercontinentaux sous-marins et terrestres, ainsi que des ondes électromagnétiques). Ce niveau est donc physiquement présent dans les quatre autres domaines opérationnels. Il s'agit d'une infrastructure vulnérable.

— Un niveau logique qui règle le fonctionnement d'internet dans son intégralité (public et privé – du *surface web* au *dark web* en passant par le *deep web*).

— Un niveau cognitif qui pilote les applications (notamment les réseaux sociaux). Ces applications présentent certains risques pour la vie privée et la sécurité (notamment la désinformation par des acteurs étatiques en vue de manipuler et de déstabiliser la société et l'administration publique, un phénomène connu dans le jargon européen sous la dénomination "Manipulation de l'information et ingérence étrangères" (*FIMI* ou *Foreign Information Manipulation and Interference*).

Ce cyberespace est un ensemble extrêmement complexe de millions d'interactions entre ces trois niveaux, tant dans le domaine militaire (tactique et opérationnel) que dans le domaine civil. M. Van Strythem évoque ensuite plusieurs exemples de risques et d'attaques réelles, telles que la perturbation des équipements électroniques en vue de les mettre hors service, suivie de campagnes de désinformation et du piratage des serveurs du parti démocrate aux États-Unis en 2016, auquel a succédé une campagne de désinformation (FIMI).

Ce qui caractérise le cyberespace, c'est la rapidité du renouvellement des technologies, mais aussi des tactiques et des méthodes des personnes qui souhaitent en faire un usage abusif. Toute nouvelle technologie accroît la

DAMES EN HEREN,

Uw commissie heeft op 1 maart 2023 een gedachtewisseling gehouden met Generaal Majoor Michel Van Strythem over het *Cyber Command* van Defensie.

A. **Inleidende uiteenzetting door Generaal Majoor Michel Van Strythem**

Het proces tot oprichting van een *Cyber Command* op 19 oktober 2022 startte in 2010 in de schoot van ADIV. De Cyber ruimte vormt een vijfde operationeel terrein naast land, zee, lucht en ruimte. Cyber kan men opdelen in respectievelijk een burgerlijk en een militair "ecosysteem".

Waaruit bestaat "Cyberspace"?

— Fysieke laag met zenders, ontvangers en transmissiekanalen (satellieten, intercontinentale optische vezelkabels onderzee en over land, evenals elektromagnetische golven). Deze laag doorkruist dus de vier andere operationele domeinen op fysiek vlak. Dit is kwetsbare infrastructuur.

— Logische laag die de werking van het volledige internet regelt (publiek en privaat – van *surface web* over *deep web* tot *dark web*).

— Cognitieve laag die applicaties (o.a. sociale media) aanstuurt. Deze applicaties bieden bepaalde risico's voor privacy en veiligheid (o.a. desinformatie door statelijke actoren met het oog op manipulatie en destabilisering van de maatschappij en de overheidsadministratie, in het Europees jargon FIMI of *Foreign Information Manipulation and Interference*.

Deze Cyberspace is een uiterst complex gebeuren van miljoenen interacties tussen deze drie lagen. In het militair (tactisch en operationeel) maar evengoed in het burgerlijke domein. De heer Van Strythem geeft vervolgens een aantal voorbeelden van risico's en reële aanvallen, zoals de verstoring van elektronische apparatuur om de dienstverlening te verlammen gevolgd door desinformatiecampagnes en de hacking van de servers van de Democratische Partij in de VS in 2016 gevolgd door een desinformatiecampagne (FIMI).

Kenmerkend in cyber is de snelheid van technologische vernieuwing evenals van de tactieken en werkwijzen van zij die de technologie wensen te misbruiken. Een nieuwe technologie brengt telkens ook een nieuwe, verhoogde

vulnérabilité. Depuis que la guerre a éclaté en Ukraine, des cyberopérations et des cyberattaques accompagnent certaines opérations militaires de grande envergure, ce qui nécessite une planification détaillée préalable qui ne coïncide pas nécessairement avec la planification des opérations militaires classiques. Il est d'ailleurs utile de développer une cyberdéfense et une cybersécurité de qualité car elles compromettent considérablement les chances de réussite d'une attaque, tant pour le domaine militaire que pour le domaine civil. Outre les autorités, les entreprises privées ont également un rôle majeur à jouer en matière de cybersécurité, car les pouvoirs publics ne peuvent affronter seuls cette complexité.

Parmi les menaces, on peut citer le sabotage (*wipers*), l'espionnage, l'influence exercée par des puissances étrangères et la criminalité. Elles ne sont pas toujours faciles à distinguer (problème d'attribution: s'agit-il, par exemple, d'une attaque criminelle ou étatique?). Un autre problème est que les réseaux visés par des attaques se trouvent tant dans des zones internationales (espace, fonds marins…) que sur plusieurs territoires nationaux, et ils sont dès lors soumis à des règles de droit internationales et à plusieurs règles de droit nationales. Les auteurs des attaques utilisent en outre plusieurs réseaux pour mener leur action, ce qui complique davantage l'attribution de l'origine des attaques. Des outils illicites sont d'ailleurs proposés sur le *dark web* pour mener des cyberattaques.

Genèse du Cyber Command

L'exposé d'orientation politique de la ministre Dedonder du 4 novembre 2020 prévoyait la création d'une composante Cyber pour la fin de la législature, moyennant quatre conditions préalables importantes, à savoir le renforcement des mission du SGRS pour cette composante, des investissements dans le capital humain et dans le développement des connaissances, des investissements dans l'innovation et un suivi qualitatif du processus de développement de la nouvelle composante, au service de la Défense et de toute la société.

