



**VSSE** veiligheid van de staat  
sûreté de l'état

# INTELLIGENCE REPORT 2024

**VEILIGHEID VAN DE STAAT**

**.be**



Verantwoordelijke uitgever: Francisca BOSTYN  
Koning Albert II-laan, 6 - 1000 Brussel

# INHOUDSTAFEL

---

## 4 VOORWOORD VAN DE ADMINISTRATEUR-GENERAAL

## 6

### DEEL 1: DE VSSE ALS INLICHTINGEDIENST

- Een escalatie van hybride dreigingen in België en Europa 7
- Rusland kiest voor agressieve strategieën om het Westen te destabiliseren 8
- De Noordzee: een ideaal actieterrain voor hybride oorlogsvoering 10
- Desinformatie en polarisering in een dubbel verkiezingsjaar 11
- België niet immuun voor cyberaanvallen 13
- De VSSE strijdt tegen het omzeilen van de sancties tegen Rusland 14
- De VSSE werkte mee aan onderzoek naar Russische inmenging in het Europees Parlement 15
- Spionage en inmenging in het Strafwetboek 16
- China: een moeilijk evenwicht tussen belangen en risico's 18
- De jihadistische terreurdreiging is een veelkoppig monster 20
- Bijna één op drie betrokkenen in terrorismedossiers van de VSSE is minderjarig 22
- Extremistische propaganda spoort *lone actors* aan tot terreur 24
- De conflicten in het Midden-Oosten en hun impact op België 26
- De dreiging van religieus en ideologisch extremisme 27
- De VSSE en de ADIV leggen wekelijks terrorismedossiers voor aan politie en parket 29
- De VSSE draagt bij tot de strijd tegen de georganiseerde criminaliteit 31

## 32

### DEEL 2: DE VSSE ALS VEILIGHEIDSDIENST

- De VSSE werkt aan een versterking van de veiligheidscultuur 33
- De NVO leverde bijna 5 keer meer veiligheidsmachtigingen af op 5 jaar tijd 34
- De VSSE verrichtte 36 procent meer veiligheidsverificaties in 2024 35
- De VSSE formuleerde 86 adviezen over buitenlandse directe investeringen 36

## 37

### DEEL 3: OVER DE VSSE

- De VSSE in cijfers in 2024 38
- De VSSE declassificeert haar archieven over Wereldoorlog II 39



Francisca BOSTYN  
Administrateur-generaal

## VOORWOORD

Naar goede jaarlijkse traditie presenteer ik u het *Intelligence Report* van de Veiligheid van de Staat (VSSE). Ook nu kunnen we er opnieuw niet omheen dat de internationale geopolitieke context een invloed uitoefent op onze binnenlandse veiligheid. De Russische agressie is daar de laatste jaren natuurlijk een belangrijke aanjager in. Er blijven bijvoorbeeld pogingen tot inmenging in democratische processen naar boven komen. Denken we in dit verband maar aan het *Voice of Europe*-verhaal dat vorig jaar werd bloot gelegd.

Maar er zijn ook nieuwe strijdtonelen ontstaan die in het verleden niet altijd op onze radar stonden, zoals bijvoorbeeld de Noordzee. Verdachte acties van schepen op de Noordzee zijn vandaag niet meer weg te denken uit het nieuws en verplichten de VSSE om samen met de Belgische partners actief dit soort nieuwe evoluties op te volgen.

Desinformatie en polarisering zijn dan weer jaarlijks terugkerende problematieken, en zeker in een verkiezingsjaar was dit iets om extra oplettend voor te zijn. Ik ben ervan overtuigd dat deze oplettendheid een standaardonderdeel moet zijn van onze aanpak van buitenlandse dreigingen tegen onze Westerse democratieën. Elk maatschappelijk gevoelig onderwerp kan en zal door buitenlandse actoren namelijk worden gebruikt om polarisering aan te wakkeren. Polarisering, aangeblazen door desinformatie, is subtiel en moeilijk aan te pakken maar kan maatschappelijk bijzonder ontwrichtend zijn. Dit opvolgen, zal dus een blijvende uitdaging zijn voor de VSSE.

In hun hybride acties gaan onze tegenstanders vaak ook heel inventief te werk. Samen met andere Europese inlichtingendiensten stellen we bijvoorbeeld vast dat individuen op een veel lossere basis worden gerekruteerd, bijvoorbeeld via Telegram – het gaat bij wijze van spreken om *freelancers* die ad hoc worden ingeschakeld om onder meer spionage- of sabotageacties uit te voeren. Het spreekt voor zich dat deze manier van werken het voor inlichtingen- en veiligheidsdiensten complexer maakt om op te treden.

In deze context moeten we als inlichtingendienst flexibel zijn en moeten we kunnen beschikken over aangepaste middelen om ons te beschermen. Ik ben dus heel tevreden dat de VSSE sinds 2024 kan rekenen op het herziene Strafwetboek waarin spionage en inmenging strafbaar worden gesteld.

Recente aanslagen in New Orleans en Maagdenburg tonen aan dat terreur een van de belangrijkste dreigingen blijft, ook voor de VSSE. De Islamitische Staat (IS) en zijn franchise in de Khorasan Provincie (ISKP) vormen daarbij de voornaamste bedreigingen voor België, ook al omdat hun ideologie *lone actors* kan aanzetten tot acties. De ISKP-dreiging leidde zo in ons land in juli 2024 tot gerechtelijke tussenkomsten bij een aantal sympathisanten. Een andere opvallende en onrustwekkende vaststelling is het feit dat één op de drie betrokkenen in terrorismedossiers van de VSSE minderjarig is. Dit is niet alleen een uitdaging voor de veiligheidsdiensten maar ook voor sociopreventieve spelers die zich

richten op jeugd. Gelukkig zijn de actiemogelijkheden voor minderjarigen beperkter, waardoor ze minder vaak in de uitvoeringsfase van hun aanslagplannen terecht komen.

De ontwikkelingen in Syrië in december 2024 duwden de problematiek van de resterende Belgische *foreign terrorist fighters* in die zone terug op de voorgrond. Het is het duidelijkste voorbeeld van hoe buitenlandse evoluties een invloed kunnen hebben op onze eigen veiligheid: onafhankelijk van welke oplossing men ziet voor dit probleem kan men namelijk niet ontkennen dat deze *foreign terrorist fighters* een veiligheidsprobleem zijn voor ons land.

Daarnaast wil ik erop wijzen dat de VSSE meer is dan enkel een inlichtingendienst, we zijn ook een organisatie die een belangrijke opdracht heeft op het vlak van veiligheid. Dit is meer dan ooit het geval sinds de Nationale Veiligheidsoverheid begin 2024 een onderdeel is geworden van de VSSE. De Nationale Veiligheidsoverheid is onder meer verantwoordelijk voor het afleveren van veiligheidsmachtigingen en het garanderen van de correcte omgang met geclassificeerde informatie – dat laatste doen we onder andere via het actief sensibiliseren van de veiligheidsofficieren die in meer en meer organisaties aanwezig zijn. De veiligheidscontext waarin we leven en een toegenomen veiligheidsbewustzijn hebben geleid tot een sterke stijging van de werklust, het is belangrijk dat we dit erkennen en ook kenbaar maken.

Tot slot wil ik graag nog op een aantal belangrijke uitdagingen voor de toekomst wijzen.

Er zijn eerst en vooral de uitdagingen verbonden aan cyberdreigingen en aan de razendsnelle ontwikkelingen op het vlak van nieuwe technologieën. Om mee te blijven, moeten we ze ons snel eigen maken. De waaier aan technologieën die we moeten afdekken, is echter ruim en gaat van het integreren van artificiële intelligentie in ons dagelijks werk tot het vinden van oplossingen voor toegang tot versleutelde communicatie.

De technologische uitdaging brengt drie andere uitdagingen met zich mee. Ten eerste is er de menselijke. Het vinden van gekwalificeerd personeel dat deze technologische complexiteit beheerst, is niet evident. En als we ze vinden, hoe zorgen we er dan voor dat we hen een aantrekkelijk loon en attractieve arbeidsvoorwaarden kunnen bieden? Dit soort specialisaties is zeer gegeerd op de private markt, die veel meer financiële slagkracht bezit dan

een federale administratie.

Ten tweede is er de juridische uitdaging: de snel evoluerende dreigingen en technologische evoluties vragen om voortdurend aangepaste wetgeving die veel tijd vraagt om tot stand te brengen. En ten derde is er de exponentiële toename van gegevens. Als inlichtingendienst moeten we constant nieuwe manieren vinden om die enorme hoeveelheden informatie te verwerken. Binnen de VSSE zijn we nog volop bezig met de implementatie van een nieuw onderzoeksmodel en een nieuwe IT-omgeving die ons op termijn in staat moeten stellen om hier beter mee om te gaan. En dit zal ook in de toekomst blijvende investeringen vragen.

Een laatste grote uitdaging die ik zie, is de bijdrage die de VSSE zal moeten leveren om ons land weerbaarder te maken in tijden waarin weer openlijk over oorlog in Europa wordt gesproken. De politieke wereld en de veiligheidsdiensten zijn zich er meer en meer van bewust dat we onze maatschappij beter moeten voorbereiden op oorlog en andere crisissituaties. Hoe blijven ziekenhuizen en energiecentrales draaien? Hoe maken we grote troepenverplaatsingen mogelijk? En hoe moet de VSSE haar inlichtingenwerking aanpassen wanneer België betrokken wordt in een gewapend conflict? De vraag is ook hoe we onze economische welvaart kunnen vrijwaren. Dat gaat niet alleen over het beschermen van onze intellectuele eigendom, maar ook over de fysieke bescherming van onze kritieke infrastructuur. De druk op ons economisch weefsel is iets waar België en Europa in de toekomst nog meer aandacht voor moeten hebben, te meer gezien de toenemende assertiviteit van landen als China.

Samen met onze Belgische en internationale partners – samenwerken is essentieel in een wereld waarin grenzen niet bestaan als het over veiligheid gaat – blijven we ons elke dag dubbelplooien om onze democratie en de inwoners van ons land te beschermen. De voorbije jaren hebben we de kans gekregen om onze dienst gevoelig te versterken op het vlak van personeel en budget. Alle nieuwe en minder nieuwe medewerkers wil ik langs deze weg ook danken voor hun dagelijkse inzet, gedrevenheid en geloof in onze missie. Ik ben ervan overtuigd dat we met zijn allen klaar zijn om onze verantwoordelijkheid te nemen in de nieuwe realiteit waarin we leven.

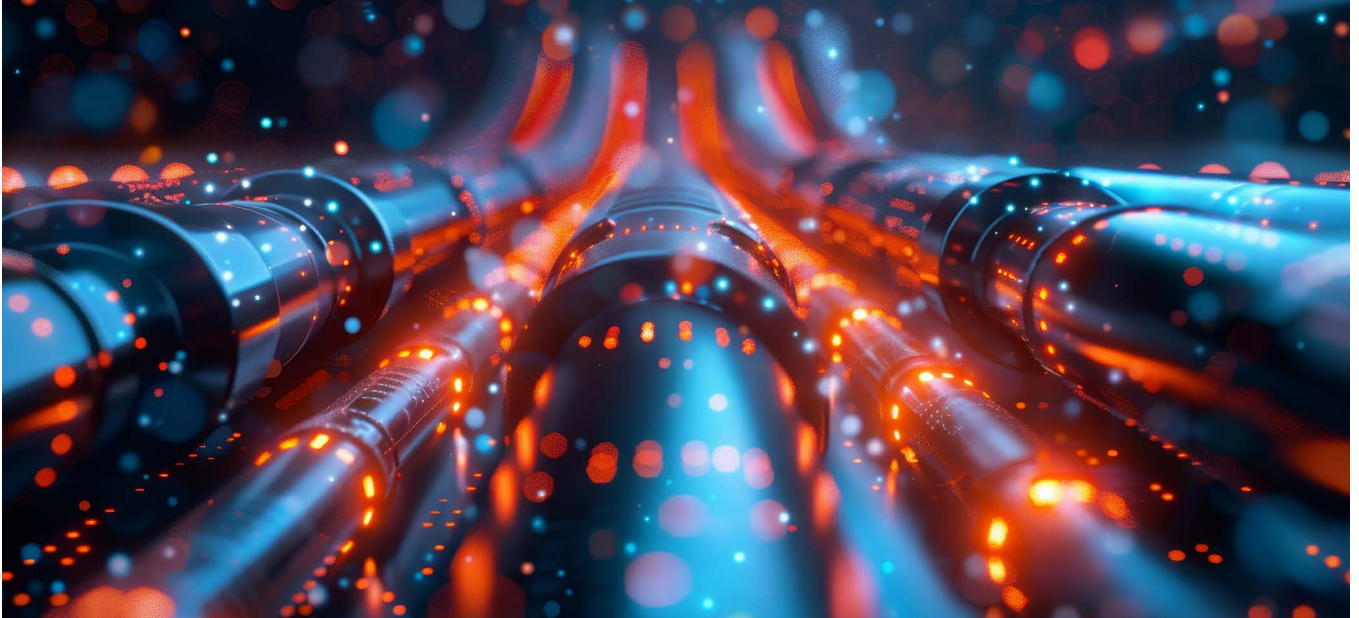
Francisca Boslyn

# 01

**DE VSSE ALS INLICHTINGDIENST**

# EEN ESCALATIE VAN HYBRIDE DREIGINGEN IN BELGIË EN EUROPA

Exploderende pakketjes in sorteercentra van een koerierdienst op Europese luchthavens, sabotage aan spoorwegen, verkenningdrones boven militaire kazernes, cyberaanvallen, slepende scheepsankers die internetkabels aan flarden trekken op de zeebodem, polariserende desinformatie. 2024 was het jaar van de escalatie van de hybride dreigingen. Doorgaans te wijten aan de Russische hybride oorlogsvoering.



De term hybride dreiging verwijst naar een combinatie van activiteiten, uitgevoerd door statelijke en/of niet-statale actoren, met als doel om ongemerkt een tegenstander of zijn instellingen negatief te beïnvloeden of schade toe te brengen. Belangrijk hierbij is het 'ongemerkt' karakter. Een hybride dreiging kan even concreet zijn als een klassieke kinetische aanval, maar het wordt nooit duidelijk voor wiens rekening de aanval juist werd uitgevoerd. Die strategie wordt welbewust gehanteerd. Ze verhindert immers dat er een geconsolideerde reactie komt, bijvoorbeeld van de NAVO. Door de hybride aanpak, via moeilijk definieerbare daders, is het niet eenvoudig om dergelijke acties met zekerheid toe te wijzen, en dus blijft ook een reactie soms uit.

