



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

# INTELLIGENCE REPORT 2024

**SÛRETÉ DE L'ÉTAT**

**.be**



Éditeur responsable : Francisca BOSTYN  
Boulevard du Roi Albert II, 6 - 1000 Bruxelles

# TABLE DES MATIÈRES

---

<b>4</b>	<b>PRÉFACE DE L'ADMINISTRATRICE GÉNÉRALE</b>	
<b>6</b>	<b>PARTIE 1 : LA VSSE COMME SERVICE DE RENSEIGNEMENT</b>	
	- Escalation des menaces hybrides en Belgique et en Europe	7
	- La Russie opte pour des stratégies agressives afin de déstabiliser l'occident	8
	- Mer du Nord : un parfait terrain d'action pour une guerre hybride	10
	- Désinformation et polarisation dans une double année électorale	11
	- Cyberattaques : la Belgique n'est pas immunisée	13
	- La VSSE lutte contre le contournement des sanctions visant la Russie	14
	- La VSSE collabore à l'enquête sur l'ingérence russe au sein du Parlement européen	15
	- Espionnage et ingérence dans le code pénal	16
	- Chine : difficile équilibre entre intérêts et risques	18
	- L'hydre de la menace terroriste djihadiste	20
	- Près d'un tiers des personnes impliquées dans les dossiers de terrorisme de la VSSE sont mineures	22
	- La propagande extrémiste encourage les <i>lone actors</i> à avoir recours à la terreur	24
	- Les conflits au Moyen-Orient et leur impact en Belgique	26
	- Menace de l'extrémisme religieux et idéologique	27
	- La VSSE et le SGRS transmettent chaque semaine des dossiers terrorisme à la police et au parquet	29
	- La VSSE contribue à la lutte contre le crime organisé	31
<b>32</b>	<b>PARTIE 2 : LA VSSE COMME SERVICE DE SÉCURITÉ</b>	
	- La VSSE travaille au renforcement de la culture de sécurité	33
	- L'ANS a délivré près de cinq fois plus d'habilitations de sécurité en cinq ans	34
	- Les vérifications effectuées par la VSSE en hausse de 36 % en 2024	35
	- La VSSE a formulé 86 avis sur des investissements directs étrangers	36
<b>37</b>	<b>PARTIE 3 : À PROPOS DE LA VSSE</b>	
	- Les chiffres de la VSSE en 2024	38
	- La VSSE déclassifie ses archives sur la seconde Guerre mondiale	39



Francisca BOSTYN  
Administratrice générale

## PRÉFACE

Suivant la tradition annuelle, je vous présente l'*Intelligence Report* de la Sûreté de l'État (VSSE). En 2024, nous ne pouvons à nouveau pas ignorer l'impact du contexte géopolitique international sur notre sécurité intérieure. L'agression russe a sans nul doute joué un rôle prépondérant à ce niveau ces dernières années. Ainsi, des tentatives d'ingérence dans les processus démocratiques continuent d'émerger. À titre d'exemple citons l'affaire *Voice of Europe*, révélée l'an dernier.

Mais de nouveaux théâtres d'opérations qui ne se trouvaient auparavant pas sur notre radar sont apparus, comme par exemple la mer du Nord. Aujourd'hui, les actions suspectes de navires en mer du Nord ne sont plus à exclure de l'actualité et requièrent de la part de la VSSE un suivi actif

des nouvelles évolutions du genre, en coopération avec ses partenaires belges.

La désinformation et la polarisation sont des problématiques récurrentes au fil des ans, et nous avons dû redoubler de vigilance en cette année de période électorale. Je suis convaincue de la nécessité d'ancrer cette vigilance dans notre approche des menaces étrangères à l'encontre de nos démocraties occidentales. En effet, toute question sociétale sensible peut et pourra être utilisée par des acteurs étrangers désireux d'attiser la polarisation. La polarisation, avivée par la désinformation, est subtile et difficile à contrer et peut se révéler extrêmement perturbatrice pour la société. Le suivi de ce phénomène constituera dès lors un défi permanent pour la VSSE.

Dans leurs actions hybrides, nos adversaires se montrent souvent très inventifs. À l'instar d'autres services de renseignement européens, nous constatons ainsi que le recrutement d'individus s'effectue sur une base beaucoup plus souple, par exemple via Telegram, où des agents *freelance* sont recrutés ponctuellement pour des opérations d'espionnage ou de sabotage. Il va sans dire que cette façon de travailler complexifie l'intervention des services de renseignement et de sécurité.

Dans ce contexte, en tant que service de renseignement, nous devons faire preuve de flexibilité et disposer de moyens de protection adaptés. Je me réjouis par conséquent que la VSSE puisse avoir recours depuis 2024 à un Code pénal révisé, classant l'espionnage et l'ingérence au rang des infractions pénales.

Les récents attentats à la Nouvelle-Orléans et Magdebourg ont montré que le terrorisme restait l'une des principales menaces, y compris pour la VSSE. À cet égard, l'État islamique (EI) et sa branche du Khorasan (ISKP) constituent les menaces prédominantes dans notre pays, notamment car leur idéologie peut inciter des *lone actors* à passer à l'action. La menace de l'ISKP a donné lieu à une série d'interventions judiciaires dans notre pays en juillet 2024 visant un certain nombre de sympathisants de cette organisation. Un autre constat frappant et alarmant est le fait que près d'une personne sur trois impliquée dans les dossiers de terrorisme de la VSSE est mineure d'âge. Ce défi concerne les services de sécurité, certes, mais aussi les acteurs sociopréventifs s'adressant à la jeunesse. Toutefois, les mineurs d'âge parviennent fort heureusement moins souvent à la phase d'exécution en raison de leurs moyens d'action plus réduits.

Les développements survenus en Syrie en décembre 2024 ont à nouveau propulsé à l'avant-plan la question des *foreign terrorist fighters* belges encore présents dans cette zone. Il s'agit là de l'exemple le plus manifeste de la manière dont certaines évolutions à l'étranger peuvent impacter notre propre sécurité : quelle que soit la solution envisagée face au problème, force est en effet de constater que ces *foreign terrorist fighters* posent un problème de sécurité pour notre pays.

De plus, je tiens à souligner que la VSSE est plus qu'un simple service de renseignement : nous sommes également une organisation dotée d'une importante mission de sécurité. C'est d'autant plus le cas depuis l'intégration de l'Autorité nationale de Sécurité au début de 2024. L'Autorité nationale de Sécurité est notamment chargée de délivrer des habilitations de sécurité et de veiller au traitement adéquat des informations classifiées – une mission que nous exécutons entre autres en sensibilisant activement les officiers de sécurité présents dans un nombre croissant d'organisations. Le contexte sécuritaire dans lequel nous vivons et le renforcement de la conscience de l'importance de la sécurité ont entraîné une hausse significative de la charge de travail, un constat qu'il importe de reconnaître et de relayer.

Pour conclure, je souhaite aborder différents défis majeurs pour l'avenir.

D'abord et avant tout, les défis liés aux cybermenaces et à l'évolution fulgurante des nouvelles technologies. Pour ne pas nous laisser distancer, nous devons nous les approprier rapidement. L'éventail des technologies à couvrir est cependant large et va de l'intégration de l'intelligence artificielle dans notre travail quotidien à la recherche de solutions d'accès aux communications cryptées.

Le défi technologique en appelle trois autres. Premièrement, le défi humain. Il n'est pas évident de trouver du personnel qualifié à même de maîtriser cette complexité technologique. Et si nous le trouvons, comment nous assurer que nous pouvons offrir à ces collaborateurs des conditions de travail et des salaires attrayants ? Ce type de spécialisations est très convoité sur le marché privé, dont le poids excède de loin celui d'une administration fédérale.

Deuxièmement, vient le défi juridique : l'évolution rapide des menaces et progrès technologiques implique une mise à jour permanente de la législation qui demande un temps certain pour être adaptée. Le troisième défi est l'augmentation ex-

ponentielle des données. En tant que service de renseignement, nous devons constamment trouver de nouvelles méthodes pour traiter ces énormes quantités d'informations. À la VSSE, nous sommes pleinement engagés dans la mise en œuvre d'un nouveau modèle d'enquête et d'un nouvel environnement IT qui devraient nous permettre, à terme, de mieux faire face à cette situation. En outre, cela nécessitera des investissements constants à l'avenir.