Mi-2021, une équipe de projet a été constituée sous la direction du général Van Strythem afin de mettre au point la création de la nouvelle composante, ce qui a débouché sur la cartographie du cyberécosystème (comparaison internationale, conclusion de partenariats, coopération interdépartementale…), un recensement de ce qui existait déjà au sein de la Défense en matière de cybersécurité (SGRS, CCB) et le lancement d'une série de projets d'innovation et de nouveaux partenariats.

Le *Cyber Command* a finalement été créé le 19 octobre 2022 en tant que partie intégrante de la structure du SGRS et se compose d'une division opérationnelle

kwetsbaarheid mee. Sinds de oorlog in Oekraïne worden ook cyberoperaties en –aanvallen uitgevoerd in grote militaire operaties, iets wat een uitvoerige voorafgaandelijke planning vergt die niet noodzakelijk gelijkloopt met de klassieke militaire operatieplanning. Overigens loont het om een degelijke cyberverdediging en -beveiliging uit te bouwen, aangezien dit een geslaagde aanval aanzienlijk bemoeilijkt – dit geldt overigens zowel voor het militaire als voor het civiele domein. Naast de overheid hebben ook privébedrijven een belangrijke rol inzake cyberveiligheid, aangezien de overheid deze complexiteit niet alleen aankan.

De bedreigingen betreffen sabotage (*wipers*), spionage, beïnvloeding en criminaliteit, waarbij het onderscheid niet altijd eenvoudig te maken valt (probleem van toewijzing of attributie, bijvoorbeeld gaat het om een criminele of om een statelijke aanval?). Een ander probleem is dat de netwerken die worden aangevallen zich bevinden in zowel internationale zones (ruimte, onderzee…) als op meerdere nationale territoria, en derhalve onderworpen zijn aan internationale en meerdere nationale rechtsregels. De aanvallers gebruiken bovendien meerdere netwerken om hun actie uit te voeren, wat de toewijzing verder bemoeilijkt. Op het *dark web* worden overigens criminele instrumenten aangeboden om cyberaanvallen uit te voeren.

Voorgeschiedenis van de Cyber Command

De Beleidsverklaring van minister Dedonder van 4 november 2020 voorzag de oprichting van een component Cyber tegen het einde van de legislatuur met 4 belangrijke randvoorwaarden: de versterking van de opdrachten van ADIV door deze component, investering in het menselijk kapitaal en kennisontwikkeling, investeren in innovatie en een degelijke opvolging van het groeiproces van de nieuwe component ten dienste van Defensie en de hele maatschappij.

Midden 2021 werd een projectteam samengesteld o.l.v. generaal Van Strythem om de oprichting van de nieuwe component uit te werken. Dit resulteerde in het in kaart brengen van het cyber ecosysteem (internationale benchmark, afsluiten van partnerschappen, interdepartementele samenwerking…), een overzicht van wat reeds bestond in de schoot van Defensie inzake cyberveiligheid (ADIV, CCB) en de start van een aantal innovatieprojecten en nieuwe partnerschappen.

Uiteindelijk werd de *Cyber Command* opgericht op 19 oktober 2022, ingebed in de structuur van ADIV met een operationele en een zogenaamde *development*

et d'une division *development and readiness*. La nouvelle composante fournit en outre également un appui à l'ensemble des autres composantes et activités de la Défense (air, terre, marine, composante médicale, approvisionnement militaire et communication par satellite).

Missions du Cyber Command

• exécuter des opérations dans le cyberespace (renseignement, sécurité, opérations défensives);

• appuyer les autres composantes et activités (défensives et offensives);

• renforcer la résilience nationale (notamment en ce qui concerne l'activation du plan d'urgence cybernétique du CCB et du Centre de crise national).

Place du Cyber Command dans le cyberécosystème public

Le *Cyber Command* coopère au niveau national avec une série de partenaires dans le cadre de la stratégie nationale de sécurité. Chaque partenaire exerce dans ce cadre une série de missions essentielles en appui de l'ensemble. La Défense (le SGRS et le *Cyber Command*) participe au plan d'urgence cybernétique, notamment par l'intermédiaire de la CERT (*Cyber Emergency Response Team*). En cas de crise nationale, l'ensemble des acteurs sont réunis en une plateforme opérationnelle unique, au sein de laquelle le Cyber Command dirigera l'enquête de renseignement (y compris l'attribution et l'expertise juridique). Il va de soi que tout ce processus se déroule conformément aux dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Malgré sa complexité, cette structure constitue un instrument performant.

Domaines d'activité

• action préventive (homologation des réseaux, directives relatives aux bonnes pratiques, sensibilisation aux risques…);

• surveillance active des réseaux;

• collecte du renseignement;

• déploiement militaire (défensif et offensif, c*yber force protection*); protection des systèmes d'armement interconnectés au travers des différentes composantes.

and readiness afdeling. De nieuwe component levert daarbij ook ondersteuning aan alle andere componenten en activiteiten van Defensie (lucht, land, marine, medisch, militaire bevoorrading en satellietcommunicatie).

Missies van de Cyber Command

• Operaties uitvoeren in de cyberruimte (inlichtingen, veiligheid, defensieve operaties);

• steun aan de andere componenten en activiteiten (defensief en offensief);

• versterking van de nationale weerbaarheid (o.a. inz. activering van het cyber crisisplan van CCB en van het Nationaal Crisiscentrum).

Plaats van het Cyber Command in het openbaar cyber ecosysteem

Het *Cyber Command* werkt op nationaal vlak samen met een aantal partners in het kader van de nationale veiligheidsstrategie. Elke partner heeft in dit verband een aantal kernopdrachten ter ondersteuning van het geheel. Defensie (ADIV en *Cyber Command*) nemen deel aan het Cyber Emergency Plan, o.m. via het *Cyber Emergency response Team*. In geval van een nationale crisis worden alle actoren samengeroepen in één operationeel platform waarbij *Cyber Command* het inlichtingenonderzoek zal leiden (inbegrepen de attributie en juridische expertise). Vanzelfsprekend gebeurt alles overeenkomstig de bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. Ondanks de complexiteit biedt deze structuur een goed functionerend apparaat.