Dat is het succes van de hybride dreiging: het lanceren van activiteiten die schade veroorzaken, zonder veel risico op een reactie. Er zijn bijzonder veel aanwijzingen dat Rusland het voorbije jaar zijn hybride acties in Europa heeft opgeschaald. Zowel geografisch, van Oost- tot West-Europa, als qua methode. Rusland is erg bedreven in de hybride oorlogsvoering en werkt met hackerscollectieven (cyberdreiging), met criminele organisaties (aanslagen op kritieke infrastructuur) en met *freelance* agenten om dit zo veel als mogelijk verholven te doen.

Waar de blik de jongste twee jaren focust op de acties die toe te wijzen zijn aan Rusland, laten ook andere statelijke of niet-statale actoren zich niet onbetuigd. Zo blijft met name ook China gebruik maken van een breed scala aan hybride methoden.

## ► EEN WHOLE OF SOCIETY-AANPAK

Een van de belangrijkste uitdagingen voor inlichtingendiensten vandaag is om te anticiperen op deze aanvallen, ze in kaart te brengen (niet iedereen in een commerciële omgeving pakt graag uit met zijn zwakheden), en ze toe te kunnen wijzen aan een specifieke actor. Dat is specialistenwerk waar de VSSE op nationaal en op internationaal vlak rond samenwerkt.

Elke actor heeft op dit terrein een rol te spelen. In België werkt de VSSE op dit vlak nauw samen met het Nationaal Crisiscentrum (NCCN), de Algemene Dienst Inlichting en Veiligheid (ADIV), de Federale Politie, het OCAD en het Centrum voor Cybersecurity België (CCB), maar ook met bedrijven uit de privésector. Het zal van onze collectieve reactie afhangen of we zwakker dan wel sterker uit deze periode komen.

# RUSLAND KIEST VOOR AGRESSIEVE STRATEGIEËN OM HET WESTEN TE DESTABILISEREN

De massale uitwijzingen van Russische inlichtingsofficieren onder diplomatieke dekmantel uit EU-landen hebben Moskou in een lastig parket gebracht: de capaciteiten van de Russische inlichtingendiensten op Europese bodem hebben een stevige knauw gekregen, terwijl hun ambities onveranderd zijn. In een poging dit op te lossen, gaan de Russische inlichtingendiensten creatief te werk.



Sinds de grootschalige invasie van Oekraïne door Rusland begin 2022 hebben honderden 'klassieke' Russische inlichtingsofficieren de Europese Unie en partnerlanden als het Verenigd Koninkrijk en Noorwegen moeten verlaten. Deze inlichtingsofficieren hadden doorgaans een officieel statuut als diplomaat bij de Russische vertegenwoordigingen – in België waren dat de Russische ambassade en de missie bij de EU in Brussel, en het consulaat-generaal in Antwerpen (de Russische missie bij de NAVO sloot al in 2021 de deuren, op eigen initiatief). De uitwijzingen in 2022 en 2023 gebeurden grotendeels door hen 'persona non grata' te verklaren. Ons land zorgde er zo voor dat tientallen Russische inlichtingsofficieren zich gedwongen zagen naar Moskou terug te keren.

Dit betekende enerzijds dat Ruslands inlichtingendiensten hun capaciteit en bewegingsvrijheid op Europese bodem ernstig beperkt zagen. Anderzijds verdwenen de Russische inlichtingen-

behoefte hier niet, integendeel. De oorlog blijft aanslepen en Moskou omschrijft zijn agressie als een strijd met de Westerse wereld. Rusland kiest hierbij voor een agressieve, hybride strategie: enerzijds wil het specifieke inlichtingen over bijvoorbeeld de Europese militaire en financiële steun aan Oekraïne of over sanctieregimes, anderzijds streeft het ook naar het destabiliseren en decredibiliseren van de Westerse wereld door maatschappelijke onrust te creëren of op te poken, of door zijn eigen ideologische narratieven te verspreiden.

Het voorbije jaar is duidelijk geworden dat de Russische diensten in hun zoektocht naar nieuwe manieren om inlichtingen te verzamelen en operaties uit te voeren, zijn overgeschakeld op een innovatieve manier van rekrutering en tasking van agenten, in de logica van de *gig economy* – dit is een arbeidsmarkt gebaseerd op flexibele, tijdelijke of *freelance jobs*. Via sociale media (met name Telegram) en met gebruik van (meerdere) tussen-





personen worden opdrachten wijd verspreid, op te pikken door wie er maar voor openstaat, net zoals eerder via Uber 'eventjes' taxichauffeur kan zijn, of via Deliveroo een zakcentje kan bijverdienen als fietskoerier. De Russische diensten doen ook in toenemende mate een beroep op criminele netwerken, wat de detectie van hun activiteiten moeilijker maakt.

De opdrachten die uitbesteed worden aan deze *freelancers* of aan criminele organisaties gaan van het verzamelen van inlichtingen, over propaganda-acties tot militaire verkenning en sabotage (zie kader). Zo werd in Londen een depot voor materiele steun aan Oekraïne in brand gestoken; de daders worden momenteel berecht. In België zijn er tot nu geen bevestigde gevallen van spionage- en subversieacties uitgevoerd door *freelance* agenten of criminele organisaties in opdracht van de Russische inlichtingendiensten, maar dat betekent althans dat we ons niet moeten voorbereiden op dergelijke acties.

De inzet van criminele organisaties en de toepassing van de principes en lessen uit de *gig economy* zijn trouwens geen exclusiviteit voor de Russische inlichtingendiensten. Het inzetten van individuen die geen enkele zichtbare, directe band hebben met het milieu van de inlichtingendiensten voor welomschreven inlichtingenoperaties is een fenomeen dat aan belang en omvang wint. Dit verkleint immers de kansen dat professionele inlichtingsofficieren gecompromitteerd worden tijdens een operatie, en het verhoogt de *plausible deniability*

## ► FREELANCEN ALS AGENT VOOR RUSLAND

Rekrutering van *freelance* agenten via sociale media is een stapsgewijs proces, waarbij potentiële agenten zich enerzijds moeten bewijzen en anderzijds verstrikt raken in steeds verdere compromittering, net zoals dat bij klassieke rekrutering gebeurt.

- Een zoekertje met een simpele opdracht verschijnt in een Telegramgroep: 'ga een stel anti-Oekraïense stickers plakken in het straatbeeld en krijg 20 euro'. Een geïnteresseerde gaat erop in, een bot stelt hem enkele basisvragen.
- De kandidaat slaagt voor de testvragen. Een Russisch inlichtingsofficier neemt de chat over en geeft hem verdere instructies. De agent voert de taak uit en stuurt een foto door als bewijs. Hij wordt betaald in cryptomunten.
- Een tweede, risicovollere en mogelijk onwettige opdracht volgt: 'ga deze militaire infrastructuur fotograferen'.
- De opdrachten volgen elkaar op en worden almaar zwaarder. De uitvoerder zit nu diep in de illegaliteit. Uiteindelijk volgt een vraag tot sabotage.

Dit is een geabstraheerd voorbeeld.

waar vijandige inlichtingendiensten (en hun politieke leiders) naar streven.

Kortom, door een beroep te doen op *freelancers* en criminele organisaties slaan de buitenlandse inlichtingendiensten twee vliegen in één klap: ze wekken de indruk dat ze overal actief (kunnen) zijn, terwijl de activiteiten zelden echt tot hen te herleiden zijn.

## ► GEEN PANIEK

Het doel van Rusland is hierbij niet alleen om de steun aan Oekraïne te dwarsbomen, maar ook het destabiliseren van westerse samenlevingen is een doelstelling op zich. Het is verleidelijk om plots in elk voorval de hand van Moskou te zien. Dat zou het Kremlin echter in de kaart spelen: paniek doen ontstaan door de valse indruk te wekken dat Rusland eerder waar, eerder wanneer kan toeslaan. Dat is net een van de objectieven van deze nieuwe *modus operandi*. Daarom moeten de VSSE en haar partners er over waken geen loze ophef te creëren bij de opvolging van dit fenomeen.

# DE NOORDZEE: EEN IDEEAAL ACTIETERREIN VOOR HYBRIDE OORLOGSVOERING



**De Noordzee is een ideaal actieterrein voor hybride oorlogsvoering. Op zee kan een vijandelijke actor immers vrij gemakkelijk ongemerkt ageren. Zeker indien hij daarvoor niet alleen militaire schepen, maar ook containerschepen, onderzoeksschepen of zelfs gewone zeiljachten kan inzetten. Wat is er immers verdacht aan een zeilschip dat op de Noordzee wat ronddobbert? Of een cargoschip dat zijn anker wat te lang laat slepen over de zeebodem?**

De Noordzee is bij uitstek een strategische omgeving waar datakabels, energiekabels en gaspijpleidingen liggen. Het aantal incidenten met zulke leidingen en kabels in onder meer de Oostzee neemt toe. Ook het stukje Noordzee voor de Belgische kust is een mogelijk doelwit. De laatste maanden worden steeds meer verdachte bewegingen vastgesteld van schepen die soms ook illegale trajecten volgen.

Het moge duidelijk zijn dat deze verdachte bewegingen goed opgevolgd worden door de verschillende Belgische diensten in het Maritiem Informatieknooppunt (MIK). Het MIK is een onderdeel van de kustwachtcentrale in België. In dit centrum in Zeebrugge bundelen Douane, de Scheepvaartpolitie, Defensie en de cel maritieme beveiliging van de FOD Mobiliteit hun krachten en bevoegdheden om informatie te verzamelen, te analyseren en te delen. Zij werken zowel preventief

## ► ER BEWEEGT IETS ROND DE NOORDZEE

In april 2024 sloten de bevoegde ministers in zes landen die grenzen aan de Noordzee op initiatief van de Belgische minister van de Noordzee Paul Van Tigchelt een overeenkomst af waarin ze verklaren dat ze samen zullen werken om kritieke onderwaterinfrastructuur te beschermen tegen sabotage en aanvallen. Een onderdeel van die overeenkomst is de ontwikkeling van een systeem om veilig informatie over incidenten uit te kunnen wisselen.

In augustus 2024 was er dan in de marge van een energieconferentie in Stavanger, Noorwegen, een oproep van de inlichtingendiensten van acht Noordzeelanden om de onderwaterinfrastructuur op de Noordzee beter te beschermen.

In december 2024 organiseerde de Haven van Antwerpen-Brugge een interactieve avond over maritieme veiligheid voor vertegenwoordigers van de Belgische industrie, de maritieme wereld, het bankwezen, de academische wereld en de veiligheidssector.

als reactief om de veiligheid in de havens en op zee te verhogen. Een belangrijke taak want voor onze kust ligt een van de drukste scheepvaartroutes ter wereld. De VSSE staat continu in contact met het MIK en wisselt daarnaast ook informatie over de problematiek uit op internationale fora.



# DESINFORMATIE EN POLARISERING IN EEN DUBBEL VERKIEZINGSJAAR

2024 was een ongezien verkiezingsjaar. Wereldwijd konden meer dan 2 miljard mensen hun stem uitbrengen. Ook België hield verkiezingen, op alle niveaus, van het lokale tot het Europese. Om te verzekeren dat die vrij en eerlijk konden verlopen, zette de VSSE zowel in op eigen onderzoeken, als op een krachtenbundeling met binnen- en buitenlandse partners.



Verkiezingen zijn een gevoelige periode waarin desinformatie en inmenging potentieel een grotere impact kunnen hebben. Ook vijandige actoren beseffen dat. In het verkiezingsjaar 2024 circuleerde er dan ook heel wat desinformatie in het Belgische informatielandschap.

Maar Belgische politici, partijen of – meer algemeen – ons verkiezingsproces waren slechts zelden expliciet een doelwit. Die vaststelling is zowat de rode draad voor het hele Belgische verkiezingsjaar.

Wel trokken enkele extremistische en anti-establishmentstemmen uit eigen land bijvoorbeeld het eerlijke verloop van de verkiezingen in twijfel, onder andere met ongefundeerde insinuaties over de stemcomputers. Ook waren er anarchistische

en salafistische actoren die opriepen om niet te gaan stemmen. Maar de aantallen en het bereik van die boodschappen bleef erg beperkt. En nooit ging het om desinformatie die in staat was om de verkiezingen te verstoren of een impact te hebben op het resultaat.

## ► CONTINUE POLARISERING

Maar daarmee is het probleem niet weg. Vijandige actoren zoals Rusland bestoken haast continu het westerse – en dus ook het Belgische – informatielandschap met polariserende en antidemocratische boodschappen. Soms gaat het om volledig valse berichten, maar veel vaker trachten ze simpelweg gevoelige onderwerpen op te poken of polariserende incidenten te versterken en te misbruiken.

Naast 'klassiekers' zoals migratie of LGBTQI+-rechten, ging het in 2024 onder meer om de boerenprotesten, het conflict in Gaza of de westerse steun aan Oekraïne. Het doel is steeds hetzelfde: onze maatschappij verdelen en het geloof in onze democratie ondermijnen.

### ► VERSPREIDEN DESINFORMATIE ONDER BEPAALDE OMSTANDIGHEDEN STRAFBAAR

De VSSE is geen gedachtepolitie, noch zijn we factcheckers.

Valse informatie komt op onze radar wanneer vijandige actoren onze openheid en fundamentele vrijheden misbruiken om er hun eigen strategische belangen mee na te streven.