Un ultime défi majeur, à mes yeux, est la contribution que la VSSE devra apporter en vue d'accroître la résilience de notre pays à une époque où le débat sur la guerre en Europe est rouvert. Le monde politique et les services de sécurité sont de plus en plus conscients de la nécessité de mieux préparer notre société à la guerre et à d'autres situations de crise. Comment les centrales électriques et les hôpitaux continueront-ils à fonctionner ? De quelle manière assurerons-nous les grands mouvements de troupes ? Et comment la VSSE devra-t-elle adapter son travail de renseignement si la Belgique devait s'engager dans un conflit armé ? Sans oublier la question de la sauvegarde de notre prospérité économique. Il importe de protéger non seulement notre propriété intellectuelle, mais aussi nos infrastructures critiques. À l'avenir, la Belgique et l'Europe devront accorder une attention accrue à la pression exercée sur notre tissu économique, d'autant plus au vu de l'assertivité croissante de pays tels que la Chine.

Avec nos partenaires belges et internationaux – coopérer est primordial dans un monde où il n'existe pas de frontières en matière de sécurité – nous continuons chaque jour à faire tout ce qui est en notre pouvoir afin de protéger notre démocratie et les habitants de notre pays. Ces dernières années, nous avons eu l'occasion de renforcer sensiblement notre service en termes de personnel et de budget. Je tiens du reste à profiter de l'occasion pour remercier les nouveaux et moins nouveaux collaborateurs pour l'engagement, l'enthousiasme et la foi en notre mission dont ils font preuve au quotidien.

Nous sommes tous, j'en suis convaincue, prêts à assumer nos responsabilités dans cette nouvelle réalité qui est la nôtre.

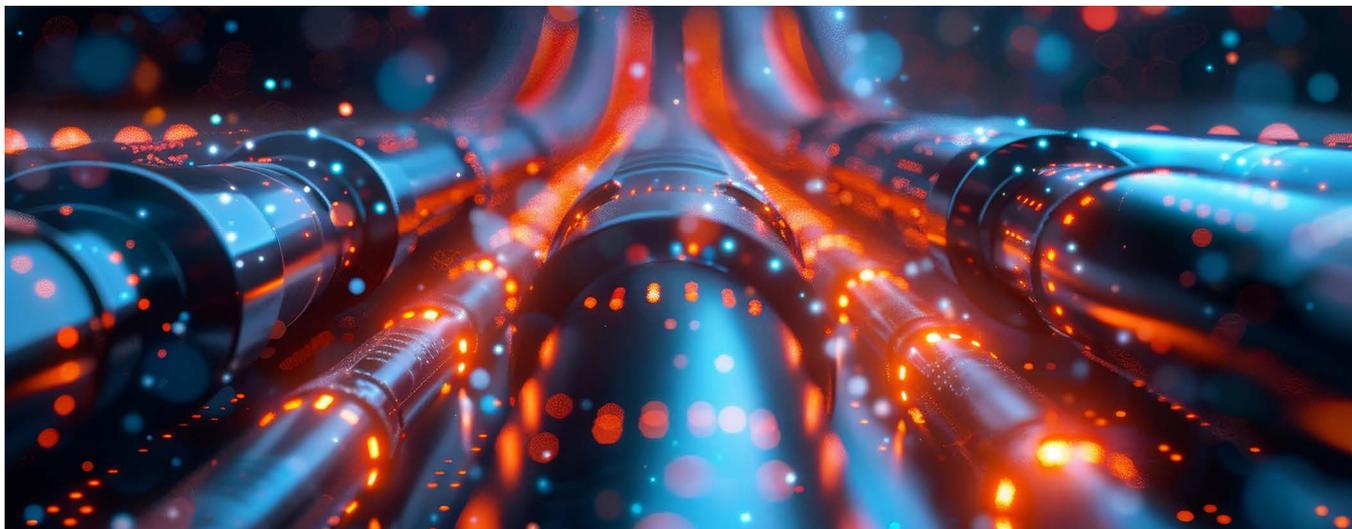
Francisca Boslyn

# 01

**LA VSSE COMME  
SERVICE DE RENSEIGNEMENT**

## ESCALATION DES MENACES HYBRIDES EN BELGIQUE ET EN EUROPE

Explosion de colis dans les centres de tri d'un service de courrier d'aéroports européens, sabotage de voies ferrées, drones de reconnaissance survolant des casernes militaires, cyberattaques, ancrs de navires sectionnant des câbles internet sous-marins, campagnes de désinformation polarisantes visant à influencer les élections. 2024 a été l'année de l'escalation des menaces hybrides, attribuées en grande partie à la guerre hybride russe.



Le concept de menace hybride renvoie à une combinaison d'activités menées par des acteurs étatiques et/ou non étatiques, dans le but d'influencer négativement et de manière inaperçue un opposant ou ses institutions, ou d'occasionner des dégâts. Le caractère « inaperçu » revêt à cet égard une grande importance. Une menace hybride peut être tout aussi concrète qu'une attaque cinétique traditionnelle, mais le commanditaire de cette attaque n'est jamais clairement identifiable. Cette stratégie est appliquée à dessein. En effet, elle empêche toute réaction consolidée, de l'OTAN par exemple. Cette approche hybride – adoptée par des auteurs difficilement identifiables – ne permet pas d'attribuer aisément et avec certitude la responsabilité de ces actions à un auteur donné, et reste dès lors parfois sans réaction.

C'est le succès des menaces hybrides : le déploiement d'activités préjudiciables sans grand risque de réaction. Des indices particulièrement nombreux laissent supposer que l'année dernière, la Russie a intensifié ses actions hybrides en Europe, tant d'un point de vue géographique, de l'Europe de l'Est vers l'Europe de l'Ouest, que d'un point de vue méthodologique. La Russie est rompue à la guerre hybride et œuvre avec des collectivités de hackers (cybermenace), des organisations criminelles (attaques contre des infrastructures critiques) et des

agents *freelance* pour opérer le plus discrètement possible.

Si, ces deux dernières années, l'attention s'est portée sur les actions attribuables à la Russie, d'autres acteurs – étatiques ou non – ne sont pas en reste. À titre d'exemple, citons la Chine, qui fait usage à grande échelle de méthodes hybrides.

### ► UNE APPROCHE *WHOLE OF SOCIETY*

À l'heure actuelle, l'un des défis majeurs des services de renseignement consiste à anticiper les attaques, à les identifier (les acteurs du monde commercial n'apprécient pas particulièrement dévoiler leurs faiblesses) et à pouvoir les attribuer à un acteur spécifique. Il s'agit là d'un travail de spécialiste auquel la VSSE coopère au niveau national et international.

Chaque acteur a un rôle spécifique à jouer dans ce domaine. En Belgique, la VSSE coopère étroitement avec le Centre de crise National (NCCN), le Service Général du Renseignement et de la Sécurité (SGRS), la Police Fédérale, l'OCAM et le Centre pour la Cybersécurité Belgique (CCB) mais aussi avec des entreprises du secteur privé. Notre réponse collective déterminera si nous sortirons renforcés ou affaiblis de cette période. ■

# LA RUSSIE OPTÉ POUR DES STRATÉGIES AGRESSIVES AFIN DE DÉSTABILISER L'OCCIDENT

Les expulsions massives d'officiers de renseignement russes sous couverture diplomatique de pays européens ont placé Moscou dans une position délicate. La capacité des services de renseignement russes sur le territoire européen a été sérieusement ébranlée, alors que leurs ambitions demeurent inchangées. Afin de tenter de résoudre le problème, les services de renseignement russes opèrent de manière toujours plus créative.



Depuis l'invasion à grande échelle de l'Ukraine par la Russie au début de l'année 2022, des centaines d'officiers de renseignement russes « traditionnels » ont été contraints de quitter l'Union européenne et ses pays partenaires tels que le Royaume-Uni et la Norvège. Ces officiers avaient généralement un statut officiel de diplomate auprès des représentations russes ; en Belgique, il s'agit de l'ambassade de Russie, de la mission russe auprès de l'Union européenne à Bruxelles et du consulat général de Russie à Anvers (la mission russe auprès de l'OTAN avait déjà fermé ses portes de sa propre initiative en 2021). Les officiers expulsés en 2022 et 2023 ont pour la plupart été déclarés « *persona non grata* ». Notre pays a ainsi fait en sorte que des dizaines d'officiers de renseignement russes soient contraints de rentrer à Moscou.

Ces expulsions ont fortement limité la capacité des services de renseignement russes et leur liberté de mouvement sur le territoire européen. D'un autre côté les besoins en renseignements de la Russie n'ont pas disparu pour autant. Au contraire. La

guerre persiste, et en présentant son agression comme une lutte contre le monde occidental, la Russie opte pour une stratégie hybride agressive. D'une part, elle souhaite obtenir des renseignements spécifiques, par exemple sur le soutien militaire et financier apporté à l'Ukraine par les pays européens ou sur les régimes de sanctions ; d'autre part, elle a également pour ambition de déstabiliser et de décrédibiliser le monde occidental en alimentant voire en créant un climat d'agitation sociale ou par la diffusion de ses propres narratifs idéologiques.