Activiteitsdomeinen

• preventieve werking (homologatie van netwerken, richtlijnen van goede praktijken, bewustmaking van risico's…);

• actieve monitoring van netwerken;

• inlichtingenvergaring;

• militaire inzet (defensief en offensief, *cyber force protection*); bescherming van de nieuwe geïnterconnecteerde wapensystemen doorheen de verschillende componenten.

Défis

• Financement (par des moyens provenant du plan STAR et du plan de relance national et européen);

• Mise en œuvre de l'ensemble des programmes et des contrats avec les partenaires;

• Défis en matière de personnel, capital humain: diversification des canaux de recrutement, développement des connaissances et rétention (5 à 7 ans suivis d'un système d'alumni dans la cyber-réserve). La Défense collabore également étroitement avec l'ERM (École royale militaire) et d'autres écoles supérieures ("*outreach*"), ainsi qu'avec l'industrie et des centres de recherche et développement.

B. **Questions et observations des membres**

M. Michael Freilich (N-VA) souligne l'importance des investissements dans la cyberdéfense compte tenu de l'effet déstabilisant des cyberattaques sur la société et l'économie. Le général Van Strythem pourrait-il indiquer quel sera l'effectif de la composante *Cyber* à l'horizon 2030 et si cet objectif est réaliste? Comment les valeurs de référence ont-elles été établies et quel est le niveau d'ambition? Le recrutement sera-t-il effectué par le biais du Selor ou sera-t-il assuré par la Défense elle-même (cf. enquête de sécurité)? Est-il indiqué de travailler également de manière complémentaire dans ce domaine tant dans un cadre européen que dans le cadre de l'OTAN? Qu'est-ce que la Défense compte faire elle-même et que compte-t-elle sous-traiter? Les moyens budgétisés seront-ils suffisants jusqu'en 2030 et comment seront-ils ventilés entre le matériel et les frais de personnel? La Défense devra-t-elle également investir dans des ordinateurs puissants? En ce qui concerne le recrutement, la Défense entend collaborer avec des programmes sociaux (notamment MolenGeek). Comment cette intention se concilie-t-elle avec les exigences élevées imposées aux candidats? Cette coopération se situe-t-elle dans le domaine civil ou dans le domaine militaire? Des civils occuperont-ils également des fonctions dirigeantes (de commandement)? Un trajet a-t-il déjà été défini en vue de la coopération avec l'industrie ou de la sous-traitance à l'industrie? La Défense compte-t-elle avoir recours en permanence à des externes ou ce recours n'est-il que temporaire? Jusqu'à quel point la population est-elle influencée (infox, etc.)? Existe-t-il déjà au sein de la Défense des directives limitant l'utilisation des vecteurs à haut risque comme TikTok, quelle

Uitdagingen

• Financiering (via middelen uit het STAR-plan en het nationaal en Europees relanceplan);

• Implementatie van alle programma's en contracten met partners;

• Personeelsuitdagingen, menselijk kapitaal: diversificatie van rekruteringskanalen, kennisontwikkeling en retentie (5 à 7 jaar gevolgd door alumnisysteem in de cyber-reserve). Er is ook nauwe samenwerking met de KMS (Koninklijke Militaire School) en andere hogescholen ("*outreach*"), industrie en onderzoek- en ontwikkelingscentra.

B. **Vragen en opmerkingen van de leden**

De heer Michael Freilich (N-VA) wijst op het belang van de investeringen in cyberdefensie gelet op het destabiliserend effect van cyberaanvallen op maatschappij en economie. Kan generaal Van Strythem toelichten wat het personeelsbestand van de Cybercomponent zal zijn anno 2030 en is dat realistisch? Hoe werd de benchmark opgesteld, wat is het ambitieniveau? Zal de rekrutering via Selor verlopen of gaat Defensie dat zelf doen (cf. veiligheidsscreening)? Is het aangewezen ook in dit domein zowel in Europees als in NAVO-verband aanvullend te werken, wat gaat Defensie zelf doen en wat gaat ze uitbesteden? Volstaan de gebudgetteerde middelen tot horizon 2030 en hoeveel gaat naar materieel, resp. personeelskosten? Moet Defensie ook in zware computers investeren? Inzake rekrutering wil Defensie samenwerken met sociale programma's (o.a. MolenGeek), in welke mate strookt deze intentie met de hoge eisen die aan de kandidaten worden gesteld? Situeert deze samenwerking zich in het burgerlijke of militaire domein? Zullen ook burgers leidinggevende (commando)functies vervullen? Is er al een traject uitgewerkt voor samenwerking met en uitbesteding aan de industrie? Gaat Defensie blijvend beroep doen op externe krachten of is dit slechts tijdelijk? Hoe ver gaat de beïnvloeding van de bevolking (*fake news* etc.). Zijn er binnen Defensie al beperkende richtlijnen voor het gebruik van hoog risicovectoren zoals TikTok, hoe vaak komen incidenten voor? Moet hiervan geen specifieke lijst worden opgesteld? Wat betreft het attributieproces: de cyberaanval vorig jaar op Defensie werd toegewezen aan China, volgens generaal Van Strythem op basis van bewijsmateriaal; wat is het diplomatiek traject, hoe

est la fréquence des incidents? Ne conviendrait-il pas d'établir une liste spécifique de ces vecteurs? En ce qui concerne le processus d'attribution: selon le général Van Strythem, la cyberattaque menée l'année dernière contre la Défense a été attribuée à la Chine sur la base d'éléments de preuve; quel est le trajet diplomatique suivi, en quoi consiste exactement cette administration de la preuve et de quelle manière la Défense peut-elle récupérer les dommages et les frais encourus?