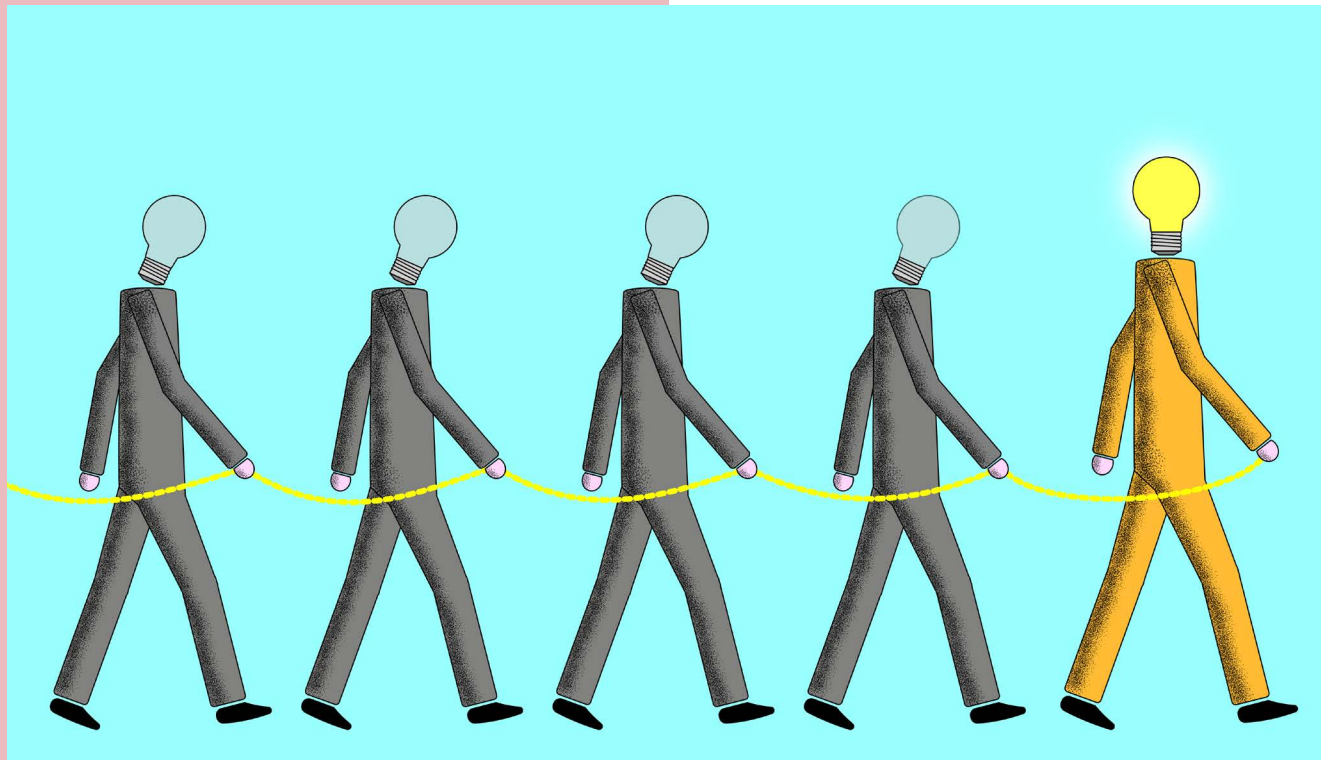
Het is nuttig op te merken dat het verstrekken van foute essentiële informatie aan Belgische overheden met het doel hen te misleiden en zo de essentiële nationale belangen te beschadigen, een strafbaar feit is. Een en ander is het gevolg van de nieuwe strafwet die sinds april 2024 van kracht is.

Geen enkele dienst kan daar alleen tegenop. Inlichtingendiensten zijn slechts één schakel in de strijd tegen desinformatie, waarin vooral media, onderwijs en het middenveld een belangrijke rol te spelen hebben.

### ► ARTIFICIËLE INTELLIGENTIE

Het gebruik van artificiële intelligentie was nauwelijks van tel bij de Belgische verkiezingen. Vooraf leefde de vrees dat artificiële intelligentie een turbo kon zetten op allerlei vormen van desinformatie. Denk bijvoorbeeld aan *deepfakes*, waarbij valse video- of audioclips van politici zouden opduiken om hen te compromitteren. Die vrees bleek – althans voor ons land – ongegrond.

Maar opnieuw geldt: waakzaamheid blijft geboden. Want ook los van verkiezingen kunnen valse filmpjes, *memes* en berichten blijven knagen aan onze maatschappelijke cohesie en het vertrouwen in onze democratische instellingen. En met artificiële intelligentie kan die inhoud steeds goedkoper, sneller én veel meer op maat van het doelpubliek worden aangemaakt en verspreid. ■



# BELGIË NIET IMMUUN VOOR CYBERAANVALLEN



**Dat België niet immuun is voor grootschalige cyberaanvallen werd duidelijk in de aanloop naar de gemeenteraadsverkiezingen van oktober 2024, toen tientallen websites onder vuur werden genomen door een pro-Russische hackersgroep. Deze aanval werd vooral aangewend voor propaganda-doeleinden, in andere gevallen worden soms ook vertrouwelijke gegevens ontvreemd.**

In de periode van 7 tot 13 oktober 2024 lanceerde de pro-Russische hacktivistgroep NoName057(16) cyberaanvallen gericht tegen diverse Belgische websites. Het ging om Distributed Denial of Service (DDoS) aanvallen, waarbij websites/online services worden bestookt met grote hoeveelheden internetverkeer met als doelstelling deze te overbelasten zodat ze tijdelijk niet langer (vlot) bereikbaar zijn voor gebruikers. Bij dit type aanval worden geen gegevens gestolen of is er geen sprake van intrusie.

## ► VERGELDING VOOR OEKRAÏNE

De aanvallen waren volgens berichtgeving van de groepering een vergelding voor de wapenleveringen die België plande ter ondersteuning van Oekraïne. Er werd specifiek naar de beloofde levering van CAESAR-artillerieëenheden verwezen. Ondanks de timing van de aanvallen – een week voor de lokale verkiezingen – en een beperkte melding van deze verkiezingen in de communicatie van de groep, lag de focus dus niet op de verkiezingen.

De DDoS-aanvallen waren gericht tegen verschillende doelwitten. Het overgrote deel van de aanvallen werd uitgevoerd tegen de websites van lokale overheden (gemeenten en provincies). Maar ook enkele websites van de federale overheid (FOD Financiën, FOD Economie), websites van zeehavens, bpost, sectorfederaties (Febelgra, Febelfin), persagentschap Belga,... werden gevisieerd door

de aanvallen. De impact van deze aanvallen bleef grotendeels beperkt. Sommige websites waren een tijdlang niet bereikbaar.

De groepering, actief sinds 2022, voerde in het verleden al enkele cyberaanvallen uit tegen Belgische websites. In januari 2024 werden onder andere websites gelinkt aan de Kanselarij, de Kamer van Volksvertegenwoordigers, de Senaat,... gevisieerd. De groepering is internationaal actief, en voerde reeds DDoS-aanvallen uit tegen websites van overheidsagentschappen, mediabedrijven, kritieke infrastructuur en private ondernemingen in diverse Europese landen maar ook daarbuiten (VS, VK).

Bij zulke incidenten staat de VSSE in voortdurend contact met partnerdiensten die de 'lead' hebben in de strijd tegen cyberaanvallen zoals het Centrum voor Cybersecurity België (CCB) voor de technische analyse en de Algemene Dienst Inlichting en Veiligheid (ADIV) van de Krijgsmacht voor de operationele werking. De VSSE poogt om in cyberonderzoeken het aspect *counter intelligence* te belichten. Op die manier wil de VSSE meer informatie verzamelen over waar statelijke en niet-statale hackers specifiek naar op zoek gaan, welke informatie gecompromiteerd werd en welke conclusies ze daar dient uit te trekken over de bedoelingen van onze tegenstanders.

## DE VSSE STRIJDT TEGEN HET OMZEILEN VAN DE SANCTIES TEGEN RUSLAND

Onder de wereldwijde geopolitieke en veiligheidsuitdagingen vormen programma's voor nucleaire, biologische, chemische en radiologische massavernietigingswapens en hun overbrengingsmiddelen een cruciale uitdaging voor de veiligheid van ons land en van onze bondgenoten. Voorkomen dat bepaalde statelijke actoren goederen en technologieën verwerven die onder sanctieregimes vallen, is op die manier ook één van de opdrachten van de VSSE.

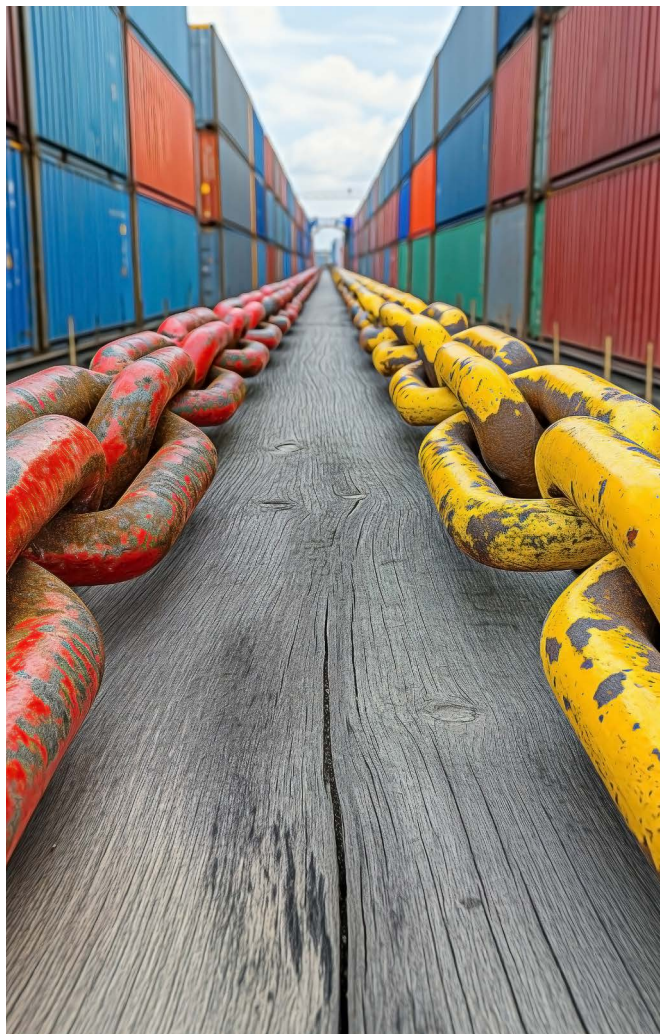
De VSSE steunt de internationaal opgelegde strategie met twee duidelijk omschreven doelstellingen: de capaciteiten tegengaan van het Russische militair-industrieel complex dat de inval in Oekraïne steunt, en Rusland zware structurele gevolgen opleggen voor de acties tegen zijn Oekraïense buur.

De evolutie van de oorlog in Oekraïne en de verschillende sanctiepakketten tegen Rusland dwingen het land om zich aan te passen en nieuwe kanalen te vinden om de nodige goederen voor onconventionele en zeer geavanceerde wapenprogramma's te verkrijgen. Het gaat vaak om zogenaamde goederen voor tweërlei gebruik: goederen die zowel civiel als militair aangewend kunnen worden. Behalve hoogtechnologische componenten kan het ook gaan om relatief rudimentaire goederen, die eveneens kunnen worden gebruikt voor het productieproces van bepaalde wapens.

Concreet proberen Russische bedrijven, vaak aangestuurd door de staat en zijn inlichtingendiensten, op deze manier in of via België goederen en technologieën te verwerven die nuttig zijn voor de Russische oorlogsinspanningen. Dat kan onder meer gebeuren via de hulp van bedrijven in derde landen in Azië, het Midden-Oosten, Europa of Afrika.

De VSSE draagt actief bij aan de toepassing van de internationale sancties tegen Rusland. Onder meer door samen met de nationale en internationale partners te detecteren hoe de sancties worden omzeild en dit te belemmeren.

Bovendien zet de VSSE zich samen met hen volop in om te voorkomen dat andere actoren de materia-



len, technologieën, knowhow en kennis verwerven die nodig zijn voor de ontwikkeling van programma's voor massavernietigingswapens en hun overbrengingsmiddelen, zoals raketten en drones. Het gaat met name om staten als Iran en Noord-Korea, die het voorwerp uitmaken van internationale sancties.



# DE VSSE WERKTE MEE AAN ONDERZOEK NAAR RUSSISCHE INMENGING IN EUROPEES PARLEMENT

De VSSE is alert voor clandestiene buitenlandse inmenging in de besluitvorming in België, maar speelt die rol ook als inlichtingen- en veiligheidsdienst van de *host nation* van Europese en internationale instellingen zoals de EU en de NAVO. In die context hielp de VSSE het afgelopen jaar mee aan het onderzoek naar een pro-Russisch inmengingsnetwerk rond het medium *Voice of Europe*.



In het kader van haar opdracht om inmengingsactiviteiten in en rond het Europees Parlement te helpen voorkomen, voerde de VSSE, in nauwe samenwerking met verschillende Europese partnerdiensten, een onderzoek naar een pro-Russisch inmengingsnetwerk dat, via een aantal tussenpersonen, aangestuurd en gefinancierd werd door een pro-Russische Oekraïense oligarch en media-magnaat.

Zulke inmengingsnetwerken trachten 'bevriende' parlementsleden voor zich te winnen – al dan niet met behulp van financiële vergoedingen. Daarnaast streven ze er naar om de aanwezigheid van pro-Russische parlementsleden in het Europees Parlement te vergroten en om hun activiteiten beter te coördineren en te organiseren, waarbij ook parlementaire assistenten worden ingezet.

Dit inmengingsnetwerk werd ondersteund door een eigen media-organisatie *Voice of Europe*, die werd geleid door een stroman in Tsjechië.

Enkele Europese diensten (inclusief de VSSE) werkten intensief samen om dit netwerk bloot te leggen. In maart 2024 beslisten de Tsjechische autoriteiten

om de oligarch, zijn stroman in Tsjechië en *Voice of Europe* omwille van hun inmengingsactiviteiten op een sanctielijst te plaatsen.

## ► EEN DUNNE GRENS

Op zich is het niet ongewoon dat individuen, groepen, organisaties en staten hun belangen proberen verdedigen via diplomatie, economische vertegenwoordiging, pr-campagnes, culturele verenigingen enz. Dit maakt deel uit van het normale politieke en diplomatieke spel. Om terug te keren naar het voorbeeld van *Voice of Europe*: Rusland beschikt nog steeds over een omvangrijke diplomatieke vertegenwoordiging bij de EU en in België, en heeft, vanuit dit opzicht, het netwerk rond de Oekraïense mediamagnaat niet nodig om op een legitieme manier zijn belangen te verdedigen.

Het cruciale onderscheid met lobbying of diplomatie zit net in het feit dat het bij inmenging om 'bedrieglijke, ongeoorloofde of clandestiene middelen' gaat.

# SPIONAGE EN INMENGING IN HET STRAFWETBOEK

Sinds april 2024 beschikt België over nieuwe middelen in de strijd tegen spionage en buitenlandse inmenging. Tot dat moment konden activiteiten van spionage en inmenging enkel bestraft worden wanneer ze plaatsvonden in een militaire of oorlogscontext. In realiteit waren inmenging en spionage dus nauwelijks strafbaar.

Betekent dit dat inmenging en spionage voor april 2024 straffeloos konden gebeuren? Neen, uiteraard niet. Er waren steeds administratieve maatregelen mogelijk, en het is ook zo dat inmenging en spionage vaak samengaan met andere feiten die wel strafbaar waren (bijvoorbeeld corruptie of bendevoorming).

In de wereld van vandaag was dat echter niet voldoende, vandaar dat de wetgever beslist heeft om de strafbaarstellingen rond inmenging en spionage die voorzien waren voor het nieuwe Strafwetboek van 2026 vervroegd in werking te laten treden. Hiermee neemt ons land zijn verantwoordelijkheid om spionage en inmenging op ons grondgebied, niet enkel tegen de Belgische belangen, maar ook tegen de internationale instellingen op ons grondgebied, effectief aan te pakken.