L'an dernier, il est clairement apparu que, dans leur quête de nouvelles méthodes visant à collecter des informations et d'exécuter des actions en Europe, les services de renseignement russes avaient adopté une approche innovante de recrutement et de *tasking* des agents. Cette approche s'inscrit dans la logique de la *gig economy* – un marché du travail basé sur des contrats flexibles, temporaires ou en *freelance*. Par le biais des réseaux sociaux (notamment Telegram) et en utilisant plusieurs



intermédiaires, des missions sont largement diffusées, et proposées à toute personne intéressée, tout comme n'importe qui peut s'improviser chauffeur de taxi via Uber ou arrondir ses fins de mois comme livreur à vélo via Deliveroo. Les services de renseignement russes font également de plus en plus appel aux réseaux criminels, ce qui complique également la détection de leurs activités.

Les missions confiées à ces *freelancers* ou organisations criminelles vont de la collecte de renseignements ou des actions de propagande à la reconnaissance militaire en passant par le sabotage (voir encadré). À Londres par exemple, un entrepôt abritant de l'aide matérielle pour l'Ukraine a été incendié ; le sort des auteurs est actuellement entre les mains de la justice. En Belgique, aucune activité confirmée d'espionnage ou de subversion menée par des agents *freelance* en mission pour les services de renseignement russes n'a encore été recensée, ce qui ne signifie en aucun cas que nous ne devons pas nous préparer à ce genre d'actions.

Par ailleurs, le recours à des organisations criminelles et l'application des principes et des leçons de la *gig economy* n'est pas l'exclusivité des services de renseignement russes. Le recours à des individus ne présentant aucun lien direct manifeste avec le milieu des services de renseignement pour des opérations de renseignement bien définies est un phénomène qui gagne en intérêt et en ampleur. Cela réduit en effet les risques de compromission pour les officiers de renseignement professionnels au cours d'une opération et renforce la *plausible deniability* recherchée par les services de renseignement hostiles (et leurs dirigeants politiques).

## ► DES FREELANCERS COMME AGENT POUR LA RUSSIE

Le recrutement d'agents *freelance* via les médias sociaux s'effectue par étapes : comme dans le cas d'un recrutement classique, les agents potentiels doivent, d'une part, faire leurs preuves et, d'autre part, se compromettre toujours davantage.

- Une petite annonce pour une mission simple apparaît dans un groupe Telegram : « Allez coller des stickers anti-Ukraine dans la rue et recevez 20 euros ». Une personne marque son intérêt. Un bot lui pose une série de questions de base.
- Le candidat répond correctement aux questions-test. Un officier de renseignement russe reprend alors la conversation et lui fournit davantage d'instructions. L'agent exécute la mission et transmet une photo en guise de preuve. Il est payé en cryptomonnaie.
- S'ensuit une deuxième mission, plus risquée voire illégale : « Allez photographier cette infrastructure militaire ».
- Les missions se succèdent et deviennent de plus en plus lourdes. L'exécutant s'enfoncé toujours plus dans l'illégalité pour se voir finalement confier une demande de sabotage.

Il s'agit d'un exemple abstrait.

Ainsi, en faisant appel à des *freelancers* et à des organisations criminelles, les services de renseignement étrangers font d'une pierre deux coups : ils donnent l'impression d'être (ou de pouvoir être) actifs partout, alors que les activités ne peuvent que rarement leur être réellement attribuées.

## ► PAS DE PANIQUE

La Russie entend non seulement bloquer le soutien à l'Ukraine, mais la déstabilisation des sociétés occidentales est aussi un objectif en tant que tel. Il est tentant de voir systématiquement l'empreinte de Moscou dans chaque incident. Céder à ce raisonnement ferait cependant le jeu du Kremlin. L'un des objectifs de ce nouveau mode opératoire consiste en effet précisément à semer la panique en donnant la fausse impression que la Russie peut frapper partout, à tout moment. C'est pourquoi la VSSE et ses partenaires doivent veiller à ne pas créer de polémiques inutiles dans le cadre du suivi de ce phénomène.

# LA MER DU NORD : UN PARFAIT TERRAIN D'ACTION POUR UNE GUERRE HYBRIDE



**La mer du Nord représente un terrain d'action idéal pour une guerre hybride. En mer, les acteurs hostiles peuvent en effet opérer de façon relativement inaperçue, surtout s'ils déploient pour cela non seulement des navires de guerre mais aussi des porte-conteneurs, des navires de recherche voire de simples voiliers. Pourquoi finalement s'inquiéter d'un voilier navigant paisiblement au gré des flots de la mer du Nord ou d'un navire cargo dont l'ancre reste un peu trop longtemps dans les fonds marins ?**

La mer du Nord est un environnement stratégique par excellence, traversée par des câbles de données, des câbles énergétiques et des gazoducs. Le nombre d'incidents concernant de tels câbles et conduites ne fait qu'augmenter, notamment en mer Baltique. La mer du Nord au large de la Belgique est également une cible potentielle. Au cours des derniers mois, de plus en plus de mouvements suspects ont été détectés sur des navires qui, parfois, suivent également des itinéraires illégaux.

Il est évident que ces mouvements suspects sont suivis de près par les différents services belges dans le cadre du Carrefour de l'Information Maritime (MIK). Le MIK est une des composantes de la Centrale Garde côtière en Belgique. Dans ce centre situé à Zeebrugge, la Douane, la police maritime, la Défense et la cellule de sécurité maritime du SPF Mobilité unissent leurs forces et leurs compétences pour collecter, analyser et partager les informations. Ils travaillent à la fois de manière pré-

## ► QUELQUE CHOSE SE TRAME EN MER DU NORD

En avril 2024, à l'initiative du ministre belge de la mer du Nord, Paul Van Tigchelt, les ministres compétents de six pays bordant la mer du Nord ont conclu un accord dans lequel ils déclarent qu'ils vont collaborer à la protection des infrastructures sous-marines critiques contre les actes de sabotage et les attaques. Un volet de cet accord concerne le développement d'un système sécurisé d'échange d'informations sur les incidents.

En août 2024, en marge d'une conférence sur l'énergie organisée à Stavanger, en Norvège, les services de renseignement de huit pays proches de la mer du Nord ont appelé à renforcer la sécurité des infrastructures sous-marines en mer du Nord.

En décembre 2024, le port d'Anvers-Bruges a convié des représentants de l'industrie belge, du secteur maritime, des institutions bancaires, du monde académique et du secteur de la sécurité – dont la VSSE – à une soirée interactive sur le thème de la sécurité maritime.

ventive et réactive pour améliorer la sécurité dans les ports et en mer. Une tâche importante : au large de nos côtes se trouve l'une des voies maritimes les plus fréquentées au monde. La VSSE est en contact permanent avec le MIK et échange notamment sur cette problématique lors de fora internationaux. ■

# DÉSINFORMATION ET POLARISATION DANS UNE DOUBLE ANNÉE ÉLECTORALE

L'année 2024 fut une année électorale sans précédent. Plus de 2 milliards de personnes ont en effet pu exprimer leur vote dans le monde entier. La Belgique aussi a connu des élections, à tous les niveaux également : du local à l'europpéen. Pour en garantir le déroulement libre et équitable, la VSSE a non seulement mené ses propres enquêtes, mais elle a aussi étroitement collaboré avec ses partenaires belges et étrangers.



Les élections représentent une période sensible, lors de laquelle les activités de désinformation et d'ingérence peuvent potentiellement avoir un impact plus grand. Les acteurs hostiles en sont également conscients. Au cours de l'année électorale 2024, la désinformation a largement circulé dans le paysage de l'information de notre pays.

Les responsables et partis politiques belges et – plus généralement – notre processus électoral en ont toutefois été rarement les cibles explicites. Ce constat est en quelque sorte le fil conducteur de l'année électorale belge dans son ensemble.

Quelques voix extrémistes et antisystèmes se sont bien élevées au sein de notre propre pays, remettant par exemple en cause le déroulement équitable des élections, notamment par des insinua-

tions infondées à propos des ordinateurs de vote. Des acteurs anarchistes et salafistes ont aussi appelé à l'abstention. Le nombre et la portée de ces messages sont néanmoins restés très limités. De plus, il n'a jamais été question de désinformation ayant permis de perturber réellement les élections ou d'en altérer les résultats.