M. Samuel Cogolati (Ecolo-Groen) estime, lui aussi, que la création du *Cyber Command* constitue une avancée importante. L'intervenant précise qu'il a lui-même été victime d'actes de cyberpiratage organisés par l'*advanced persistent threat 31* (APT31) chinoise. Il rappelle par ailleurs qu'en 2021, alors qu'il était prévu d'entendre des Ouïghours en commission des Relations extérieures, cette audition a dû être annulée, également à la suite d'une cyberattaque orchestrée par la Chine. M. Van Strythem pourrait-il fournir davantage de détails à propos de ces menaces en provenance de Chine, en particulier concernant l'APT 31? Cette organisation a-t-elle également visé des cibles belges autres que le SPF Intérieur et la Défense? Quelle est l'ampleur de la cybermenace chinoise qui pèse sur les institutions belges? Y a-t-il d'autres victimes? Les autorités belges sont-elles également menacées par d'autres acteurs étatiques que la Chine? Par ailleurs, qui peut bénéficier de la protection du *Cyber Command*? S'agit-il uniquement des institutions publiques fédérales ou également de personnes et d'organisations vulnérables? Ou celles-ci doivent-elles faire appel au CCB? Quelles sont les lignes directrices données en Belgique aux membres du gouvernement et aux institutions publiques en ce qui concerne TikTok?

M. Christophe Lacroix (PS) souligne l'importance et l'ampleur de la mission confiée au général Van Strythem. Les objectifs de recrutement du *Cyber Command*, notamment en ce qui concerne la répartition entre militaires et civils, ont-ils déjà été fixés et quels sont les obstacles éventuels à leur concrétisation? Quels sont les effectifs actuels du *Cyber Command*? Comment le général Van Strythem envisage-t-il la coopération structurelle avec d'autres acteurs de la Défense, mais aussi avec d'autres acteurs publics en matière de cybersécurité (police fédérale et judiciaire – Computer Crime Unit – CCB…)? Quel est le rôle du *Cyber Command* à l'égard des villes et des communes, qui sont souvent victimes de cyberattaques? Quelle est la mission du *Cyber Command* en ce qui concerne la protection des institutions démocratiques (Parlement, gouvernement, etc.)? Quelle est la base légale de l'action défensive et offensive du *Cyber Command* et qui doit prendre la direction en dernier ressort en cas de cyberattaque massive dirigée contre notre pays (*Cyber Command*,

verloopt deze bewijsvoering precies en wat hoe kan Defensie de opgelopen schade en kosten recupereren?

De heer Samuel Cogolati (Ecolo-Groen) bevestigt eveneens het belang van de oprichting van de *Cyber Command*. De heer Cogolati is trouwens zelf het slachtoffer van cyberpiraterij door de Chinese *advanced persistent threat 31* (APT31). In 2021 moest bovendien een hoorzitting met Oeigoeren in de commissie voor Buitenlandse betrekkingen worden geannuleerd, eveneens na een cyberaanval vanuit China. Kan de heer Van Strythem meer toelichting geven bij deze dreigingen vanuit China en meer bepaald APT 31: heeft deze organisatie ook andere Belgische doelwitten dan de FOD BiZa en Defensie geviseerd? Hoe ver gaat die Chinese cyberdreiging op de Belgische instellingen, zijn er nog andere slachtoffers? Zijn er naast China nog andere statelijke actoren die de Belgische overheden bedreigen? Wie kan voorts genieten van de bescherming vanwege het *Cyber Command*, zijn dat enkel de federale overheidsinstellingen of eveneens kwetsbare personen en organisaties – of moeten deze beroep doen op het CCB? Wat zijn de richtlijnen in België voor regeringsleden en overheidsinstellingen inzake TikTok?

De heer Christophe Lacroix (PS) wijst op het belang en de omvang van de opdracht toevertrouwd aan generaal Van Strythem. Zijn de rekruteringsdoelstellingen van het *Cyber Command*, inz. de opdeling tussen militairen en burgers, reeds vastgelegd en wat zijn de eventuele obstakels om ze te behalen? Wat is het huidige effectief van het *Cyber Command*? Hoe ziet generaal Van Strythem de structurele samenwerking met andere actoren binnen Defensie maar ook met andere overheidsactoren inzake cyberveiligheid (federale en gerechtelijke politie – Computer Crime Unit – CCB…)? Welke rol heeft het *Cyber Command* tegenover steden en gemeenten, die vaak slachtoffer zijn van cyberaanvallen? Wat is de opdracht van het militaire *Cyber Command* inzake de beveiliging van de democratische instellingen (Parlement, regering…). Wat is de wettelijke basis voor het defensief en offensief optreden van het *Cyber Command*, wie neemt uiteindelijk de leiding in geval van een massale cyberaanval op ons land (het *Cyber Command*, het Crisiscentrum, ADIV…)? Is er controle op *Cyber Command*

Centre de crise, SGRS, etc.)? Le Comité R exerce-t-il un contrôle sur le *Cyber Command*? Comment le général Van Strythem envisage-t-il la collaboration avec d'autres États membres européens? La Belgique compte-t-elle également créer une cyberréserve constituée de civils, comme la France? Quels sont les risques liés aux réseaux sociaux en général (outre TikTok, Facebook et Twitter)? Comment le *Cyber Command* collabore-t-il avec les régions pour protéger nos intérêts industriels (industrie, ports, aéroports)? Quel est le cyberrisque en ce qui concerne les systèmes d'armes létaux autonomes, par exemple? Y a-t-il des risques pour les systèmes de pilotage des F35 d'origine étrangère et quel sera le rôle du *Cyber Command* à cet égard?