## ► STAATSGEHEIM

Deze nieuwe bepalingen maken het mogelijk om spionage te vervolgen, of het daarbij nu gaat om het overdragen, bekendmaken, reproduceren of ontvangen van een staatsgeheim. Dat is ook het geval voor poging tot spionage of de voorbereiding voor het overdragen van een staatsgeheim. Daartoe werd het begrip 'staatsgeheim' ook in de wet omschreven. Deze term slaat niet alleen op alle geclassificeerde informatie, maar ook op alle informatie die niet toegankelijk is voor het publiek en die van grote waarde is voor de bescherming van de Belgische belangen.

Ook kan iedereen die zich toelegt op actieve inmenging met de intentie de democratische beslissingsprocessen te beïnvloeden (het resultaat van verkiezingen, een stemming in het parlement, de gunning van een overheidsopdracht) voortaan







## ► DE VSSE EN DE ADIV WERKEN SAMEN IN THEMATISCHE HOUSES

In 2024 werd de samenwerking tussen de VSSE en de ADIV ook inzake contraspionage en buitenlandse inmenging naar een niveau hoger getild. Zo leggen de VSSE en de ADIV hun inlichtingen in deze materies sinds het voorjaar van 2024 op regelmatige basis samen binnen thematische *Houses* die zich concentreren op één bepaalde geografische regio of één bepaalde thematiek. Dit zorgt ervoor dat er geen dubbel werk wordt verricht en dat beide diensten hun onderzoeken beter op elkaar kunnen afstemmen.

worden vervolgd wanneer dit op clandestiene wijze gebeurt, dat is buiten het medeweten van de Belgische overheid en met als doel de nationale belangen ernstige schade te berokkenen.

### ► SAMENWERKINGSPLATFORM

Concreet komen de diensten die op deze thematieken werken samen in een platform waar zij dossiers bespreken. Voor elk zaak wordt een afweging gemaakt welke opvolgingsmethode de meeste kans op slagen heeft. Zijn er voldoende strafbare elementen die bewezen kunnen worden? Dan is strafrechtelijke vervolging een optie. Valt er uit dit dossier nog veel informatie te halen voor de inlichtingendiensten, of is het nog niet helemaal duidelijk? Dan is verder werken op inlichtingenniveau een betere optie. Dit systeem is geïnspireerd op de JIC/JDC-methode die voor terrorismezaken gebruikt wordt.

Deze afweging dient steeds met voldoende context en nuance te worden gemaakt. Een strafrechtelijke vervolging kan een groot afschrik-effect of signaaleffect hebben. Dit is in sommige dossiers het meest effectieve antwoord. In andere dossiers zijn er geen strafbare feiten gepleegd, en kunnen administratieve maatregelen aan de orde zijn.

### ► NIET BEPERKT TOT *USUAL SUSPECTS*

Het spreekt vanzelf dat de opname van spionage en inmenging in de nieuwe strafwet gevolgen heeft voor alle buitenlandse actoren die zich toeleggen op spionage of inmenging om op clandestiene wijze het democratische beslissingsproces te beïnvloeden. De VSSE stelt vast dat naast landen zoals Rusland en China ook verschillende andere landen aan spionage en inmenging doen in België. ■

## CHINA: EEN MOEILIJK EVENWICHT TUSSEN BELANGEN EN RISICO'S



Hoewel de – voornamelijk economische – relatie tussen China en België of China en Europa belangrijk is, gaan er van China verschillende dreigingen uit gericht tegen België en Europa: dreigingen op het vlak van cyber, spionage of inmenging, dreigingen die risico's inhouden voor ons wetenschappelijk of economisch potentieel, pogingen om de diaspora te controleren, enz. Het is de taak van de VSSE om die dreigingen op te sporen, de beleidsmakers hiervan op de hoogte te brengen en de verschillende Belgische actoren – zowel overheidsactoren als actoren uit de academische of economische wereld – bewust te maken van de risico's waaraan ze zijn blootgesteld. Op basis van die informatie moeten de beleidsmakers het juiste evenwicht vinden tussen enerzijds de economische belangen van België en anderzijds de veiligheidsrisico's.

China heeft zich in 2024 ten opzichte van Europa assertiever opgesteld dan voorheen, voornamelijk wat betreft het verdedigen van zijn politieke en economische belangen. Het land heeft zich in dit verband afgestemd op Rusland, met dat verschil dat China de handelsbetrekkingen met Europa, dat voor hen nog steeds een belangrijke economische partner is, wil behouden.

Deze assertieve houding blijkt onder meer uit hybride dreigingen gericht tegen België en Europa. En ongetwijfeld nog meer dan andere tegenstanders brengt China die dreigingen door middel van alle mogelijke actoren op subtiele wijze tot uiting, zowel op het diplomatieke, economische, sociale, of culturele vlak, als – uiteraard – op het vlak van inlichtingen. Dit is wat men de Chinese totaal-aanpak noemt. In die aanpak, waarbij het begrip nationale veiligheid onder Xi Jinping nog werd

verruimd, werd de rol van de inlichtingendiensten recent uitgebreid. De Chinese inlichtingendiensten – waaronder het MSS als de voornaamste burgerlijke inlichtingendienst – zijn in alle domeinen van de maatschappij aanwezig. Omdat hun capaciteit werd uitgebreid, is er meer druk om resultaten te behalen.

In het kader van deze aanpak wordt vaak een combinatie van legitieme en clandestiene activiteiten waargenomen. Wat inmenging betreft, zijn de doelstellingen van China enerzijds het samenbrengen en ondersteunen van groepen besluitvormers in Europa, die het besluitvormingsproces in het voordeel van China moeten proberen te beïnvloeden, en anderzijds het verdelen van westerse bondgenoten, met name door te proberen de trans-Atlantische of inter-Europese relaties te schaden.

Het algemene gedrag mag dan wel gewijzigd zijn, de VSSE heeft niet vastgesteld dat de modus operandi die de Chinese inlichtingendiensten in België gebruiken recent gewijzigd is. De rekrutering of zelfs de betaling van personen waarin ze geïnteresseerd zijn, gebeurt vaak in of vanuit China, zoals we hebben kunnen vaststellen in een dossier dat eind 2022 openbaar werd gemaakt. Dit systeem vermindert de risico's voor de Chinese inlichtingendiensten, omdat ze niet naar 'vijandige' landen hoeven te reizen.

De eerdergenoemde totaalaanpak waarbij elke Chinese actor, of het nu om een statelijke of niet-statale gaat, verplicht is om met de inlichtingendiensten samen te werken, alsook de modus operandi die subtiel en moeilijk op te sporen is, bemoeilijken het werk van onze dienst bij het opsporen van Chinese inlichtingendiensten. Dit maakt het des te belangrijker dat Belgische actoren bewust worden gemaakt van de dreiging, zodat onze veerkracht kan worden verbeterd en zodat iedereen de dreiging correct kan beoordelen.

## ► HET RISICO VAN CHINESE APPS

De Chinese apps die het afgelopen jaar meermaals onder de aandacht kwamen zijn een goed voorbeeld van hoe de Volksrepubliek te werk gaat. Door middel van een ogenschijnlijk onschuldige toepassing (online shoppen, grappige filmpjes) wordt een massa data over de gebruikers verzameld en opgeslagen. Is de schade direct zichtbaar voor de gebruikers? Neen, maar de gegevens kunnen wel gebruikt worden op langere termijn. De data kunnen bijvoorbeeld worden gebruikt om smartphones te infecteren, om desinformatie effectiever te verspreiden, om bepaalde discours te versterken of te onderdrukken, of om bepaalde tools te voeden die teren op grote hoeveelheden data zoals artificiële intelligentie. Conform het juridische kader in China zijn er geen obstakels voor de Chinese inlichtingendiensten om gebruik te maken van deze gegevens. Zij kunnen deze toepassen om personen of hun familieleden te viseren voor, bijvoorbeeld, spionage of inmengingsdoeleinden. Voorzichtigheid blijft dus geboden. Daarom is het aan te raden om op apparaten voor professioneel gebruik, of waarop gevoelige informatie staat, geen apps te installeren die niet noodzakelijk zijn.



# DE JIHADISTISCHE TERREURDREIGING IS EEN VEELKOPPIG MONSTER

De belangrijkste terreurdreiging in ons land gaat in 2024 nog steeds uit van jihadistische terreurbewegingen. Achter die vaststelling – die al jarenlang dezelfde is – gaan echter belangrijke evoluties en verschuivingen schuil.



## ► IS IN DE KHORASAN PROVINCIE

De voornaamste bron van de jihadistische terreurdreiging voor België blijft Islamitische Staat (IS) en in het bijzonder zijn Centraal-Aziatische franchise in de Khorasan Provincie (ISKP). Deze historische Khorasan Provincie is gelegen in de Centraal-Aziatische regio van Afghanistan, Pakistan, Iran, Tadzjikistan, Oezbekistan en Turkmenistan.

Voorals ISKP wist zich het voorbije jaar – zoals enigszins gevreesd – te profileren als een organisatie die in staat is om complexere terroristische operaties uit te voeren, zowel binnen als buiten de eigen regio. De aanslag door ISKP op de rouwstoet van de leider van de Iraanse Revolutionaire Garde op 3 januari 2024 in het Iraanse Kerman met 96 dodelijke slachtoffers als gevolg was een eerste teken aan de wand. Later die maand volgde een kleinschaligere aanslag in Turkije, met twee dodelijke slachtoffers. Op 22 maart 2024 was het de beurt

aan Rusland met de aanslag op het Crocus theater waarbij 145 dodelijke slachtoffers vielen. Het werd meteen een van de bloederigste aanslagen sinds de aanslagen in Parijs op 13 november 2015.

ISKP heeft zich daarmee op de kaart gezet als de meest dynamische tak van het hele netwerk rond IS. Hoewel ISKP geen eigen territorium controleert in Pakistan en Afghanistan heeft de organisatie zich met haar acties op Russische, Turkse en Iraanse bodem een imago aangemeten waarmee ze nieuwe financiële middelen en sympathisanten blijft aantrekken.

Hoewel ISKP het voorbije jaar zijn wil en capaciteit heeft aangetoond om operaties uit te voeren met centraal aangestuurde cellen, blijven ISKP en IS in het algemeen ook via online propaganda voortdurende inspiratiebronnen voor *lone ac-*

tors. Met hun gewelddadige propaganda zetten ze mensen aan tot gewelddadige acties, die achteraf worden opgeëist. Ook in West-Europa werden het afgelopen jaar terreurplannen van mensen die sympathiseerden met ISKP vrijdeld, zoals in Oostenrijk. In België waren er onder meer huiszoekingen en arrestaties in het milieu van ISKP-aanhangers aan de vooravond van de opening van de Olympische Spelen in Parijs in juli 2024.

### ► IS IN SYRIË EN IRAK

Ondanks het verlies van het fysieke kalifaat in Syrië en Irak in 2019, verblijven er op verschillende plaatsen in de regio nog zogenaamde *Foreign Terrorist Fighters* (FTF). Een aantal van hen heeft ook linken met ons land: ze beschikken over de Belgische nationaliteit of zijn bijvoorbeeld vanuit België vertrokken om deel te nemen aan de jihad. In veruit de meeste gevallen zijn ze destijds vertrokken om de rangen van IS te vervoegen, ook al belandden veel 'Belgische' FTF uiteindelijk bij een waaier aan uiteenlopende jihadistische groeperingen.

De plotse implosie van het regime van Bashar al-Assad op 8 december 2024 in Syrië, na de onverwacht snelle opmars van de rebellen van Hayat Tahrir al-Sham (HTS), kunnen de komende weken en maanden ook gevolgen hebben voor de veiligheidssituatie in België.

Volgens de informatie waar de VSSE eind 2024 over beschikte, zouden er 13 aan België gelinkte mannelijke FTF verblijven in gevangnissen in het noordoosten van Syrië dat onder controle staat van Koerdische strijders. In de kampen al-Hol en al-Roj in dezelfde regio zouden nog eens 8 vrouwelijke FTF en 9 kinderen verblijven. Nog eens 24 strijders

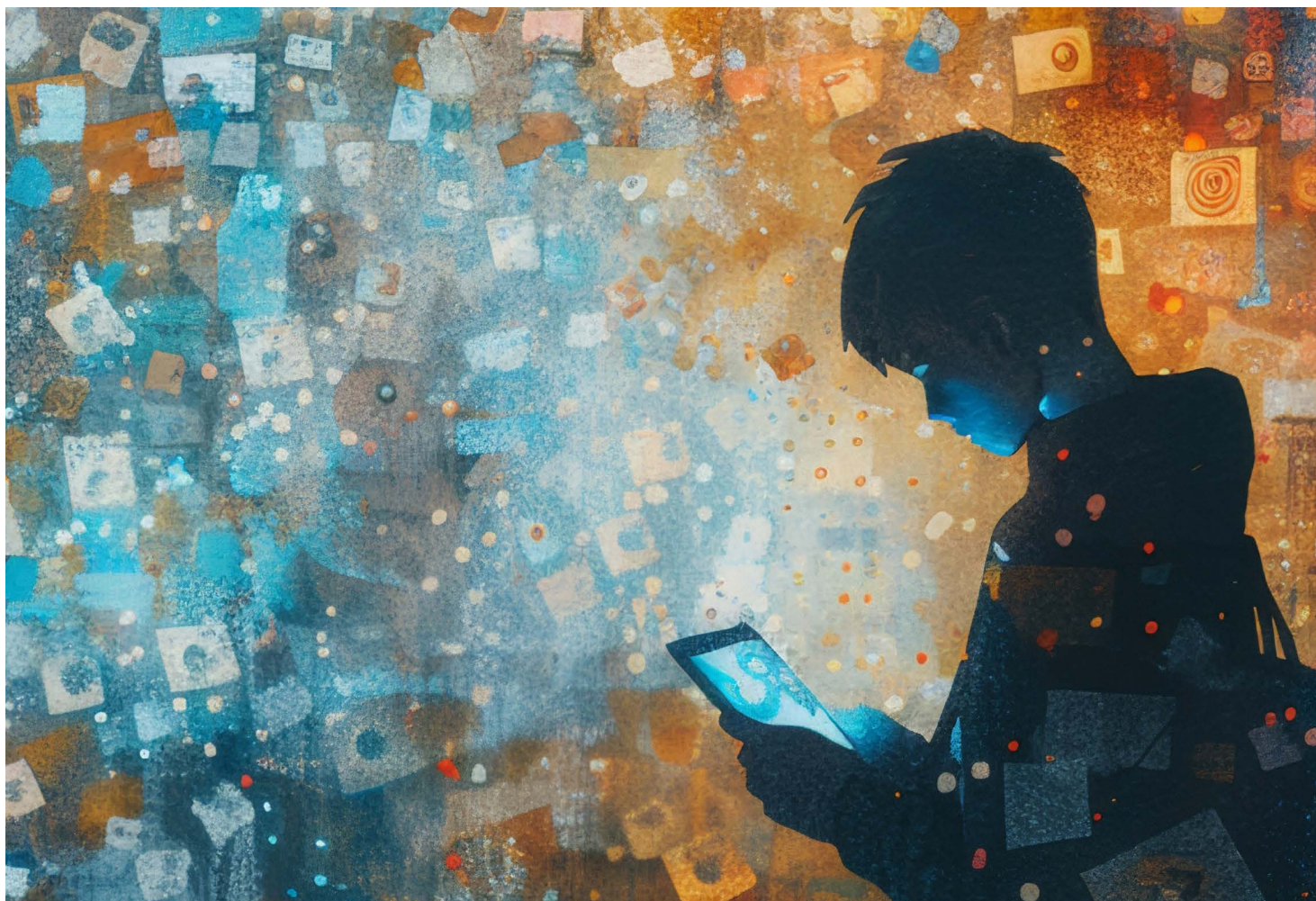
met banden met België en 48 kinderen zouden verblijven in het Noordwesten van Syrië. Onder hen een handvol FTF die de rebellenbeweging HTS zouden steunen of er deel van zouden uitmaken. Het spreekt voor zich dat de VSSE zeer aandachtig is voor het wedervaren van deze FTF. Indien ze door de snel wijzigende situatie de mogelijkheid zouden krijgen om ongemerkt en ongecontroleerd terug te keren, kan dat een impact hebben op de veiligheidssituatie in België.