## ► POLARISATION PERMANENTE

Le problème n'est pas résolu pour autant. Des acteurs hostiles, tels que la Russie, bombardent quasiment en continu le paysage de l'information occidentale – et donc également le paysage belge – de messages polarisants et antidémocratiques. S'il s'agit parfois de messages entièrement faux, ils tentent le plus souvent d'attiser tout simplement des sujets sensibles ou d'amplifier et d'exploiter des incidents polarisants.

Outre les thèmes « classiques », tels que la migration et les droits des personnes transgenres et LGBTQI+, des événements tels que les manifestations des agriculteurs, le conflit à Gaza ou encore le soutien occidental à l'Ukraine ont aussi été utilisés en 2024. L'objectif est toujours le même : diviser notre société et ébranler la confiance en notre démocratie.

### ► LA DIFFUSION DE DÉSINFORMATION PUNISSABLE DANS CERTAINS CAS

La VSSE n'est pas une police idéologique. Nous ne sommes pas non plus des *fact-checkers*. La circulation de fausses informations ne relève pas des compétences intrinsèques de la VSSE.

De fausses informations arrivent sur notre radar lorsque des acteurs hostiles exploitent notre ouverture et nos libertés fondamentales en vue de promouvoir clandestinement leurs propres intérêts stratégiques.

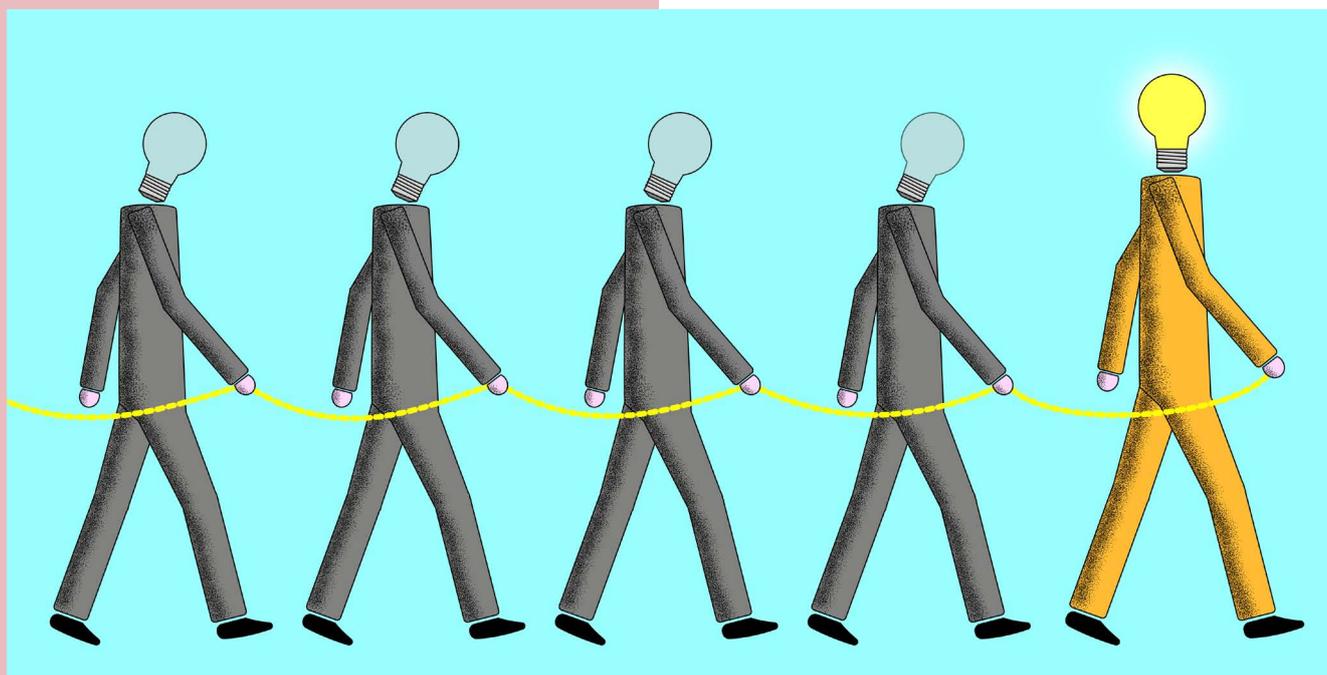
À noter que la communication d'informations essentielles erronées à des autorités belges dans le but de les induire en erreur et de porter ainsi atteinte aux intérêts nationaux essentiels constitue une infraction pénale depuis avril 2024.

Aucun service ne peut faire face seul à ce phénomène. Les services de renseignement ne sont qu'un maillon de la lutte contre la désinformation, dans le cadre de laquelle les médias, l'enseignement et la société civile ont un rôle important à jouer.

### ► INTELLIGENCE ARTIFICIELLE

L'utilisation de l'intelligence artificielle (IA) n'a eu qu'un impact extrêmement limité sur les élections en Belgique. On craignait avant celles-ci que l'IA soit un catalyseur de toutes formes de désinformation. Les *deepfakes*, de faux clips vidéo et audio diffusés pour compromettre des personnalités politiques, en sont un exemple parmi d'autres. Les craintes à ce sujet se sont révélées infondées – pour notre pays du moins.

Mais rappelons que la vigilance reste de mise. En effet, indépendamment des élections, le risque court toujours que de fausses vidéos, *memes* et messages divers continuent d'éroder la cohésion de notre société ainsi que la confiance en nos institutions démocratiques. Et l'intelligence artificielle permet de créer et de diffuser ce genre de contenu de plus en plus rapidement, à des coûts toujours moindres et de manière toujours plus ciblée par rapport au public visé.



# CYBERATTQUES : LA BELGIQUE N'EST PAS IMMUNISÉE



Suite aux attaques dirigées par un groupe de hackers prusses contre des dizaines de sites web belges à l'approche des élections communales d'octobre 2024, il est clairement apparu que notre pays n'était pas immunisé contre les cyberattaques à grande échelle. Cette attaque a été principalement utilisée à des fins de propagande ; dans d'autres cas, des informations confidentielles sont parfois également dérobées.

Au cours de la période du 7 au 13 octobre 2024, le groupe d'activistes prusses NoName057(16) a ainsi ciblé différents sites web belges. Il s'agissait d'attaques de type *Distributed Denial of Service* (DDoS), consistant à inonder de trafic des sites web/services en ligne dans le but de les surcharger et de les rendre temporairement indisponibles aux utilisateurs. Ce genre d'attaque ne permet pas le vol de données et n'implique pas d'intrusion dans les systèmes.

## ► SOUTIEN À L'UKRAINE ET REPRÉSAILLES

Selon les informations communiquées par le groupement, les attaques avaient été menées en guise de représailles pour les livraisons d'armes prévues par la Belgique en soutien à l'Ukraine, en particulier la livraison de pièces d'artillerie CAESAR. Malgré le timing des attaques – une semaine avant les élections locales – et la référence limitée à celles-ci dans la communication du groupe, l'accent n'était pas mis sur les élections.

Les attaques DDoS ont visé différentes cibles : majoritairement les sites web d'administrations locales (communales et provinciales) mais aussi certains sites des autorités fédérales (SPF Finances, SPF Économie), de ports maritimes, de Bpost, de fédérations sectorielles (Febelgra, Febelfin), de l'agence de presse Belga, etc. L'impact de ces attaques était globalement limité. Plusieurs sites web sont restés inaccessibles pendant un certain temps.

Le groupement en question, actif depuis 2022, avait déjà mené diverses cyberattaques contre des sites web belges par le passé. En janvier 2024, des sites notamment liés à la Chancellerie, à la Chambre des Représentants ou encore au Sénat ont été pris pour cible. NoName057(16) est actif au niveau international et a déjà dirigé des attaques DDoS contre les sites web d'agences gouvernementales, de sociétés de médias, d'infrastructures critiques et d'entreprises privées dans plusieurs pays européens, mais aussi en dehors de l'Union européenne (États-Unis, Royaume-Uni).

Lors de tels incidents, la VSSE reste en contact permanent avec les services partenaires ayant le lead dans la lutte contre les cyberattaques, tels que le Centre pour la Cybersécurité Belgique (CCB) pour l'analyse technique et le Service Général du Renseignement et de la Sécurité (SGRS) des Forces armées pour le travail opérationnel. La VSSE a pour objectif de donner forme à l'aspect « contre-espionnage » dans les enquêtes cyber. L'objectif est ainsi de recueillir davantage d'informations sur les centres d'intérêts des hackers étatiques et non étatiques, sur les informations compromises et sur les conclusions que nous devons tirer sur les intentions de nos adversaires.