M. Denis Ducarme (MR) déplore le manque de clarté de l'exposé du général Van Strythem. En ce qui concerne TikTok, M. Van Strythem a-t-il rédigé un rapport sur les risques liés à l'utilisation de cette application à l'intention de la ministre de la Défense, qui en fait un usage intensif? La mésaventure de M. Cogolati devrait inciter à donner des instructions concrètes aux parlementaires en matière de sécurité des données. De quel budget le *Cyber Command* dispose-t-il aujourd'hui et quels sont les budgets nécessaires pour atteindre les objectifs fixés? Le budget actuel est-il suffisant, tant pour ce qui est des équipements que pour ce qui est des ressources humaines (recrutement)? Le statut du personnel est-il suffisamment attractif? Des accords concrets ont-ils été conclus en matière de recrutement avec l'ERM, le monde industriel et le monde académique? A-t-on pu déterminer les origines des différentes cyberattaques lancées contre notre pays? Le *Cyber Command* fonctionne-t-il en concertation avec l'Agence de l'Union européenne pour la cybersécurité Enisa? A-t-on élaboré une feuille de route sur la cyberdéfense, comme l'a demandé la Commission européenne?

M. Steven De Vuyst (PVDA-PTB) souligne la multipolarité croissante de l'ordre mondial et la rivalité toujours plus intense entre les différentes puissances. Cette situation présente certains risques de piratage et de désinformation. L'intervenant estime qu'il ne faut pas se montrer naïf à cet égard et qu'on ne peut pas exclure le piratage et la manipulation par des pays amis. Il songe notamment aux activités de la *National Security Agency* américaine et à l'enquête menée par un consortium international de journalistes sur le collectif de pirates informatiques israéliens Team Jorge, qui manipulerait des élections dans le monde entier. Le général Van Strythem dispose-t-il de plus amples informations à ce sujet, notamment à propos de l'origine des attaques et de la question de savoir si notre pays a également été touché? Quelle est

vanwege Comité I? Hoe ziet generaal Van Strythem de samenwerking met andere Europese lidstaten, zijn er in België ook plannen voor de oprichting van een cyberburgerreserve, zoals in Frankrijk? Welke risico's houden de sociale media-applicaties in het algemeen in (naast TikTok ook Facebook en Twitter)? Hoe werkt het *Cyber Command* samen met de regio's ter bescherming van onze industriële belangen (industrie, havens, luchthavens)? Welk cyber-risico is er ten aanzien van bijvoorbeeld dodelijke autonome wapensystemen? Zijn er risico's voor de besturingssystemen van de F35 die van buitenlandse oorsprong zijn en welke rol heeft het *Cyber Command* daarin te vervullen?

De heer Denis Ducarme (MR) betreurt de vaagheid van de uiteenzetting van generaal van Strythem. Heeft de heer van Strythem inzake TikTok een rapport opgemaakt over de gebruiksrisico's ten behoeve van de minister van Landsverdediging die een fervent gebruikster is van deze applicatie? Het wedervaren van de heer Cogolati moet een aansporing zijn om aan de parlementsleden concrete instructies te bezorgen over databeveiliging. Welk budget heeft het *Cyber Command* vandaag en wat zijn de budgettaire noden om de gestelde objectieven te behalen? Volstaat dit budget, zowel op materieel vlak als op vlak van personeel (rekrutering). Is het personeelsstatuut voldoende aantrekkelijk? Zijn er concrete afspraken voor rekrutering met de KMS, met de industrie, met de academische wereld? Zijn alle cyberaanvallen op ons land toegewezen? Werkt het *Cyber Command* samen met Enisa – het Agentschap van de Europese Unie voor cyberbeveiliging, werd er een routeplan uitgeschreven inzake cyberdefensie zoals gevraagd door de Europese Commissie?

De heer Steven De Vuyst (PVDA-PTB) wijst op de toenemende multipolaire wereldorde en rivaliteit tussen verschillende machtsblokken, die bepaalde risico's van hacking en desinformatie meebrengen. De heer de Vuyst meent dat men daarbij niet naïef mag zijn en hacking en manipulatie door bevriende landen niet mag uitsluiten, hij verwijst naar activiteiten van het Amerikaanse *National Security Agency* en naar het onderzoek van een internationaal journalistenconsortium naar Team Jorge, een Israëlisch hackerscollectief dat wereldwijd verkiezingen zou manipuleren. Heeft generaal Van Strythem daarover meer informatie, onder meer betreffende de oorsprong van de aanvallen en of dit ook in België is gebeurd? Hoe weerbaar is België tegen dergelijke aanvallen en zijn we niet te goedgelovig tegenover onze eigen bondgenoten?

la capacité de la Belgique à résister à de telles attaques et ne sommes-nous pas trop crédules à l'égard de nos propres alliés? Par ailleurs, comment le Cyber Command peut-il assurer la cybersécurité des pouvoirs locaux?

M. Jasper Pillen (Open Vld) se joint aux questions déjà posées à propos du budget, du recrutement et des défis y afférents. Recruter les profils souhaités peut nécessiter de s'écarter des procédures traditionnelles du SELOR. Comment le *Cyber Command* gérera-t-il les tensions éventuelles entre le personnel civil et le personnel militaire? L'intervenant songe en l'espèce à ce qu'on a pu constater à cet égard au sein du SGRS. Quelles sont les procédures appliquées pour déterminer l'origine des cyberattaques et est-il utile ou nécessaire de publier celles-ci? Pourquoi n'a-t-on interdit, à titre général, l'utilisation de certaines applications comme TikTok sur les appareils appartenant aux pouvoirs publics?