Eind 2024 leek het er niet op dat IS een significante rol zou opnemen in het Syrische strijdtoneel, ook al kan de organisatie nog op heel wat sympathisanten rekenen in de bredere regio en is een heropleving van IS niet helemaal uit te sluiten.

### ► IS IN DE SAHEL EN SOMALIË

Op het Afrikaanse continent en met name in de Sahelregio en de Hoorn van Afrika neemt de slagkracht van terroristische organisaties toe. Zowel aan IS als aan Al Qaeda gelieerde groepen controleren in die gebieden een belangrijk territorium. Dit maakt dat deze groeperingen zich in deze regio kunnen hergroeperen en hun capaciteit kunnen opbouwen. Een recent voorbeeld van deze capaciteit is de gecoördineerde aanslag die IS in Somalië pleegde op 31 december 2024. Vooralsnog beschikt de VSSE niet over indicaties dat de regionale situatie een directe impact heeft op het dreigingsbeeld in België. Via haar binnen- en buitenlandse partners volgt de VSSE de situatie op. ■

## BIJNA ÉÉN OP DRIE BETROKKENEN IN TERRORISMEDOSSIERS VAN DE VSSE IS MINDERJARIG



Tussen 2022 en 2024 was bijna één op de drie personen die broedden op gewelddadige acties in België jonger dan 18 jaar. Het online radicaliseringsproces van deze jongeren verloopt razendsnel. Deze dreigingen tijdig detecteren en aanpakken is een hele uitdaging voor de VSSE en haar partners.

De Belgische inlichtingen- en veiligheidsdiensten worden in toenemende mate geconfronteerd met de aanwezigheid van minderjarigen in dreigingsdossiers. De vaststelling is niet nieuw, maar het fenomeen lijkt te escaleren.

In de terrorismedossiers van de VSSE van de jongste drie jaren (2022 tot en met 2024) blijkt net iets minder dan een derde van de personen die plannen maakten om geweldsdaden te plegen minderjarig. De jongste verdachte die in 2024 werd aangehouden was 13 jaar. De mediaanleeftijd schommelt rond de 16 jaar. De minderjarigen die rondliepen met plannen voor gewelddadige acties waren allemaal jongens.

### ► 3 OP 4 GEDREVEN DOOR RADICALE ISLAM

In zowat drie op de vier gevallen werden deze minderjarigen gedreven door een radicale versie van de soennitische islam. Een kwart van de minderjarigen had eerder een rechts-extremistische motivatie of handelde uit haat tegen het establishment.

Het radicaliseringsproces van die minderjarigen vindt online plaats en gaat vaak bijzonder snel. In deze hedendaagse hypergeconnecteerde samenleving staan er immers slechts enkele muisklikken tussen extremistisch en terroristisch propagandamateriaal en deze jongeren die op zoek zijn naar een identiteit of een doel in hun leven. Naast het consumeren van dergelijk propagandamateriaal stelt de VSSE vast dat in sommige dossiers minderjarigen zelf overgaan tot het produceren en het verspreiden van propagandamateriaal.

Sociale druk blijkt een belangrijke factor in de radicalisering van minderjarigen. De VSSE stelt vast dat radicaliserende minderjarigen vaak deel uitmaakten van een (online) netwerk of groep van gelijkgezinden. Binnen die netwerken treedt er regelmatig een versterkende trend op waarbij jongeren elkaar aansporen om steeds meer en steeds extremere content te consumeren. Het doorbreken van die trend zonder het doorknippen van de sociale banden met de andere leden van de groep blijkt zeer moeilijk.

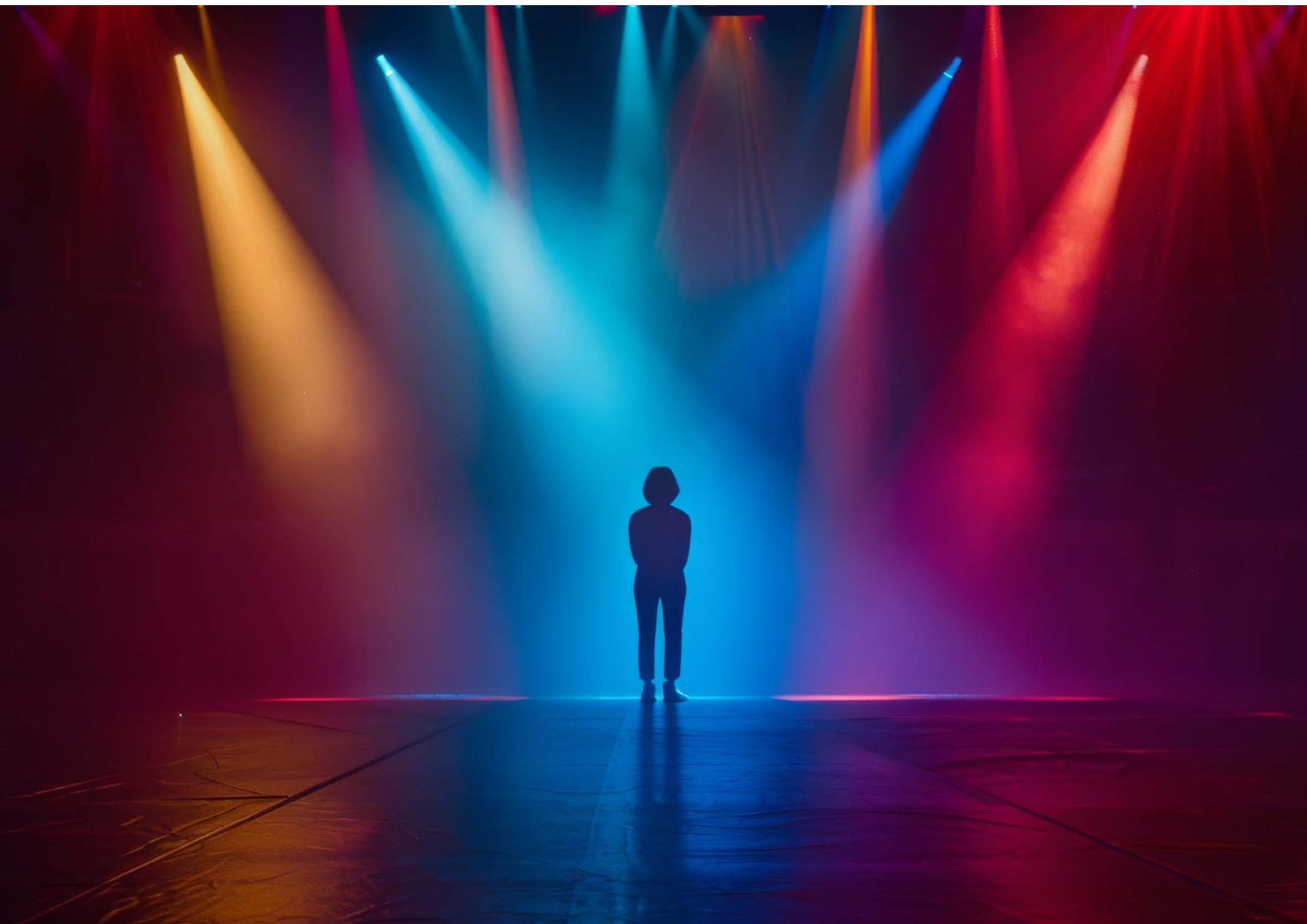
De snelheid van het radicaliseringsproces heeft als gevolg dat de intentie om over te gaan tot het plegen van een terroristische actie vaak weinig ideologisch onderbouwd is. Het ontbreken van een ontwikkeld ideologisch kader heeft echter geen negatieve impact op de motivatie van de betrokken personen. De VSSE stelt vast dat er in vele gevallen sprake is van een verheerlijking van geweld. Die fascinatie voor geweld en gewelddadige onderwerpen vormt vaak de aanleiding voor de introductie van personen in problematische (online) groepen. Na enige tijd wordt geweld gepercipieerd als de enige manier om hun extremistische doelstellingen te bereiken.

Minderjarigen hebben door hun afhankelijkheid, ouderlijke controle en gebrek aan toegangen gelukkig doorgaans veel meer moeite dan volwassenen met het bekomen van middelen voor de uitvoering van hun plannen. Dat weerhoudt terroristische organisaties er echter niet van om deze beïnvloedbare jongeren aan te zetten tot het plegen van gewelddadige acties.

Voor inlichtingen- en veiligheidsdiensten is het dan ook een uitdaging om dergelijke dreigingen tijdig te detecteren. De minderjarigen in kwestie zijn immers doorgaans een onbeschreven blad voor ze in het vizier van een inlichtingendienst komen. Uitmaken van welke jongeren er een reële dreiging uitgaat en wie slechts stoere praat verkoopt achter zijn klavier blijft voor een inlichtingendienst een zeer moeilijke en tijdrovende beoordeling.

Naast de VSSE en andere veiligheidsactoren spelen in deze problematiek ook sociopreventieve partners een belangrijke rol zoals de Lokale Integrale Veiligheidscellen (LIVC) en de gemeenschappen. ■

## EXTREMISTISCHE PROPAGANDA SPOORT LONE ACTORS AAN TOT TERREUR



**Extremistische propaganda is een belangrijke katalysator die *lone actors* aanzet tot gewelddadige acties. Zo blijft de Islamitische Staat (IS) ondanks het verlies van het kalifaat de belangrijkste inspiratiebron voor aanslagplannen in België dankzij zijn online propagandamachine. Uit een analyse van de VSSE blijkt dat extremistische propaganda vaak in enorme hoeveelheden wordt aangetroffen op in beslag genomen telefoons van jihadi's in België.**

Het soennitische jihadisme blijft in omvang veruit de grootste dreiging voor gewelddadige terreur in België. Die dreiging kan van buitenaf komen, maar evengoed van binnen de landsgrenzen. In beide gevallen speelt extremistische propaganda vaak een cruciale rol als katalysator.

Dat blijkt uit een onderzoek van de VSSE naar een vijftigtal in beslag genomen telefoons en andere elektronica van individuen in jihadistische terrorismezaken. In 72 procent van die elektronische dragers werden enorme hoeveelheden IS-propaganda

gevonden. In mindere mate werd er ook propaganda gelinkt aan Al Qaeda teruggevonden.

Zowel Islamitische Staat als Al Qaeda beschikken anno 2024 nog steeds over een robuust en uitgebreid propaganda-apparaat. Het einde van het fysieke kalifaat belette niet dat IS er nog steeds in slaagt om de mobiliserende kracht van zijn ideologie uit te spelen. In die zin blijft IS als een 'online' kalifaat bestaan. Het zorgt ervoor dat IS nog steeds de belangrijkste inspiratiebron blijft voor aanslagplannen in ons land en elders in het Westen, zoals



op nieuwjaarsdag bleek uit de aanslag in New Orleans in de Verenigde Staten.

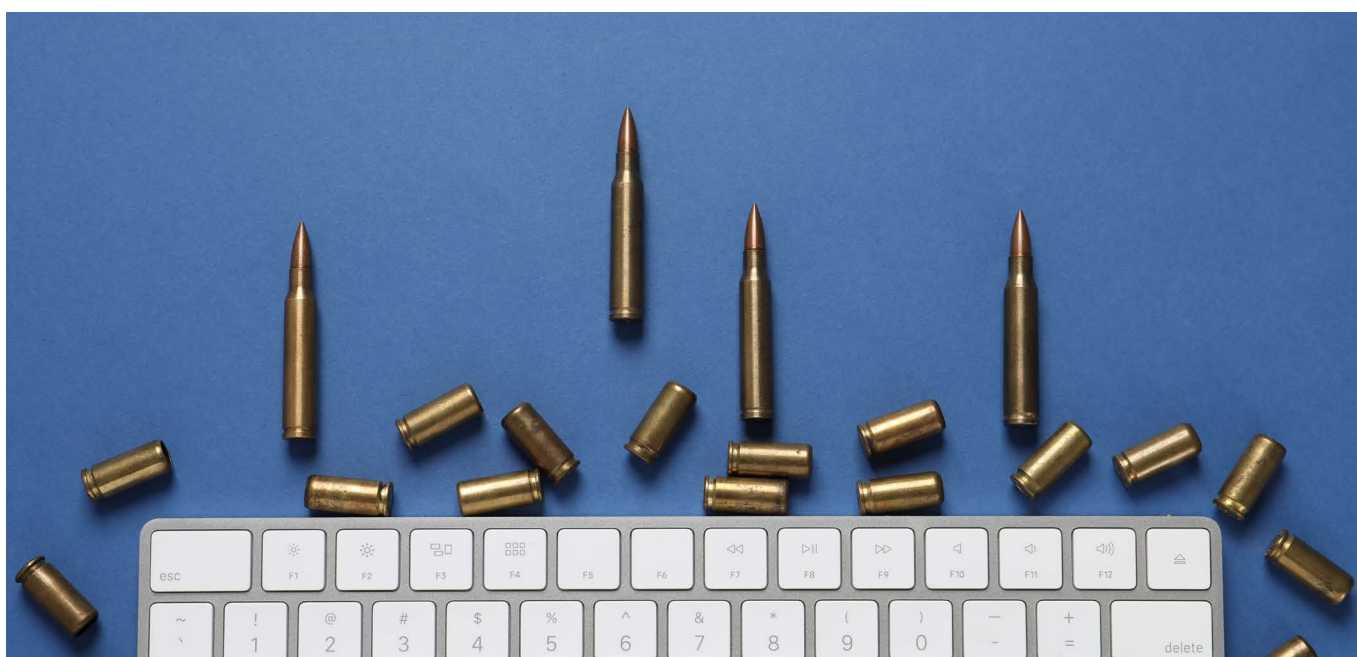
Ook Al Qaeda blijft nog steeds actief op het internet en op sociale media met een propagandanetwerk dat nog steeds uitbreidt. Zowel IS als Al Qaeda zijn erg bedreven in de recyclage en het hermonteren van oud propagandamateriaal, maar tot op de dag van vandaag wordt ook nieuw propagandamateriaal geproduceerd. Zowel IS als Al Qaeda beroepen zich op officiële en onofficiële mediakanalen om hun propaganda te verspreiden. Zo hebben ze beiden, elk op hun eigen manier, een online ecosysteem opgebouwd dat ook in 2024 wereldwijd bezoekers trekt. Inhoudelijk kiest Al Qaeda voor een doorgedreven ideologisch verhaal, terwijl IS doorgaans gewelddadige en choquerende beelden verkiest.