## LA VSSE LUTTE CONTRE LE CONTOURNEMENT DES SANCTIONS VISANT LA RUSSIE

Parmi les enjeux géopolitiques et sécuritaires mondiaux, les programmes des armes de destruction massive nucléaires, biologiques, chimiques et radiologiques et de leurs vecteurs représentent un défi crucial pour la sécurité de notre pays et celle de nos alliés. Ainsi, empêcher certains acteurs étatiques d'acquérir des biens et technologies visés par des régimes de sanctions est aussi une des missions de la VSSE.

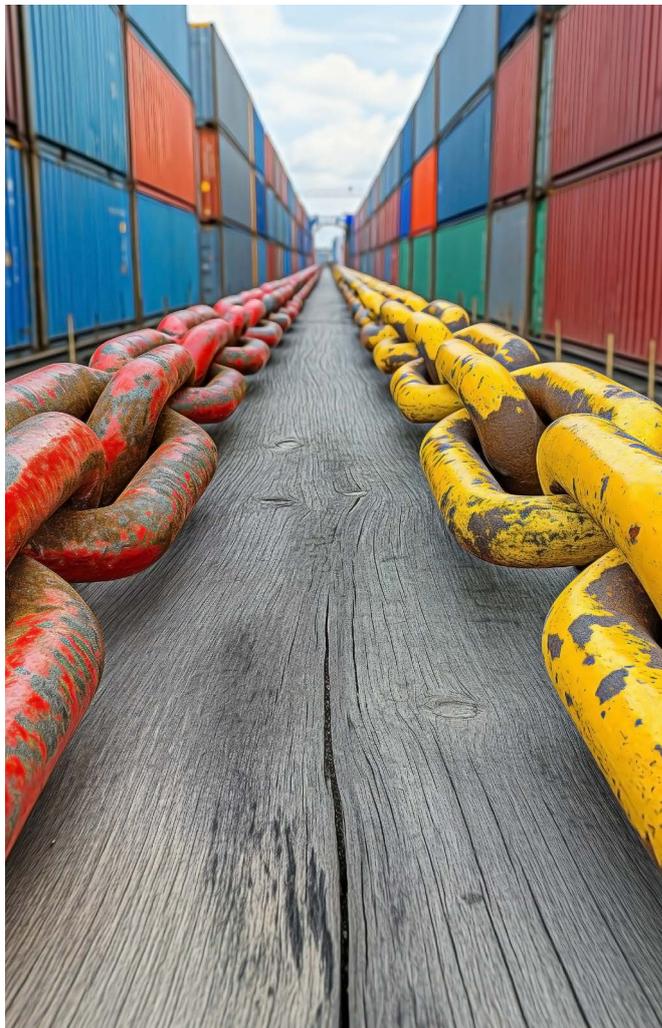
La VSSE soutient la stratégie internationale ayant deux objectifs clairement identifiés : d'une part contrer les capacités du complexe militaro-industriel russe qui soutient l'agression en Ukraine et d'autre part imposer à la Russie des conséquences structurelles lourdes pour ses actions envers son voisin ukrainien.

L'évolution de la guerre en Ukraine et les différents trains de sanctions imposées à la Russie les obligent à s'adapter et à trouver des nouveaux canaux afin de se procurer des biens nécessaires aux programmes d'armes non-conventionnelles et très avancées. Il s'agit souvent de biens dits à double usage, à savoir des biens pouvant avoir tant un usage civil que militaire. À côté de composants de haute technologie, il peut aussi s'agir de biens relativement rudimentaires qui peuvent être utilisés pour le processus de fabrication de certaines armes ou moyens de transmission.

Concrètement, des sociétés russes, souvent pilotées par l'État et ses services de renseignement, cherchent ainsi à acquérir en Belgique ou via notre pays des biens et technologies utiles à l'effort de guerre russe. Ces acquisitions peuvent se faire notamment via la contribution de sociétés installées dans des pays-tiers en Asie, au Moyen-Orient, en Europe ou en Afrique.

La VSSE contribue activement à l'application des sanctions internationales contre la Russie, notamment en identifiant et en perturbant les mécanismes de contournement des sanctions visant ce pays, et ce, en collaboration avec les partenaires nationaux et internationaux.

Enfin, la VSSE est pleinement engagée, avec ces mêmes partenaires, à empêcher d'autres acteurs d'acquérir des matériaux, des technologies, du



savoir-faire et des connaissances nécessaires au développement de programmes liés à des armes de destruction massive et leurs vecteurs, tels que les missiles et les drones. Il s'agit notamment d'États tels que l'Iran et la Corée du Nord qui font l'objet de sanctions internationales.



# LA VSSE COLLABORE À L'ENQUÊTE SUR L'INGÉRENCE RUSSE AU SEIN DU PARLEMENT EUROPÉEN

La VSSE fait preuve de vigilance face à l'ingérence étrangère clandestine dans le processus décisionnel en Belgique mais endosse par ailleurs ce rôle en sa qualité de service de renseignement et de sécurité de la nation hôte d'institutions européennes et internationales telles que l'UE et l'OTAN. Dans ce contexte, le service a contribué au cours de l'année écoulée à l'enquête sur un réseau d'ingérence prorusse articulé autour du média *Voice of Europe*.



Dans le cadre de sa mission de prévention des activités d'ingérence au sein et autour du Parlement européen, la VSSE a mené, en étroite collaboration avec différents services partenaires européens, une enquête sur un réseau d'ingérence prorusse dirigé et financé via un certain nombre d'intermédiaires par un oligarque ukrainien, magnat des médias.

De tels réseaux d'ingérence tentent de rallier à leur cause des députés « amis », au moyen ou non de compensations financières. Ils s'efforcent par ailleurs d'accroître la présence de députés prorusses au Parlement européen et à mieux organiser et coordonner leurs activités ; ces tentatives concernent également les assistants parlementaires.

Ce réseau d'ingérence a bénéficié du soutien d'une organisation médiatique propre, *Voice of Europe*, dirigée par un homme de paille en Tchéquie.

Plusieurs services européens (y compris la VSSE) ont collaboré intensivement pour mettre ce réseau en lumière. En mars 2024, les autorités tchèques ont décidé de placer l'oligarque, son homme de

paille en Tchéquie et *Voice of Europe* sur une liste de sanction en raison de leurs activités d'ingérence.

## ► UNE DÉMARCATIION TËNUE

Il n'est pas inhabituel en soi que des individus, groupes, organisations et États tentent de défendre leurs intérêts par le biais de la diplomatie, de représentations économiques, de campagnes de relations publiques, d'associations culturelles, etc. Cela fait partie du jeu politique et diplomatique classique. Pour en revenir à l'exemple de *Voice of Europe* : la Russie dispose encore d'une représentation diplomatique étendue dans l'UE et en Belgique. De ce point de vue, elle n'a pas besoin du réseau gravitant autour du magnat des médias ukrainien pour défendre ses intérêts de manière légitime.

L'ingérence diffère fondamentalement du lobbying ou de la diplomatie en ce sens qu'elle recourt à des « moyens illicites, trompeurs ou clandestins ».

# ESPIONNAGE ET INGÉRENCE DANS LE CODE PÉNAL

Depuis avril 2024, la Belgique dispose de nouveaux outils pour lutter contre l'espionnage et l'ingérence des pays étrangers. Jusqu'alors, l'espionnage et l'ingérence de pays étrangers n'étaient répréhensibles que si ces activités se produisaient dans un contexte militaire ou de guerre. En dehors de ces situations, l'ingérence et l'espionnage ne constituaient guère des infractions pénales.

Les activités d'ingérence et d'espionnage pouvaient-elles dès lors être déployées en toute impunité avant avril 2024 ? Non, bien entendu. Des mesures administratives étaient toujours envisageables. Par ailleurs, l'ingérence et l'espionnage s'accompagnent généralement d'autres faits répréhensibles (corruption ou association de malfaiteurs, par exemple).

Dans le monde actuel, ces mesures n'étaient plus suffisantes ; le législateur a dès lors décidé de faire entrer en vigueur anticipativement les incriminations relatives à l'ingérence et à l'espionnage, prévues à l'origine pour le nouveau code pénal de 2026. Notre pays assume ainsi pleinement ses responsabilités en matière de lutte contre l'espionnage et l'ingérence sur son territoire, non seulement contre les intérêts belges, mais également contre ceux des institutions internationales situées sur son sol.

## ► SECRET D'ÉTAT

Ces nouvelles infractions permettent d'engager des poursuites pour les activités d'espionnage, que ce soit pour transmission, divulgation, reproduction ou réception d'un secret d'état. Il en va de même pour les tentatives d'espionnage et les activités menées en préparation à la transmission d'un secret d'état. À cet effet, la notion de « secret d'état » est également définie dans la loi. Outre les informations classifiées, ce terme fait référence à toute information non accessible au public et qui revêt une grande importance pour la protection des intérêts de la Belgique.