M. Kris Verduyckt (Vooruit) demande si la Défense dispose actuellement d'une capacité suffisante pour faire de la prévention auprès de ses troupes – et éventuellement aussi auprès d'autres services publics – concernant l'utilisation des appareils mobiles? Cette prévention a-t-elle des effets positifs? S'attaque-t-on également au niveau européen aux risques d'interception des systèmes d'armement modernes, comme les drones et les avions? Le *Cyber Command* prendra-t-il aussi des mesures offensives anticipées pour prévenir les actions hostiles? L'actuelle enquête de sécurité dont font l'objet les recrues est-elle suffisante (cf. affaire Conings)? La sécurisation des administrations locales, des villes et des communes requiert sans doute une architecture spécifique: quel est l'avis du général Van Strythem à ce sujet?

M. Georges Dallemagne (cdH) souligne que l'on a trop longtemps négligé la cybersécurité et qu'il est extrêmement urgent de prendre des mesures en la matière. C'est ce qui ressort également de l'audition organisée aujourd'hui. À cet égard, M. Dallemagne demande au général Van Strythem de fournir à la commission un tableau de bord relatif aux moyens (humains, technologiques, financiers) dont dispose déjà le *Cyber Command* et de ceux qui lui seront nécessaires à court terme, ainsi qu'une évaluation du fondement légal des activités de la nouvelle composante en vue d'apporter d'éventuelles modifications à la législation en vigueur. Le général Van Strythem peut-il indiquer à quelles menaces il souhaite répondre en priorité? M. Dallemagne ne comprend d'ailleurs pas pourquoi la ministre de la Défense utilise toujours l'application TikTok, vu les risques qui y sont manifestement liés; M. Van Strythem lui a-t-il donné des directives à ce sujet ou bien des mesures de sécurité particulières ont-elles été prises? N'est-il pas également urgent de formuler des recommandations à

Hoe kan het *Cyber Command* de cyberveiligheid van de lokale besturen verzekeren?

De heer Jasper Pillen (Open Vld) sluit zich aan bij reeds gestelde vragen inzake budget en rekrutering en de overeenkomstige uitdagingen. De gewenste profielen aanwerven vergt wellicht een afwijking van de geijkte SELOR-procedures. Hoe zal het *Cyber Command* omgaan met de mogelijke spanningen tussen burger- en militair personeel, cf. de ervaringen binnen ADIV? Welke procedures hanteert men voor attributie van cyberaanvallen en is het wel nuttig of noodzakelijk om dit te publiceren? Waarom is er voorts geen algemeen verbod op het gebruik van bepaalde applicaties, zoals TikTok, op overheidstoestellen?

De heer Kris Verduyckt (Vooruit) vraagt of er momenteel binnen Defensie voldoende capaciteit bestaat om aan preventie te doen bij de eigen manschappen – en eventueel ook bij andere overheidsdiensten – inzake het gebruik van mobiele toestellen? Heeft deze preventie ook gunstige effecten? Worden de interceptierisico's op de moderne wapensystemen, bijvoorbeeld drones en vliegtuigen, ook op Europees niveau aangepakt? Zal het *Cyber Command* ook anticiperend offensief optreden om vijandige acties te voorkomen? Volstaat de huidige veiligheidsscreening van rekruten – cf. affaire Conings? De beveiliging van lokale besturen, steden en gemeenten, vergt wellicht een specifieke architectuur; hoe ziet generaal van Strythem dit?

De heer Georges Dallemagne (cdH) wijst erop dat men cyberveiligheid al te lang heeft verwaarloosd en dat het uiterst dringend is om maatregelen te nemen – zoals ook blijkt uit de hoorzitting vandaag. In dat verband vraagt de heer Dallemagne dat generaal Van Strythem aan de commissie een boordtabel zou bezorgen over de middelen (menselijk, technologisch, financieel) waarover het *Cyber Command* momenteel reeds beschikt en deze die op korte termijn noodzakelijk zijn, evenals een evaluatie van de wettelijke basis voor de werkzaamheden van de nieuwe component met het oog op eventuele aanpassingen aan de geldende wetgeving. Kan generaal van Strythem ook aangeven welke dreigingen hij bij voorrang wil aanpakken? De heer Dallemagne begrijpt overigens niet dat de minister van Defensie nog steeds de applicatie TikTok gebruikt, gelet op de risico's die deze kennelijk inhoudt; heeft de heer Van Strythem haar daarover richtlijnen gegeven of werden er bijzondere beveiligingsmaatregelen genomen? Moeten er ook niet dringend aanbevelingen worden geformuleerd aan alle

l'attention de tous les organismes publics, et aussi des parlementaires, afin de répondre à cette menace et de faire en sorte que tout le monde soit bien conscient des risques pour la sécurité?

Mme Julie Chanson (Ecolo-Groen) pose une série de questions ciblées. Les cyberattaques contre la Belgique ont-elles augmenté depuis la guerre en Ukraine? Cela a-t-il provoqué des perturbations importantes? Comment le *Cyber Command* collabore-t-il avec des services similaires dans d'autres pays, et l'Union européenne ne doit-elle pas jouer davantage un rôle de premier plan? L'infrastructure critique en Belgique est-elle suffisamment protégée, et de quelle manière? Est-il exact que la Belgique est plus exposée aux cyberattaques que d'autres pays (voisins), en raison de la présence de nombreuses organisations supranationales et internationales? Les installations de sécurisation de ces organisations dépendent-elles des nôtres et sont-elles efficaces? Les attaques qui n'émanent pas d'acteurs étatiques mais de collectifs de *hackers* sont-elles traitées différemment et quels en sont les risques spécifiques? La lutte contre les campagnes de déstabilisation sur Internet (cf. les campagnes de l'alt-right au sein de l'UE) fait-elle aussi partie des missions du *Cyber Command* et, si oui, comment s'y prend-il? Il est clair que les systèmes connectés sont vulnérables et peuvent être instrumentalisés par les *hackers*; font-ils l'objet d'une analyse des risques et, si oui, comment le suivi éventuel est-il effectué?