Met hun propaganda willen terroristische groeperingen zoals IS en Al Qaeda diverse doelstellingen nastreven. Zo gebruiken ze dit materiaal onder andere om hun ideologie te verspreiden, individuen te radicaliseren en te rekruteren, om fondsen te werven, maar vooral ook om jongeren te inspireren en aan te zetten tot het plegen van terroristische aanslagen.

## ► ALGORITMES

Een bijkomend probleem is dat de algoritmes van de belangrijkste openbare sociale mediakanalen zoals YouTube, TikTok of Facebook een aanzuigefect creëren door mensen die online opzoeken verrichten naar radicale onderwerpen steeds sneller en steeds meer extremere filmpjes of andere inhoud aan te bieden. Via die methoden bevinden personen zich soms, zonder het goed en wel te beseffen, in een digitale *rabbit hole* waaruit ontsnappen zeer moeilijk blijkt.

Een andere problematische tendens is het fenomeen waarbij veelal jonge gebruikers via bepaalde interessegebieden richting chatgroepen of kanalen op bijvoorbeeld Telegram worden geleid, waar een meer specifiek extremistisch narratief wordt gedeeld. In de meest zorgwekkende gevallen worden in deze private chatgroepen zeer expliciet gewelddadig propagandamateriaal en terroristische handleidingen gedeeld.



# DE CONFLICTEN IN HET MIDDEN-OOSTEN EN HUN IMPACT OP BELGIË



In 2024 escaleerde de oorlog tussen Israël en Hamas in Gaza en flakkerde het conflict tussen Israël en Hezbollah in Libanon weer op. De daaropvolgende val van het regime van de Syrische dictator Bashar al-Assad zet de deur open voor belangrijke verschuivingen in de regio met mogelijke implicaties voor ons land.

## ► SYRIË

De onverwacht snelle implosie van het regime van Bashar al-Assad op 8 december 2024 in Syrië na de succesvolle opmars van de rebellen van Hayat Tahrir al-Sham (HTS) kan de komende maanden leiden tot snel evoluerende situaties in de brede regio. Dit kan gevolgen hebben voor het lot van de aan België gelinkte *Foreign Terrorist Fighters* (FTF) in gevangnissen en kampen in het noordoosten van Syrië, maar het kan ook een impact hebben op de territoriale aspiraties van verschillende jihadistische groeperingen in Syrië. Een heropleving van IS valt niet helemaal uit te sluiten. Samen met haar netwerk van internationale partners en de ADIV volgt de VSSE de situatie op de voet op.

## ► GAZA EN LIBANON

De escalatie van het conflict tussen Israël en Hamas in Gaza en de Westelijke Jordaanoever en de opnieuw opgeflakkerde oorlog tussen Israël en Hezbollah in Libanon beïnvloeden ook de Europese en de Belgische samenleving. De gebeurtenissen in het Midden-Oosten fungeren als voedingsbodem voor radicalisering. Dit heeft al geleid tot gewelddadige acties in verschillende Europese landen, zoals de rellen tussen Israëlische voetbalsupporters en pro-Palestijnse jongeren in de straten van Amsterdam op 7 november 2024. Enkele dagen later werden ook in Antwerpen een handvol jongeren gearresteerd die geweld wilden plegen tegen de Joodse gemeenschap. In Zweden en Denemarken

werden schoten afgevuurd of handgranaten geworpen naar de Israëlische ambassade.

Terroristische organisaties zoals IS en Al Qaeda gebruiken het conflict in het Midden-Oosten in propagandamateriaal om hun jihadistische boodschap kracht bij te zetten en mensen te rekruteren. Dat kan ook in België mensen inspireren tot gewelddadige acties.

## ► HAMAS EN HEZBOLLAH

Hoewel Hamas prijkt op een Europese terreurlijst, acht de VSSE een aanslag door Hamas in België onwaarschijnlijk. Als er al geweld te verwachten is, zal dit eerder komen van geradicaliseerde *lone actors* die gemotiveerd worden door het conflict in Gaza.

Hamas is weliswaar ook in België actief, zij het voornamelijk om te lobbyen bij Belgische en internationale instellingen en om financiering voor de beweging te zoeken. Het zijn activiteiten zonder directe geweldsdreiging, maar die niettemin problematisch en soms zelfs strafbaar zijn als het gaat om de financiering van een terroristische organisatie.

Ook van de Libanese beweging Hezbollah gaat er geen directe terreurdreiging uit voor België. Hezbollah is in België vooral actief binnen de Libanese diaspora en tracht in België fondsen te werven. Het zijn activiteiten die de VSSE in samenwerking met haar nationale en internationale partners opvolgt.

# DE DREIGING VAN RELIGIEUS EN IDEOLOGISCH EXTREMISME

Niet alleen terrorisme, maar ook extremisme vormt een bedreiging voor onze democratische samenleving. Vormen van zowel religieus als ideologisch extremisme kunnen in bepaalde gevallen leiden tot verdere radicalisering en uiteindelijk tot geweld.



## ► MOSLIMBROEDERS

De Moslimbroeders zijn een heterogene beweging waarvan in België geen gewelddreiging uitgaat. Wel stelt de VSSE vast dat er binnen de aanhangers van het Moslimbroederschap in België een honderdtal personen actief proberen om een ideologie te verspreiden die kan leiden tot radicalisering en die extremisme kan bevorderen.

De Moslimbroeders onderscheiden zich van andere islamitische extremistische bewegingen door hun lobbyactiviteiten gericht op beïnvloeding van het overheidsbeleid met betrekking tot de islam, en door hun methodologie die gebaseerd is op de oprichting van organisaties om de moslimgemeenschap in de hand te houden.

Op een clandestiene manier proberen groeperingen in de invloedssfeer van de Moslimbroeders

te lobbyen voor een belangrijkere plaats voor de islam in de samenleving. Ze trachten daarbij hun banden met de Moslimbroeders te verhullen en meten zich het imago aan van legitieme vertegenwoordigers van de moslimgemeenschap in ons land. Op die manier willen ze een plaats veroveren in de Belgische instellingen en financiering voor hun initiatieven bekomen.

Het langetermijndoel van de Moslimbroeders is het creëren van een samenleving waarin elk aspect van het leven wordt beheerst door de religieuze norm; op de middellange en korte termijn draagt hun discours bij aan het creëren van een klimaat van segregatie en polarisatie. Een dergelijk klimaat vormt op zijn beurt een vruchtbare voedingsbodem voor radicalisering.

Ook al is de buitenlandse steun die de Moslimbroeders in België ontvangen afgenomen, toch kan verwacht worden dat ze hun activiteiten hier verder zullen zetten.

### ► RECHTS-EXTREMISTISCHE *LONE ACTORS*

De voornaamste dreiging die op dit ogenblik uitgaat van het rechts-extremisme in België bestaat uit de verspreiding van rechts-extremistische propaganda. Op lange termijn kan dit mogelijk het vertrouwen in de democratische instellingen, processen en rechtsorde ondermijnen.

De kans op een terroristische aanslag gepleegd door rechts-extremistische groeperingen acht de VSSE eerder laag.

Mocht het toch tot een gewelddadige actie komen vanuit rechts-extremistische middens, dan valt deze vooral te verwachten uit de hoek van veelal erg jonge *lone actors* die doorgaans online radicaliseren. Sommigen onder hen worden geïnspireerd door de doctrine van het accelerationisme. Die doctrine gaat er vanuit dat een rassenstrijd of godsdienstoorlog op termijn onvermijdelijk is en dat de uitbraak van deze oorlog idealiter uitgelokt of versneld moet worden door terroristisch geweld. Rechts-extremistische accelerationisten geloven immers onwankelbaar dat het blanke ras uiteindelijk zal overwinnen omwille van haar vermeende superioriteit. Het aantal aanhangers van het accelerationisme is in België evenwel beperkt.

### ► INTENSE LINKS-EXTREMISTISCHE MOBILISATIE

Uit het verleden weten we dat links-extremistische groeperingen zich kunnen bezighouden met sabotage en *black block* tactieken. Het voorbije jaar werden echter voornamelijk bezetting van gebouwen, vandalisme en intimidatie vastgesteld, vaak in de context van hun toegenomen inzet en mobilisatie rond het conflict in Gaza. Maar ook de verkiezingen bleken een mobiliserend thema te zijn voor links-extremisten. Om hun aanhang te verbreden trachten ze in het algemeen meer thema's te bespelen die de actualiteit beheersen, zoals de klimaatproblematiek.

De acties van links-extremisten in België zijn op dit moment voornamelijk gefocust op het rekruteren, demonstreren en het verspreiden van hun boodschappen via online en offline propaganda. Toch zien sommigen binnen het links-extremistisch milieu geweld als een geoorloofd middel om hun doel te bereiken. Op basis van de beschikbare inlichtingen beschouwt de VSSE de voorbereiding en de planning van aanslagen vanuit dit milieu evenwel als onwaarschijnlijk. ■



# DE VSSE EN DE ADIV LEGGEN WEKELIJKS TERRORISMEDOSSIER VOOR AAN POLITIE EN PARKET



In de strijd tegen terrorisme en extremisme werken de VSSE en de ADIV al enkele jaren nauw samen in een gemeenschappelijk platform. Wekelijks legt dit platform dossiers rond terrorisme voor aan politie en parket. Beide diensten werden in 2024 aangesteld als 'technisch assistent' in 33 strafonderzoeken naar terrorisme.

Sinds de aanslagen van maart 2016 en de parlementaire onderzoekscommissie die daarop volgde maakte de hele inlichtingen- en veiligheids wereld de shift van *need to know* naar *need to share*. Daartoe werden de voorbije jaren platformen opgericht om informatie vlot te laten circuleren tussen de verschillende diensten die met inlichtingen en veiligheid bezig zijn, zoals de inlichtingendiensten, het OCAD, de politiediensten en het Openbaar Ministerie.

Waar politie en parket zich richten op het opsporen van strafbare feiten, het verzamelen van bewijslast en het vervolgen van personen, richten inlichtingendiensten zich op dreigingen en het verzamelen van inlichtingen vooraleer er sprake is van strafbare feiten. Deze verschillende finaliteiten zijn niettemin complementair en zorgen voor een voortdurende wisselwerking tussen de verschillende actoren.

## ► HET PLATFORM CECT: HET CENTRALE AANSPREEKPUNT VOOR TERRORISME EN EXTREMISME VAN DE VSSE EN DE ADIV

Al enkele jaren werken de medewerkers van de VSSE en de ADIV zij aan zij in de strijd tegen jihadistisch terrorisme binnen het zogenaamde Platform CT of Platform Contraterrorisme. Sinds 2024 werd die reeds bestaande samenwerking opgeschaald naar alle dossiers rond religieus en nu ook ideologisch geïnspireerd extremisme en terrorisme. Op die wijze vervelde het oude Platform CT in 2024 tot het nieuwe Platform CECT (Platform Contra-extremisme en Contraterrorisme).

Het Platform CECT vormt een *single point of contact* voor de nationale partners in deze materies. Vanuit dit platform verzenden de VSSE en de ADIV gezamenlijke analyses en inlichtingennota's naar binnen- en buitenlandse partnerdiensten. Zo spreken beide Belgische inlichtingendiensten inzake terrorisme en extremisme met één stem. Tegelijk kan het gemeenschappelijk Platform CECT gebruikmaken van de capaciteit en de collectiemiddelen die eigen zijn aan elk van beide zusterdiensten.



In de praktijk uit dit zich in het delen van inlichtingen met betrekking tot terrorisme en extremisme via gemeenschappelijke nota's van het Platform CECT aan de politie en het Openbaar Ministerie. Zo worden inlichtingen aangeleverd die aan de basis kunnen liggen van een strafonderzoek of die een onderzoek kunnen contextualiseren.

Wanneer er relevante nieuwe informatie met betrekking tot terrorisme beschikbaar is, meldt de betrokken dienst dat aan het zogenaamde *Joint Intelligence Center* (JIC). Dat bestaat uit leden van de Federale Gerechtelijke Politie, de Centrale Dienst Terrorisme van de Federale Politie, het OCAD en het Platform CECT. Deze diensten buigen zich vervolgens samen over de nieuwe informatie waarna er een gemeenschappelijke beoordeling volgt en een voorstel wordt geformuleerd voor een geschikte opvolging: ofwel een strafonderzoek ofwel een verderzetting van het inlichtingenonderzoek ofwel een andere opvolging. Deze beslissing moet vervolgens bekrachtigd worden door het *Joint Decision Center* (JDC). Dat bestaat uit dezelfde leden als het JIC aangevuld met leden van het lokaal parket, het Federaal Parket en de bestuurlijk directeur-coördinator van de Federale Politie.