De plus, quiconque se livre activement à des activités d'ingérence dans l'intention d'influencer les processus décisionnels démocratiques (les résultats des élections, le vote au Parlement, l'attribution d'un marché public, etc.) peut désormais





## ► LA VSSE ET LE SGRS COLLABORENT AU SEIN DE HOUSES THÉMATIQUES

En 2024, la collaboration entre la VSSE et le SGRS en matière de contre-espionnage et d'ingérence étrangère a également atteint un niveau plus élevé. Ainsi, depuis le printemps 2024, la VSSE et le SGRS rassemblent régulièrement leurs renseignements dans ces matières au sein de *Houses* thématiques qui se concentrent sur une seule région géographique ou une thématique particulière. Cela permet d'éviter le double travail et de mieux harmoniser les enquêtes des deux services.

être poursuivi si ces activités s'exercent de manière clandestine, c'est-à-dire à l'insu des autorités belges et dans le but de nuire gravement aux intérêts nationaux.

### ► PLATEFORME DE COOPÉRATION

Concrètement, les services en charge de ces thématiques se réunissent pour aborder les dossiers dans le cadre d'une plateforme. Pour chaque affaire, ils évaluent la méthode de suivi ayant les plus grandes chances de réussite. Existe-t-il suffisamment d'éléments infractionnels ? Les poursuites judiciaires constituent une option. Les services de renseignement peuvent encore recueillir de nombreuses informations grâce à ce dossier ou un doute subsiste ? Alors l'option de poursuivre le travail de renseignement est sans doute une meilleure option. Ce système est inspiré de la méthode employée par les JIC/JDC dans le cadre des dossiers terrorisme.

Quelle que soit l'option choisie, celle-ci doit toujours être suffisamment contextualisée et nuancée. Des poursuites judiciaires peuvent effectivement avoir un effet dissuasif ou envoyer un signe fort. Dans certains dossiers, il s'agit de la réaction la plus efficace. Dans d'autres, dans lesquels il n'y a aucune infraction, des mesures administratives peuvent être à l'ordre du jour.

### ► PAS SEULEMENT LES *USUAL SUSPECTS*

Il va de soi que la reprise de l'espionnage et l'ingérence dans le nouveau code pénal a des conséquences pour les acteurs étrangers qui s'adonnent à de l'espionnage ou à l'ingérence pour influencer de manière clandestine le processus décisionnel démocratique. La VSSE constate qu'outre la Russie ou la Chine, d'autres pays font de l'espionnage et de l'ingérence en Belgique. ■

## CHINE : DIFFICILE ÉQUILIBRE ENTRE INTÉRÊTS ET RISQUES



Dans un contexte géopolitique tendu, la relation – principalement économique – Chine-Belgique ou Chine-Europe reste importante. Néanmoins, la Chine exerce différentes menaces contre la Belgique et l'Europe en termes de cyber, d'espionnage ou d'ingérence, de risque pour notre potentiel économique et scientifique, de tentative de contrôle de la diaspora, etc. Il revient à la VSSE de détecter ces menaces, d'en informer les décideurs et de sensibiliser les différents acteurs belges – qu'ils soient étatique, universitaire ou du monde économique – aux risques auxquels ils sont exposés. Sur base de ces informations, il appartient aux décideurs de trouver un savant équilibre entre les intérêts économiques et les risques en matière de sécurité.

En 2024, la Chine a adopté un comportement plus assertif qu'auparavant à l'encontre de l'Europe, principalement dans le cadre de la défense de ses intérêts politiques et économiques. Il y a à cet égard un alignement relatif avec la Russie ; «relatif» dans la mesure où la République populaire de Chine veut toutefois conserver des relations commerciales avec l'Europe qui reste pour elle un partenaire économique majeur.

Ce comportement assertif se manifeste notamment par le biais de menaces hybrides à l'encontre de la Belgique et de l'Europe. Et sans doute encore plus qu'ailleurs, la Chine exerce ces menaces de manière subtile au moyen de tous les vecteurs possibles, qu'ils soient diplomatique, économique, social, culturel ou – évidemment – du renseignement. C'est ce qu'on appelle l'approche glo-

bale chinoise. Dans cette approche, où le concept de sécurité nationale a été encore élargi sous Xi Jinping, le rôle des services de renseignement s'est accru récemment. Les services de renseignement chinois – dont le principal service civil, le MSS – sont déjà présents dans tous les domaines de la société. Et vu qu'ils se sont vu renforcer en termes de capacités, la pression pour obtenir des résultats s'est accrue.

Dans le cadre de cette approche, une combinaison d'activités légitimes et d'activités clandestines est souvent constatée.

En termes d'ingérence, les objectifs de la Chine sont d'une part de former et de soutenir les groupes de décideurs en Europe qui pourront à leur tour tenter d'influencer le processus décisionnel à l'avantage de la Chine, et d'autre part de diviser les alliés occidentaux notamment en tentant d'abîmer les relations transatlantiques ou intra-européennes.

Si le comportement général a évolué, la VSSE n'a pas constaté récemment de modifications dans le modus operandi utilisé par les services de renseignement chinois en Belgique. Le recrutement ou même le traitement des personnes d'intérêt pour eux se fait souvent en Chine ou depuis la Chine comme nous avons pu le constater dans un dossier rendu en partie public fin 2022. Ce système diminue les risques pour les officiers de renseignement chinois qui ne doivent pas se rendre dans des pays «hostiles».

L'approche globale susmentionnée, selon laquelle tout acteur chinois, qu'il soit étatique ou non étatique, est obligé de collaborer avec les services de renseignement – à laquelle se rajoute un modus operandi subtil et difficile à détecter – complique naturellement le travail de notre service dans la détection d'activités de renseignements chinoises. Cela rend le travail de conscientisation des acteurs belges sur la menace encore plus important, afin d'augmenter notre résilience et ainsi permettre à chacun d'évaluer correctement la menace.

## ► LE RISQUE DES APPLICATIONS CHINOISES

Les applications chinoises qui ont attiré plusieurs fois l'attention au cours de l'année écoulée sont un bon exemple du mode de fonctionnement de la République populaire de Chine. Par le biais d'une application apparemment innocente (faire du shopping en ligne, regarder des vidéos amusantes), une masse de données sur les utilisateurs est collectée et stockée. Les dommages sont-ils directement visibles par les utilisateurs ? Non, mais ces données peuvent être utilisées à long terme. Par exemple, elles peuvent être utilisées pour infecter des smartphones, pour diffuser de la désinformation de manière plus efficace, pour renforcer ou réprimer certains discours, ou pour alimenter certains outils qui reposent sur de grandes quantités de données, comme l'intelligence artificielle. Conformément au cadre juridique en Chine, il n'y a aucun obstacle à l'utilisation de ces données par les services de renseignement chinois. Ils peuvent ainsi les utiliser pour, par exemple, cibler des personnes ou leurs proches à des fins d'espionnage ou d'ingérence. La prudence reste donc de mise. C'est pourquoi il est recommandé de ne pas installer d'applications qui ne sont pas nécessaires sur ses appareils professionnels ou ceux sur lesquels se trouvent des informations sensibles.



# L'HYDRE DE LA MENACE TERRORISTE DJIHADISTE

En 2024, la principale menace terroriste dans notre pays émane encore et toujours d'organisations terroristes djihadistes. Derrière ce constat – le même depuis plusieurs années déjà – se cachent d'importants développements et changements.



## ► L'EI AU KHORASAN

En Belgique, la menace du terrorisme djihadiste a encore pour source principale l'Etat islamique (EI), et en particulier sa filiale terroriste en Asie centrale dans la province du Khorasan (ISKP). Cette province historique du Khorasan se situe dans la région d'Asie centrale qui entoure l'Afghanistan, le Pakistan, l'Iran, le Tadjikistan, l'Ouzbékistan et le Turkménistan.

Comme on le craignait, ISKP est parvenu en 2024 à se profiler comme une organisation capable de mener des opérations terroristes plus complexes aussi bien à l'intérieur qu'à l'extérieur de son territoire. L'attentat perpétré par ISKP le 3 janvier 2024 à Kerman (Iran) qui a fait 96 morts lors d'un rassemblement organisé à la mémoire du comman-

dant de la Garde républicaine iranienne, en était le premier signe. Plus tard au cours de ce même mois, une attaque de moindre envergure tuait deux personnes en Turquie. Le 22 mars 2024, c'était au tour de la Russie d'être frappée par un attentat qui allait faire 145 morts au Crocus City Hall. Il s'agissait d'un des attentats les plus sanglants commis depuis les attentats de Paris du 13 novembre 2015.