C. **Réponses de l'orateur**

M. Van Strythem souligne qu'il ne peut répondre à certaines questions en séance publique car il s'agit d'informations classifiées; il ne répondra pas non plus aux questions adressées à la ministre de la Défense.

• En ce qui concerne le développement du *Cyber Command*, il y a effectivement encore beaucoup de travail à accomplir. Ainsi, il ressort d'une étude comparative avec, notamment, son équivalent français que l'effectif du personnel devrait compter environ 800 ETP, alors qu'on n'en est même pas à la moitié. Une feuille de route pour le court terme prévoit la mise en œuvre immédiate de plusieurs programmes, conformément à la décision du Conseil des ministres du 3 février 2023. Ces programmes permettront de moderniser les systèmes défensifs et de renouveler les moyens consacrés à la collecte d'informations en matière de cybersécurité et à leur traitement. Le général Van Strythem souligne l'importance d'une mise en œuvre rapide de ces projets et demande aux membres de la commission qu'ils insistent auprès des instances de contrôle des procédures d'achat afin que ces dossiers soient traités rapidement. C'est important, car la reconversion de l'architecture d'un *cyber operation*

overheidsinstellingen, ook aan parlementsleden, teneinde deze dreiging aan te pakken en iedereen terdege bewust te maken van de veiligheidsrisico's?

Mevrouw Julie Chanson (Ecolo-Groen) stelt een aantal gerichte vragen. Zijn de cyberaanvallen gericht tegen België sinds de oorlog in Oekraïne in aantal zijn toegenomen, waren er daardoor grote storingen? Hoe werkt het *Cyber Command* samen met soortgelijke diensten in andere landen en moet de Europese Unie niet meer op het voorplan treden? Wordt de kritieke infrastructuur In België afdoende beschermd en op welke wijze dan? Klopt het dat België meer dan andere (buur)landen aan cyberaanvallen is blootgesteld, cf. de aanwezigheid in ons land van talrijke *supra*- en internationale organisaties? Zijn de beveiligingsinstallaties van deze instellingen afhankelijk van de onze en zijn ze afdoend? Worden aanvallen die niet uitgaan van statelijke actoren maar van hackerscollectieven verschillend aangepakt en wat zijn de specifieke risico's ervan? Behoort de strijd tegen destabiliseringscampagnes via internet (cf. campagnes van Alt Right in EU) ook tot de opdracht van het *Cyber Command* en hoe wordt dit desgevallend aangepakt? Geconnecteerde systemen zijn ongetwijfeld kwetsbaar en kunnen instrumenteel worden aangewend door hackers; bestaat hierover een risicoanalyse en hoe wordt die gebeurlijk opgevolgd?

C. **Antwoorden van de spreker**

De heer Van Strythem wijst erop dat hij bepaalde vragen niet kan beantwoorden in openbare zitting aangezien het geclassifieerde informatie betreft; ook de vragen gericht aan de minister van Defensie zal hij niet beantwoorden.

• Voor de uitbouw van de *Cyber Command* moet inderdaad nog heel wat gebeuren. Zo blijkt uit een benchmark met o.a. de Franse evenknie dat het personeelsbestand ongeveer 800 VTE zou moeten bedragen, terwijl men nog niet aan de helft daarvan zit. Er is een roadmap voor de korte termijn, waarbij een aantal programma's overeenkomstig de beslissing van de Ministerraad van 3 februari 2023 nu worden uitgevoerd en die zullen toelaten de defensieve systemen te moderniseren en de middelen inzake informatiegaring en -verwerking op het vlak van cyberveiligheid te vernieuwen. Generaal Van Strythem benadrukt het belang van een snelle realisatie van deze projecten en vraagt de steun van de commissieleden om bij de controle-instanties op de aankoopprocedures aan te dringen op een vlotte afhandeling van deze dossiers. Dit is belangrijk omdat de omschakeling van de architectuur van een *cyber operation centre* zo snel mogelijk moet gebeuren. Zo mogelijk nog belangrijker, zijn inderdaad

centre doit avoir lieu aussi vite que possible. La mise en place de procédures Selor adaptées afin de recruter du personnel civil pour des profils de fonction spécifiques est effectivement un point peut-être encore plus important. La rapidité et la flexibilité du processus de recrutement sont essentielles, eu égard à la concurrence féroce sur le marché du travail pour ce type de profils.

• Il y aura en effet un partenariat avec l'ERM et l'ESA (*European Space Agency*) à Redu, axé sur la transmission des connaissances.

• À l'heure actuelle, il est difficile de prédire quel effectif du personnel sera finalement requis pour la nouvelle composante en 2030. D'ailleurs, on ne connaît pas encore non plus clairement le montant total du budget qui sera nécessaire, vu la rapidité des évolutions dans ce domaine. La seule certitude est qu'il faut à présent agir vite afin de réaliser des avancées substantielles (notamment en ce qui concerne la mise en œuvre des programmes actuellement planifiés: le Plan STAR et les plans de relance FRR de l'UE et nationaux).

• Lors du lancement du *cyber project office* à la mi-2021, le nombre de cyberprojets auxquels la Belgique collabore est passé de deux à cinq. Le général Van Strythem renvoie à cet égard à une communication conjointe de la Commission européenne et du Haut représentant de l'Union pour les affaires étrangères du 10 novembre 2022 sur la stratégie de l'UE en matière de cyberdéfense, qui soulignait notamment la nécessité d'une bonne coopération et d'une bonne concertation entre les différents *cyber commands*.

• La coopération aux travaux de l'agence ENISA (Agence de l'Union européenne pour la cybersécurité) est assurée par le CCB, mais fera également l'objet d'un suivi par le cybercommandement (*Cyber command)*. Le Centre d'excellence pour la cyberdéfense en coopération (CCD CoE) de l'OTAN est également un partenaire important, notamment pour relever les défis en matière de recrutement.