### ► 50 TERRORISMEDOSSIERE

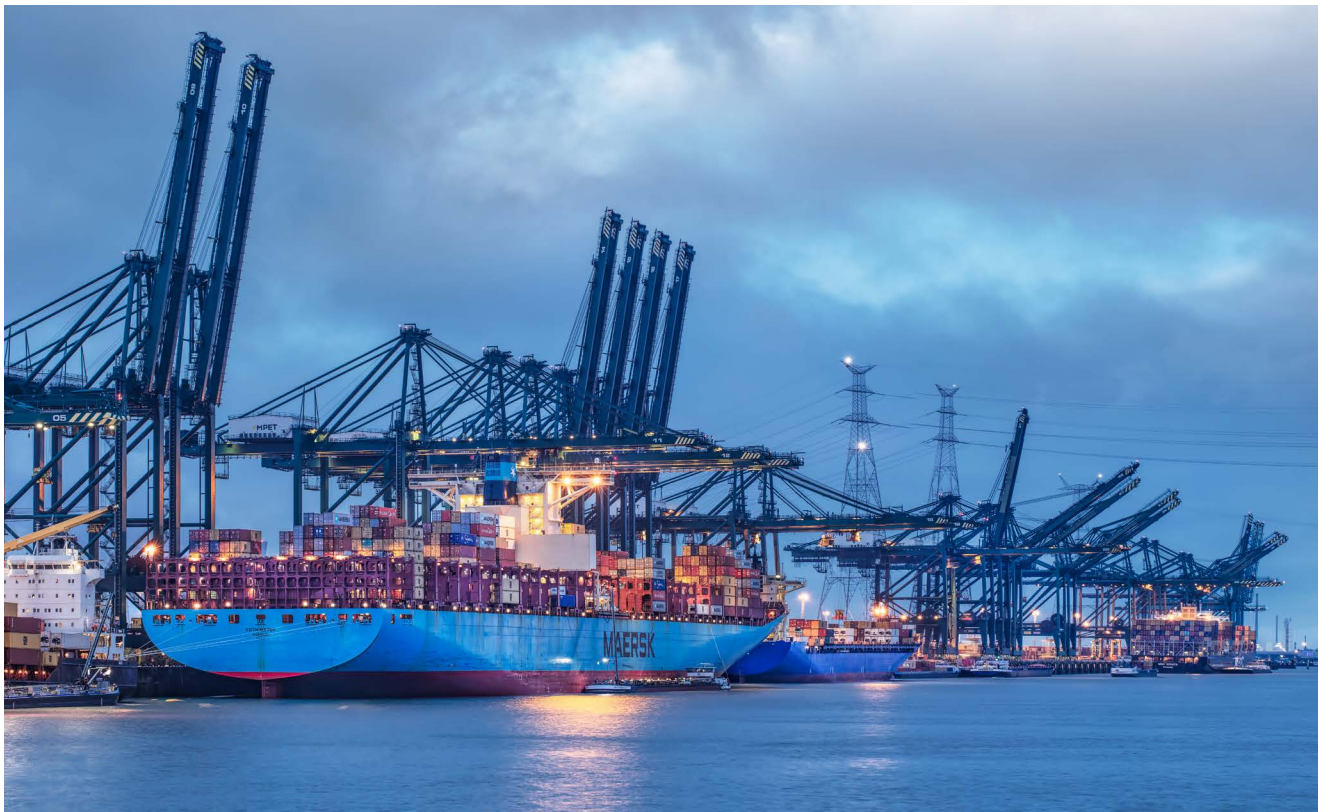
In 2024 heeft het Platform CECT 50 inlichtingendossiers met betrekking tot terrorisme aangemeld aan de verschillende JIC's. In totaal werden er het voorbije jaar 114 JIC's georganiseerd. Dat betekent dat een kleine helft van de terrorismedossiers die werden behandeld door een JIC werden aangebracht door de VSSE en de ADIV. De meeste andere dossiers werden aangemeld door de verschillende onderdelen van de Federale Politie. Dat het aandeel van de inlichtingendiensten hierin vrij hoog is, hoeft dan weer niet te verbazen: het is net de finaliteit van de inlichtingendiensten om dreigingen in een vroeg stadium te detecteren.

Van de 50 inlichtingendossiers rond terrorisme die het Platform CECT aanbracht in 2024, ging het in 22 gevallen om inlichtingen over een geweldsdreiging, in 28 gevallen handelden de dossiers eerder over propaganda voor terrorisme of de financiering van terrorisme. De 50 dossiers die het Platform CECT heeft voorgelegd hebben geleid tot de opening van 29 strafonderzoeken. In 15 gevallen bleef het bij inlichtingenonderzoeken.

Eens er een strafonderzoek loopt, kunnen de inlichtingendiensten aangeduid worden als technisch assistent. In elk terrorismedossier van het Federaal Parket wordt dit automatisch gedaan. Dit betekent dat de inlichtingendiensten toegang krijgen tot het gerechtelijk dossier en daarbij hun kennis en expertise in kunnen zetten ten voordele van het onderzoek. In 2024 werden de VSSE en de ADIV aangesteld als technisch assistent in 33 terrorismedossiers.

Wanneer een strafonderzoek afgerond is, stopt het werk van de verschillende diensten echter niet. Een gedegen opvolging is noodzakelijk via de verschillende overlegplatformen. Dat gebeurt ook onder meer op arrondissementeel niveau. Zo levert het Platform CECT voortdurend input aan de verschillende zogenaamde *Local Task Forces* in het kader van de Strategie TER – de gemeenschappelijke strategie tegen terrorisme en extremisme. ■

# DE VSSE DRAAGT BIJ TOT DE STRIJD TEGEN DE GEORGANISEERDE CRIMINALITEIT



**De aanpak van de georganiseerde misdaad in België gebeurt in de eerste plaats vanuit een politieel en gerechtelijk perspectief, steeds vaker ook aangevuld met een administratieve aanpak op lokaal niveau. De VSSE treedt als inlichtingendienst aanvullend op in ondersteuning van nationale partnerdiensten.**

In de eerste plaats voert de VSSE onderzoek naar individuen en netwerken die staatsondermijnende activiteiten ontplooiën: geweld of corruptie gericht tegen overheidsambtenaren of kwetsbare sectoren zoals de kritieke infrastructuur van ons land. Relevante inlichtingen worden gedeeld met politie en gerecht via de gebruikelijke samenwerkingsprocedures.

In 2024 kwamen er signalen dat de strijd tegen de georganiseerde drugscriminaliteit zijn vruchten begint af te werpen. Omwille van het feit dat justitie successen boekte die leidden tot een groot aantal veroordelingen, kwam ook het gevangenisstelsel onder zware druk te staan. De VSSE zet haar specifieke expertise in de gevangenisomgeving in om zicht te krijgen op dreigingen die daar kunnen ontstaan. Samen met partnerdiensten zoals het gevangeniswezen probeert de VSSE ook dreigingen tegen het penitentiair personeel vanuit de georganiseerde misdaad te detecteren.

Samen met haar partners anticipeert de VSSE ook steeds op de uitlevering aan België van belangrijke kopstukken van de internationale drugsmaffia. Zo werden ook in de laatste maanden van 2024 een aantal zogenaamde High Value Targets (HVT's) opgepakt in het buitenland. De gerechtelijke autoriteiten vragen hun uitlevering in het kader van vervolging en strafuitvoering in ons land, maar hun eventuele uitlevering gaat gepaard met een aantal veiligheidsrisico's. Samen met de Federale Politie bekijkt de VSSE hoe deze risico's het best opgevangen kunnen worden, waarbij het voorkomen van de verderzetting van criminele activiteiten vanuit detentie prioritair is. Er wordt dan onder meer gekeken naar de geschikte gevangenis en aangepaste detentieregimes voor deze HVT's.

Ook in de Belgische havens heeft de VSSE haar aanwezigheid versterkt teneinde de actoren en de processen van de havens weerbaarder te maken tegen de ondermijnende aspecten van de georganiseerde misdaad.

# 02

**DE VSSE ALS VEILIGHEIDSDIENST**



## DE VSSE WERKT AAN EEN VERSTERKING VAN DE VEILIGHEIDSCULTUUR



**De VSSE steekt samen met de Nationale Veiligheidsoverheid (NVO) die sinds 1 januari 2024 deel uitmaakt van de VSSE, de handen uit de mouwen voor de versterking van de veiligheidscultuur, zowel binnen als buiten de eigen muren.**

Op nationaal vlak staat de VSSE daarvoor in voortdurend contact met een heel netwerk van veiligheidsofficieren, en dat zowel binnen overheidsdiensten als in privéondernemingen. Het is de NVO, samen met andere departementen van de VSSE, die de taak heeft om deze mensen bij te staan met adviezen, begeleiding en richtlijnen over verschillende aspecten van veiligheid. Op die manier dragen zij bij aan het versterken van een veiligheidscultuur in België:

- **Veiligheidsbeleid:** de VSSE ondersteunt de ontwikkeling van een robuust veiligheidsbeleid bij publieke en private organisaties om zo toe te laten risico's te beheren. De VSSE sensibiliseert ook voortdurend rond deze problematiek. Zo organiseerde de NVO in 2024 evenementen voor veiligheidsofficieren die door bijna 500 deelnemers uit de publieke en private sector werden bijgewoond.
- **Veiligheid van informatie:** de NVO zorgt voor de bescherming van gevoelige en wettelijk geclassificeerde informatie, treedt op bij veiligheidsincidenten en het opstellen van richtlijnen voor het beheer van dergelijke informatie.
- **Veiligheid van het personeel:** de NVO, samen met andere departementen van de VSSE, begeleidt haar partners bij het aanvragen van veiligheidsmachtigingen. Daarnaast voeren de VSSE en de ADIV veiligheidsonderzoeken uit om na te gaan of mensen die een veiligheidsmachtiging aanvragen voldoende

loyaal, integer en discreet zijn.

- **Fysieke en technologische veiligheid:** de NVO speelt een rol in de certificering van bepaalde informatie- en communicatiesystemen, gebouwen of gevoelige zones. Daarnaast adviseert de NVO haar partners over de bescherming van hun informatie, bijvoorbeeld wanneer ze reizen naar risicolanden.

Deze verschillende opdrachten, die zeker aan belang hebben gewonnen na de integratie van de NVO in de VSSE, zullen de komende jaren alleen maar in belang toenemen.

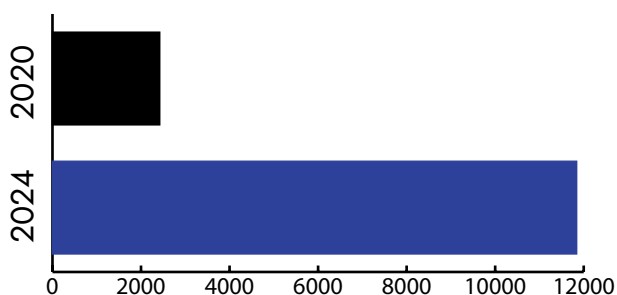
Voor het versterken van de veiligheidscultuur kijkt de VSSE daarnaast naar de eigen werking. De laatste jaren werd dan ook werk gemaakt van het aanscherpen van het veiligheidsbeleid binnen de eigen muren. Dat heeft zeker gevolgen gehad voor het eigen personeel, bijvoorbeeld voor wat het gebruik van persoonlijk elektronisch materiaal betreft, maar ook met betrekking tot de toegang tot geclassificeerde informatie op basis van het *need to know*-principe of als het over de noodzakelijke discretie gaat die medewerkers van een inlichtingendienst aan de dag moeten leggen, ook binnen de naaste familiekring.

De VSSE wil met haar veiligheidsbeleid op die manier een voorbeeld en inspiratie zijn voor andere spelers uit de publieke en private sector.

## DE NVO LEVERDE BIJNA 5 KEER MEER VEILIGHEIDSMACHTIGINGEN AF OP 5 JAAR TIJD

Sinds 1 januari 2024 maakt de Nationale Veiligheidsoverheid (NVO) deel uit van de VSSE. Met de integratie van de NVO streeft de VSSE ernaar de veiligheidscultuur in België gevoelig te verbeteren. In die context leverde de NVO in 2024 bijna 12.000 veiligheidsmachtigingen af, zowat vijf maal meer dan in 2020.

De VSSE is een inlichtingen- én veiligheidsdienst. Die pijler veiligheid werd de jongste jaren fors uitgebouwd, onder meer dankzij het onderbrengen van de NVO bij de VSSE. Die NVO maakte lang deel uit van de FOD Buitenlandse Zaken maar in februari 2022 besliste de Nationale Veiligheidsraad om de NVO te hervormen. Bij die hervorming werd beslist dat de bevoegdheid van de NVO met betrekking tot de veiligheidsverificaties werd overgedragen aan de Federale Politie. De NVO op zich, het personeel (een twintigtal personen) en de resterende bevoegdheden – waaronder dus het afleveren van de veiligheidsmachtigingen aan personen en ondernemingen die geclassificeerde informatie behandelen – werden ondergebracht bij de VSSE.

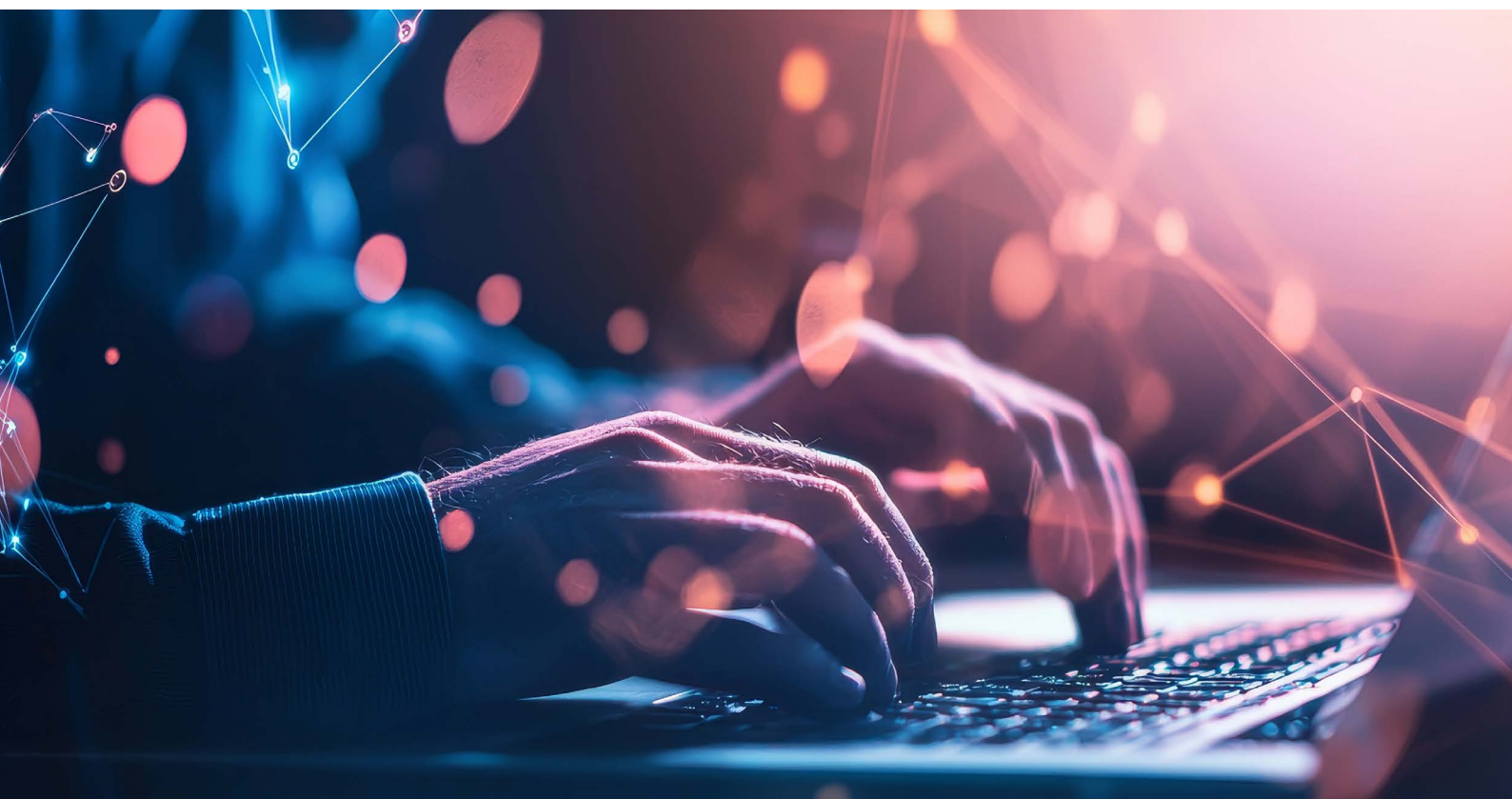


### ► 40 MEDEWERKERS

Sinds de NVO onder de vleugels van de VSSE opereert is de dienst gevoelig versterkt. Zo telt de NVO nu 40 medewerkers. Zij hebben het voorbije jaar hard gewerkt om de reactiviteit te verbeteren en het sterk verouderde wettelijk kader, de richtlijnen en procedures bij te werken.