ISKP est ainsi devenue la branche la plus dynamique de tout le réseau de l'EI. Bien que l'organisation ne contrôle aucun territoire au Pakistan et en Afghanistan, sa réputation bâtie sur ses actions sur le sol russe, turc et iranien lui permet de continuer à attirer de nouveaux moyens financiers et des sympathisants.

Si, au cours de l'année écoulée, ISKP a démontré sa volonté et sa capacité de mener des opérations par le biais de cellules centralisées, ISKP et l'EI en général restent également, grâce à leur propagande en ligne, des sources d'inspiration pérennes pour les *lone actors*. Leur propagande violente incite des individus à commettre des actions violentes qu'ils revendiquent par la suite. Des projets terroristes de sympathisants de ISKP ont également été déjoués en Europe occidentale au cours de l'année, notamment en Autriche le 7 août 2024. En Belgique, des perquisitions et arrestations dans le milieu des sympathisants de ISKP ont eu lieu à la veille de l'ouverture des Jeux olympiques de Paris en juillet 2024.

### ► L'EI EN SYRIE ET EN IRAK

Malgré la défaite du califat physique en Syrie et en Irak en 2019, des *Foreign Terrorist Fighters* (FTF) séjournent encore en divers endroits de la région. Certains ont également des liens avec notre pays : ils disposent par exemple de la nationalité belge ou ils sont partis de Belgique pour prendre part au djihad. Dans la grande majorité des cas, ces FTF « belges » étaient à l'époque partis en vue de rallier les rangs de l'EI, même si bon nombre d'entre eux ont finalement rejoint une pléiade de groupements djihadistes distincts.

L'implosion soudaine du régime de Bachar Al-Assad le 8 décembre 2024 en Syrie, à la suite de la progression rapide et inattendue des rebelles de Hayat Tahrir al-Sham (HTS), pourra également avoir des répercussions sur la situation sécuritaire belge dans les semaines et mois à venir.

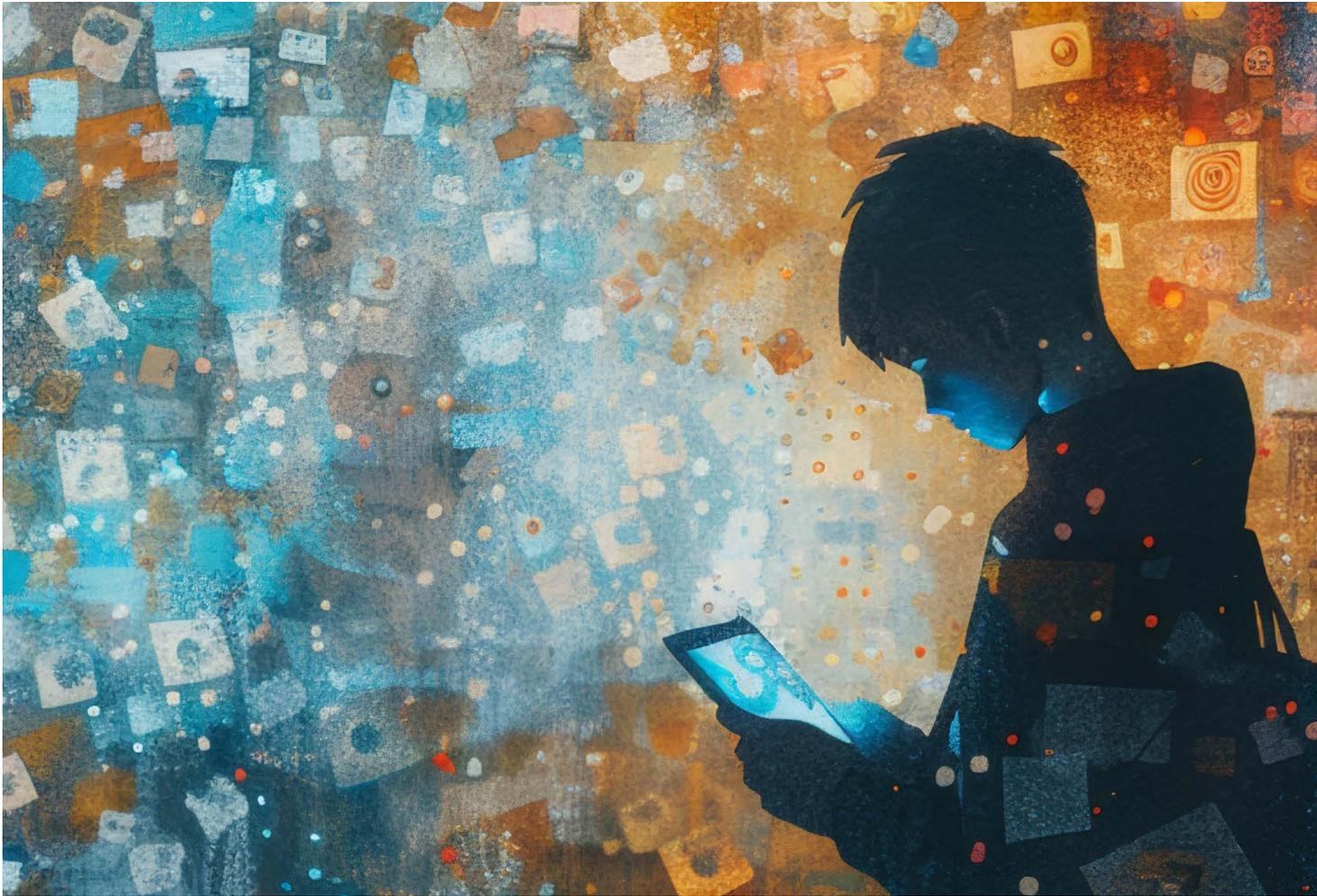
Selon les informations qui étaient en possession de la VSSE à la fin 2024, 13 hommes FTF en lien

avec la Belgique séjourneraient dans des prisons du nord-est de la Syrie contrôlées par des combattants kurdes. Les camps de Al-Hol et Al-Roj, situés dans cette même région, hébergeraient 8 femmes FTF et 9 enfants. Vingt-quatre autres combattants ayant des liens avec la Belgique et 48 enfants séjourneraient dans le nord-ouest de la Syrie. Une poignée de ces combattants soutiendraient le mouvement rebelle HTS ou en seraient membres. La VSSE est bien entendu particulièrement attentive au parcours de ces FTF. Une évolution rapide de la situation qui leur permettrait de regagner la Belgique de manière inaperçue et incontrôlée aurait un impact sur la situation sécuritaire de notre pays. Fin 2024, rien n'indiquait que l'EI était pleinement engagé sur le théâtre des opérations syrien, même si l'organisation peut encore compter sur de nombreux sympathisants dans la région au sens large et qu'une résurgence de l'EI ne peut être entièrement exclue.

### ► L'EI AU SAHEL ET EN SOMALIE

Sur le continent africain, à savoir dans la région du Sahel et dans la corne de l'Afrique, la force d'action des organisations terroristes augmente. Dans ces régions, des groupes liés à l'EI et à Al-Qaïda contrôlent un territoire important, ce qui leur permet de se regrouper et de renforcer leurs capacités. L'attaque coordonnée de l'EI en Somalie le 31 décembre 2024 en est un exemple récent. La VSSE ne dispose actuellement d'aucune indication permettant d'établir que la situation régionale aurait un impact direct sur la menace en Belgique. La VSSE suit la situation avec l'aide de ses partenaires belges et étrangers.

## PRÈS D'UN TIERS DES PERSONNES IMPLIQUÉES DANS LES DOSSIERS DE TERRORISME DE LA VSSE SONT MINEURES



**Entre 2022 et 2024, presque un tiers des personnes qui ont fomenté des projets d'attentats étaient âgées de moins de 18 ans. Le processus de radicalisation en ligne de ces jeunes est fulgurant. Détecter et s'attaquer à ces menaces à temps est une véritable gageure pour la VSSE et ses partenaires.**

Les services de renseignement et de sécurité belges sont de plus en plus confrontés à la présence de mineurs dans les dossiers de menace. Ce constat n'est pas nouveau, mais le phénomène semble s'intensifier.

Dans les dossiers de terrorisme de la VSSE des trois dernières années (de 2022 à fin 2024), près d'un tiers des personnes ayant échafaudé des projets d'actions violentes étaient mineures. Le plus jeune suspect arrêté en 2024 était âgé de 13 ans. L'âge moyen est d'environ 16 ans. Tous les mineurs qui projetaient de planifier des actions violentes étaient de sexe masculin.

### ► L'ISLAM RADICAL À L'ORIGINE DE 3 CAS SUR 4

Dans trois cas sur quatre environ, ces mineurs étaient portés par une version radicale de l'islam sunnite. Un quart des mineurs étaient guidés plutôt par une motivation d'extrême droite ou agissaient par hostilité envers l'*establishment*.