• La défense des infrastructures critiques doit être assurée par plusieurs acteurs, mais d'abord par les secteurs critiques eux-mêmes. Le CCB joue le rôle de coordinateur national. La mise en œuvre de la directive européenne 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI 2) devra en préciser les modalités. De plus, la notion d'"infrastructures critiques" (exemple: centrale électrique) a fait place à la notion d'"entité critique" (ensemble de la chaîne de production d'électricité jusqu'au consommateur). À cet égard, le point de contact central est le Centre de crise national. Sur ce plan, la Défense joue un double rôle: elle

aangepaste Selor-procedures voor de rekrutering van burgerpersoneel voor specifieke functieprofielen. De snelheid en flexibiliteit van het wervingsproces is belangrijk in het licht van de hevige concurrentie op de arbeidsmarkt voor deze profielen.

• Er komt inderdaad een partnerschap met de KMS, met het ESA in Redu (*European Space Agency*) gericht op kennisborging.

• Hoeveel personeel in 2030 uiteindelijk zal vereist zijn voor de nieuwe component, is moeilijk te zeggen op dit moment. Er is trouwens ook geen duidelijkheid, gezien de snelheid van evolutie van dit domein, over de volledige omvang van het toekomstig noodzakelijk budget. De enige zekerheid is dat er nu snel moet geschakeld worden teneinde substantiële vorderingen te maken (o.a. m.b.t. de implementatie van de huidig geplande programma's: STAR-Plan en relance plannen EU RRF en nationaal).

• Bij het opstarten van het *cyber project office* midden 2021 werd het aantal Europese cyberprojecten waaraan België meewerkt verhoogd van 2 naar 5. Generaal Van Strythem verwijst in dit verband naar een Gezamenlijke mededeling van de Europese Commissie en de Hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid van 10 november 2022 over de EU-strategie inzake cyberdefensie die onder meer de noodzaak benadrukt van een goede samenwerking en overleg tussen de onderscheiden *cyber commands*.

• De medewerking aan de werkzaamheden van ENISA (Agentschap van de Europese Unie voor cyberbeveiliging) gebeurt door het CCB, maar het *Cyber Command* volgt dit eveneens op. Ook het NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) is een belangrijke partner onder meer voor uitdagingen inzake rekrutering.

• De verdediging van kritische infrastructuur moet door meerdere spelers gebeuren, in de eerste plaats de kritische sectoren zelf. Het CCB heeft de rol van nationale coördinator. De implementatie Europese Richtlijn 2022/2555 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie (zogenaamde NIS2-richtlijn) zal de concrete uitwerking hiervan moeten verduidelijken. Overigens evolueert het begrip "kritische infrastructuur" (bijvoorbeeld een elektriciteitscentrale) naar "kritische entiteit" (de volledige elektrische productieketen tot bij de verbruiker). Het centrale contactpunt hiervoor is het Nationaal Crisiscentrum. Defensie heeft hierin een dubbele rol: de

contribue à l'élaboration d'une stratégie nationale dans le domaine de la cybersécurité et elle se concentre sur la simulation de scénarios d'attaques multiples de forte intensité. Dans ce cadre, la Défense souhaite investir dans la recherche et le développement à l'ERM, ainsi que dans la constitution de réseaux avec des centres de recherche belges et européens.

• En réponse aux questions relatives à la sensibilisation de la population, il est indiqué que cette mission relève également du CCB, qui est aussi le point de contact national en matière de cybersécurité. Le CCB gère notamment l'application *Safeonweb.be*. En cas de cyberattaque, le CCB renforcera sa capacité et fera appel à d'autres services, y compris au *Cyber Command*.

• En ce qui concerne TikTok: depuis début 2022, l'utilisation de TikTok fait l'objet d'un avis négatif du SGRS. La DG StratCom de la Défense s'appuie sur cet avis pour interdire cette application sur tout appareil disposant de comptes de la Défense et, pour pouvoir l'utiliser sur des appareils distincts, les unités doivent adresser une demande dûment motivée à la DG StratCom. Le Général Van Strythem souligne que tout réseau social peut présenter des risques et qu'il convient de satisfaire au moins à deux conditions: la double authentification et un protocole *https* sécurisé.

Les rapporteurs, *Le président,*

Samuel Cogolati
Michael Freilich

Peter Buysrogge

bijdrage aan de uitbouw van een nationale strategie voor cyberveiligheid en de focus bij de projectie van scenario's op meervoudige aanvallen van hogere intensiteit. Defensie wenst in dit verband in de schoot van de KMS te investeren in onderzoek en ontwikkeling en de netwerking met Belgische en Europese onderzoekscentra.

• Wat betreft de vragen over sensibilisering van de bevolking, dit is eveneens een taak van het CCB dat tevens het nationaal contactpunt is voor cyberveiligheid. Het CCB beheert onder meer de applicatie *Safeonweb.be*. In geval van een cyberaanval zal CCB dit opschalen en andere diensten, inbegrepen het *Cyber Command*, inschakelen.

• Betreffende TikTok: sinds begin 2022 is er een negatief advies van ADIV voor het gebruik van TikTok op basis waarvan Defensie DG StratCom de applicatie niet toelaat op toestellen waar accounts van Defensie op staan en de eenheden moeten voor het gebruik op aparte toestellen een duidelijk gemotiveerde aanvraag richten tot DG StratCom. Generaal Van Strythem benadrukt dat elke sociale media applicatie risico's kan inhouden en er minstens moet voldaan zijn aan de dubbele voorwaarde van dubbele authenticatie en een veilig *https-protocol.*

De rapporteurs, *De voorzitter,*

Samuel Cogolati
Michael Freilich

Peter Buysrogge

Imprimerie centrale – Centrale drukkerij