In 2024 behandelde de NVO maar liefst 15.366 aanvragen voor individuele veiligheidsmachtigingen. Er werden er uiteindelijk 11.840 afgeleverd. Op twee jaar tijd is het aantal afgeleverde veiligheidsmachtigingen ruim verdubbeld. Ter vergelijking: vijf jaar eerder, in 2020, werden er slechts 2.428 individuele veiligheidsmachtigingen afgeleverd.

Daarnaast behandelde de NVO in 2024 nog eens 1.271 veiligheidsmachtigingen voor publieke en private rechtspersonen en werden daarbij het voorbije jaar 485 veiligheidsmachtigingen afgeleverd om geclassificeerde informatie te mogen behandelen.



## DE VSSE VERRICHTTE 36 PROCENT MEER VEILIGHEIDSVERIFICATIES IN 2024

In 2024 heeft de VSSE 327.608 veiligheidsverificaties verricht. Dat zijn er ongeveer 36 procent meer dan het jaar voordien. Omwille van het toegenomen veiligheidsbewustzijn ziet het ernaar uit dat het aantal verificaties in de nabije toekomst alleen maar verder zal toenemen.

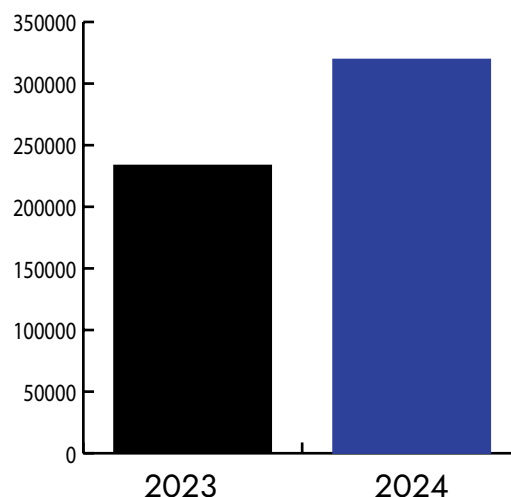
Veiligheidsverificaties zijn voorafgaande controles om mensen die een potentieel veiligheidsrisico zouden kunnen vormen, uit te sluiten van gevoelige functies of van toegang tot gevoelige zones. Voorbeelden zijn personen die werken in de beveiligde zone van de luchthaven of in de nucleaire sector. Al gebeuren zulke verificaties ook wanneer iemand de Belgische nationaliteit aanvraagt, bij asielaanvragen of vragen voor gezinshereniging.

De grote verscheidenheid aan veiligheidsverificaties maakt dat de VSSE dan ook door een waaier van partners wordt bevestigd om deze uit te voeren. De belangrijkste partner daarbij is echter de Federale Politie, die sinds 1 januari 2024 verantwoordelijk is voor het verwerken van verificaties op basis van de Classificatiewet van 1998.

Alles samen verrichtte de VSSE in 2024 welgeteld 327.608 verificaties. Dat zijn er ongeveer 36 procent meer dan de 241.197 verificaties in 2023.

Vanwaar die toch wel aanzienlijke groei van circa 36 procent? Voor luchthavenbadges wordt voortaan elk jaar een nieuwe verificatie verricht, in plaats van om de vijf jaar voordien. Het aantal aanvragen voor verificaties in het kader van procedures voor het verkrijgen van de Belgische nationaliteit zit in de lift en dat is eveneens het geval voor aanvragen voor verificaties in het kader van asielaanvragen of aanvragen voor gezinshereniging. Ook het aantal verificaties dat gebeurde in het kader van Europese topbijeenkomsten of NAVO-toppen blijft stijgen. Daarnaast gebeuren er ook veiligheidsverificaties in steeds meer nieuwe sectoren, zoals in het gevangeniswezen, de zeehavens,...

En gezien de geopolitieke toestand en een toenemend bewustzijn in onze maatschappij om op een verantwoorde manier met veiligheid om te gaan, verwacht de VSSE dat het aantal veiligheidsverificaties de komende jaren verder zal stijgen.



# DE VSSE FORMULEERDE 86 ADVIEZEN OVER BUITENLANDSE DIRECTE INVESTERINGEN

De screeningsprocedure voor *foreign direct investments* (FDI) wordt in België sinds 2023 toegepast. In 2024 beleefde de procedure zijn eerste volledige kalenderjaar. Tijdens deze periode stelde de VSSE adviezen op voor het Coördinatietoelcomité voor Inlichtingen en Veiligheid (CCIV), waarin de standpunten van elk van de betrokken partners werden samengebracht. Zo werden er in 2024 86 adviezen over veiligheids- en inlichtingenaspecten ingediend bij de Interfederale Screeningscommissie.



In een steeds complexer en onstabielere wordende geopolitieke context is het van essentieel belang dat België mechanismen ontwikkelt die een zekere veiligheid en economische autonomie helpen verzekeren, terwijl de openheid naar de buitenwereld behouden blijft.

Hoewel de overgrote meerderheid van de geverifieerde buitenlandse investeringen niet als een bedreiging werd beschouwd, vereisten bepaalde investeringen toch verdere verificaties zodat het CCIV met volledige kennis van zaken haar mening kon geven. Concreet gaat het om investeringen in een Belgische onderneming door personen of ondernemingen van buiten de Europese Unie. Daarbij worden alleen investeringen in bepaalde strategische sectoren gescreend, zoals de kritieke infrastructuur, spits technologie of leveranciers van Defensie. Ten slotte gebeurt er alleen een screening als minstens 10 tot 25 procent van de aandelen van de Belgische onderneming in buitenlandse handen komt.

## ► SCREENINGSPROCEDURE FDI

De belangrijkste taak bestaat erin de buitenlandse directe investeringen te analyseren en na te gaan of ze potentiële risico's inhouden voor de nationale veiligheid en de strategische belangen van het land.

In de praktijk werd in iets minder dan 10 procent van de dossiers een filterprocedure geopend. Dat is de zogenaamde tweede fase van de screening waarvoor de VSSE specifieke eigen capaciteit inzet voor het onderzoek naar de investering. Deze aanpak heeft de VSSE in staat gesteld een drijvende kracht te zijn in deze nieuwe nationale economische veiligheidsaanpak.

In totaal werden er in 2024 86 adviezen uitgebracht. Meer dan ooit is het essentieel om potentiële bedreigingen te identificeren en preventieve maatregelen te nemen om de veerkracht van gevoelige nationale sectoren, zoals kritieke infrastructuur, geavanceerde technologieën en energie, te helpen vergroten.



# 03

**OVER DE VSSE**

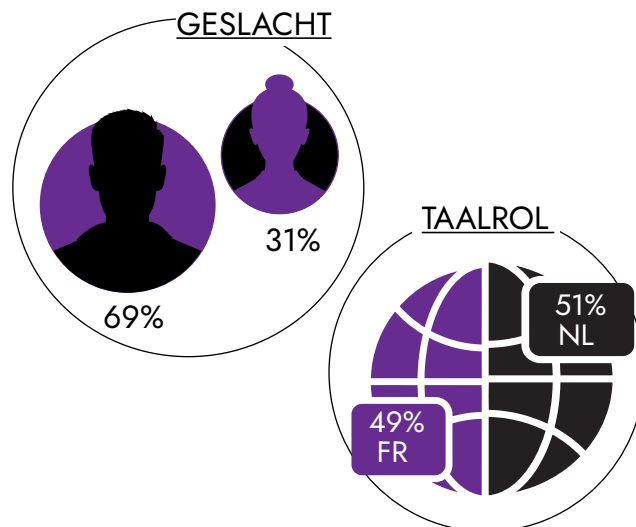
# DE VSSE IN CIJFERS IN 2024

## ► HUMAN RESSOURCES

# 954

### MEDEWERKERS

De voorbije jaren onderging de VSSE een fundamentele gedaantewisseling. In vier jaren tijd is het aantal medewerkers quasi verdubbeld. Honderden nieuwe collega's aantrekken, verwelkomen, een plek geven en intern opleiden was een echte *tour de force*.



## ► UITWISSELING VAN INLICHTINGEN

# 43.366

### INKOMENDE BERICHTEN

De inkomende berichten zijn afkomstig van binnenlandse partners zoals de ADIV, de Federale Politie, het OCAD, het Nationaal Crisiscentrum, de FOD Buitenlandse Zaken, het gevangeniswezen of de parketten. Daarnaast is een aanzienlijk deel van de inkomende informatiestroom afkomstig van buitenlandse inlichtingendiensten. Ter vergelijking: in 2020 ontving de VSSE 29.148 inkomende berichten.

# 1.492

### OVERLEG MET PARTNERS

De VSSE heeft in 2024 1.492 verslagen opge maakt van overlegmomenten waarop inlichtingen werden uitgewisseld met lokale, nationale en internationale partners.

## ► INTERNATIONALE RELATIES

### VERBINDINGSOFFICIEREN



In het buitenland



Bij multilaterale instellingen (NAVO/EU/Permanente Vertegenwoordiging bij de EU)



Het inlichtingenwerk is meer dan ooit een internationaal fenomeen: dreigingen stoppen niet aan de landsgrenzen en landen worden ook met gelijkaardige uitdagingen geconfronteerd. Om de uitwisseling van inlichtingen te optimaliseren, blijft de VSSE investeren in haar netwerk van verbindingsofficieren in het buitenland en bij de multilaterale instellingen in Brussel.

# DE VSSE DECLASSIFICEERT HAAR ARCHIEVEN OVER WERELDOORLOG II

Het voorbije jaar heeft de VSSE haar archieven over de periode rond Wereldoorlog II grotendeels gedeclineerd en klaargemaakt voor overdracht aan het Algemeen Rijksarchief. De archieven van de VSSE worden ook in toenemende mate geconsulteerd. In 2024 ging het in totaal om meer dan 250 aanvragen via het Studie- en Documentatiecentrum Oorlog en Hedendaagse Maatschappij (CEGESOMA) en rechtstreeks bij de VSSE.

In een democratische samenleving horen geclassificeerde documenten van een inlichtingendienst niet voor eeuwig en altijd achter slot en grendel te blijven omdat ze 'vertrouwelijk', 'geheim' of 'zeer geheim' werden geclassificeerd. Ooit kregen die documenten die stempel omdat hun verspreiding bijvoorbeeld zou kunnen leiden tot de onthulling van een menselijke bron of van een bijzondere inlichtingenmethode, zoals pakweg een telefoontap. Maar wat ooit geclassificeerd was, moet dat niet noodzakelijk blijven, vond ook het Belgisch parlement in 2022. Sinds 7 oktober van dat jaar heeft de VSSE de wettelijke verplichting haar historische archieven te declassificeren en daar jaarlijks over te rapporteren aan de Kamer van Volksvertegenwoordigers.

Het voorbije jaar heeft de dienst Archief en Documentatie van de VSSE met de steun van talloze medewerkers van de dienst en onder begeleiding van twee gedetacheerden van het Algemeen Rijksarchief 80 dossiers van het archiefonds over de zogenaamde 'Incivieken' gedeclineerd en geïnventariseerd. Het gaat om de dossiers rond collaborateurs tijdens de Tweede Wereldoorlog, waarvan de activiteiten ook na de oorlog door de VSSE werden opgevolgd.

Aan de andere kant van het spectrum bevindt zich het fonds met de naam 'Occupation-Résistance' dat handelt over het brede gamma van verzetsgroepen tijdens de Tweede Wereldoorlog, gaande van links-extremistische, tot royalistische of militaire verzetsgroepen. Hun doen en laten werd ook na afloop van de oorlog in de gaten gehouden door de VSSE. De 123 dossiers met documenten van dit fonds werden gedeclineerd.

Twee andere archiefonds 'Occupation Allemande' en 'Occupation-Collaboration' handelen over de (gedwongen) samenwerking met de Duitse bezetter. De twee fonds werden volledig gedeclineerd.

Naast de declassificatie buigt de dienst Archief en Documentatie van de VSSE zich ook over de inza-verzoeken voor het archief van de VSSE door onderzoekers. In 2024 werden zo 20 verzoeken gericht aan de VSSE. Driekwart van die verzoeken werden met een positief gevolg afgehandeld of zijn nog in behandeling.



## ► WEERSTANDERS

Daarnaast werden in 2024 nog eens 239 aanvragen ingediend om archiefstukken over 'Inlichtingen- en actiediensten' of 'Inlichtingen- en actieagenten' te raadplegen. Deze dossiers van de VSSE over verzetslui bevinden zich al sinds 1993 bij het CEGESOMA, het Studie- en Documentatiecentrum Oorlog en Hedendaagse Maatschappij. Het hoge aantal aanvragen – 239 aanvragen met betrekking tot maar liefst 1.068 dossiers – is wellicht het gevolg van de lancering van het online platform Wikibase Résistance/Verzet in de tweede helft van 2024 (<https://resistanceinbelgium.be>). Via dat platform kunnen geïnteresseerden gegevens opzoeken over maar liefst 150.000 verzetsmannen en -vrouwen aan de hand van hun naam, geboortedatum, woonplaats of naam van de verzetsbeweging waarin ze actief waren.