Le processus de radicalisation de ces mineurs a lieu en ligne, en général de manière particulièrement rapide. En effet, dans notre société actuelle hyperconnectée, le matériel de propagande extrémiste et terroriste se trouve à portée de clic de ces jeunes en quête d'identité ou d'un but dans l'existence. Outre la consommation de ce type de matériel de propagande, la VSSE constate que, dans certains dossiers, les mineurs produisent et diffusent eux-mêmes ce type de matériel.

La pression sociale s'avère être un facteur clé dans la radicalisation des mineurs. La VSSE observe que les mineurs radicalisés sont souvent membres d'un réseau (en ligne) ou d'un groupe de personnes partageant la même idéologie. Les jeunes de ces réseaux ont régulièrement et de plus en plus tendance à s'encourager mutuellement à consommer toujours plus de contenu, et toujours plus extrême. Il est par ailleurs très difficile de casser cette tendance sans briser les liens sociaux avec les autres membres du groupe.

La rapidité du processus de radicalisation explique que l'intention de passer à l'acte terroriste n'a souvent que peu de fondement idéologique. L'absence d'un cadre idéologique élaboré n'a toutefois aucun impact négatif sur la motivation des personnes impliquées. La VSSE constate dans un grand nombre de cas une apologie de la violence. Cette fascination pour la violence et les sujets violents est aussi souvent à l'origine de l'introduction de ces personnes dans les groupes problématiques (en ligne). Après un certain temps, les mineurs perçoivent la violence comme l'unique manière, et la plus efficace, d'atteindre leurs objectifs extrémistes. En raison de leur situation de dépendance, du contrôle parental et de l'absence d'accès à certaines plateformes, ces mineurs rencontrent en général fort heureusement bien plus de difficultés que les adultes à obtenir les moyens nécessaires à l'exécution de leur projet. Toutefois, cette situation n'empêche pas les organisations terroristes d'inciter ces jeunes influençables à commettre des actions violentes.

Détecter ces menaces à temps représente dès lors un défi pour les services de renseignement et de sécurité. En effet, les mineurs en question sont généralement de parfaits inconnus avant de se retrouver dans le collimateur des services de renseignement. Établir une distinction entre des jeunes n'ayant qu'un discours radical derrière leur clavier et d'autre part, des individus posant une menace réelle, demeure une évaluation complexe et chronophage pour un service de renseignement.

Outre la VSSE et les autres acteurs de la sécurité, les partenaires sociopréventifs – tels que les Cellules Locales de Sécurité Intégrale (CLSI) et les communes – jouent dans ce domaine un rôle important.

## LA PROPAGANDE EXTRÉMISTE ENCOURAGE LES *LONE ACTORS* À AVOIR RECOURS À LA TERREUR



**La propagande extrémiste est un important catalyseur qui incite les *lone actors* à commettre des actions violentes. C'est ainsi qu'en dépit de la perte de son califat, l'État islamique (EI) demeure la principale source d'inspiration pour les projets d'attentat en Belgique, grâce à sa machine de propagande en ligne. Une analyse de la VSSE révèle que les téléphones de djihadistes saisis en Belgique contiennent souvent des quantités impressionnantes de propagande extrémiste.**

En termes d'ampleur, le djihadisme sunnite reste de loin la principale menace d'action violente en Belgique. Cette menace peut provenir de l'extérieur, mais également de l'intérieur des frontières de notre pays. Dans les deux cas, la propagande extrémiste joue souvent un rôle de catalyseur majeur.

Cela ressort d'une enquête de la VSSE sur une cinquantaine de téléphones et autres appareils électroniques saisis chez des individus dans de dossiers de terrorisme djihadiste. Dans 72 % de ces

appareils, une énorme quantité de propagande de l'EI a été trouvée. Dans une moindre mesure, cela concernait de la propagande d'Al-Qaida.

Tant l'État islamique qu'Al-Qaida disposent toujours en 2024 d'un appareil de propagande solide et étendu. Malgré la fin du califat territorial en Syrie, l'EI reste en mesure de mettre en œuvre le pouvoir de mobilisation de son idéologie. Dans ce sens, l'EI continue dès lors d'exister en tant que califat « en ligne ». L'organisation reste ainsi la principale source d'inspiration pour des projets d'attentat

dans notre pays et ailleurs en Occident, comme l'a montré l'attentat commis le jour de l'An à la Nouvelle-Orléans aux États-Unis.

Al-Qaida reste également actif sur internet et dans les médias sociaux, avec un réseau de propagande qui ne cesse de se développer. Tant l'EI qu'Al-Qaida sont très habiles lorsqu'il s'agit de recycler et réutiliser l'ancien matériel de propagande, mais ils sont encore maintenant en mesure de produire du nouveau matériel. Ces deux organisations s'appuient ainsi sur des médias officiels et non officiels pour diffuser leur propagande. Elles ont bâti, chacune à leur manière, un écosystème en ligne qui, en 2024 encore, continue d'attirer des visiteurs du monde entier. Si, en termes de contenu, Al-Qaida opte pour des narratifs idéologiques fouillés, l'EI choisit plutôt des images violentes et choquantes.

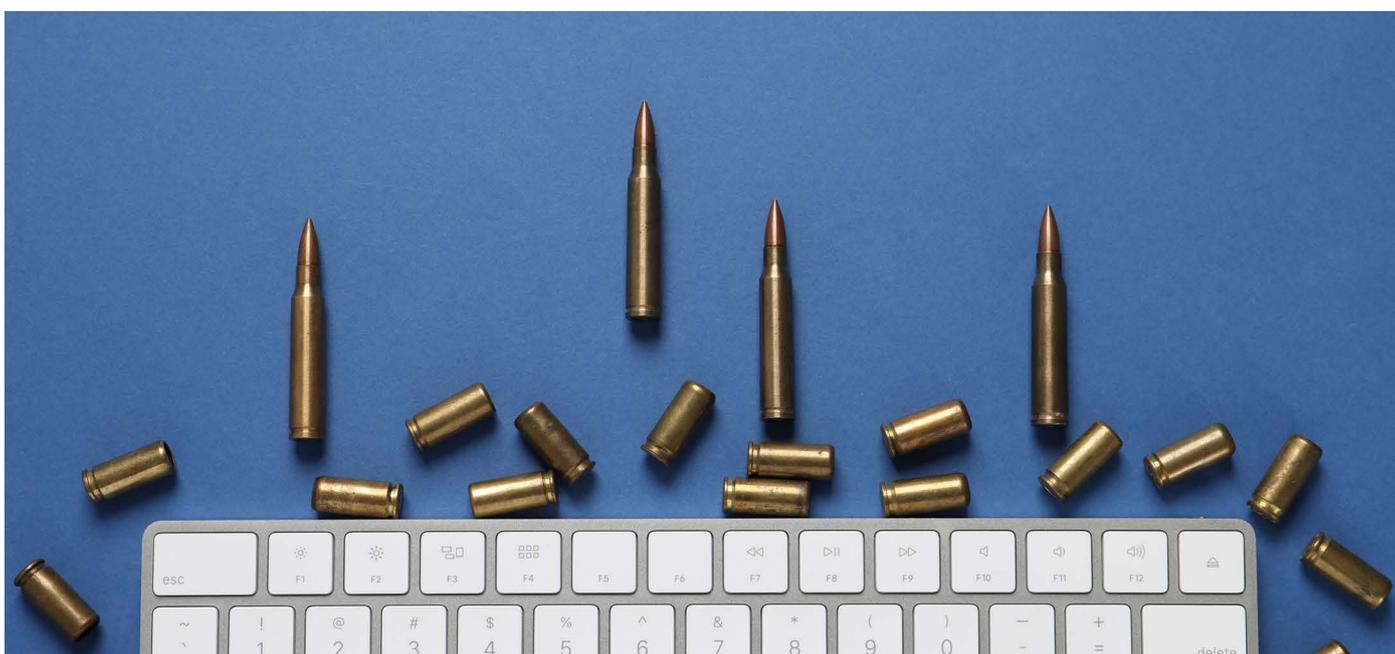
Via leur propagande, des groupements terroristes tels qu'Al-Qaida et l'EI visent plusieurs objectifs : répandre leur idéologie, radicaliser et recruter des individus, récolter des fonds, mais aussi et surtout inspirer les jeunes et les inciter à commettre des attentats terroristes.

Cette approche porte ses fruits, comme en témoigne une analyse des supports électroniques des djihadistes en Belgique. Dans la grande majorité des cas, une propagande extrémiste est retrouvée (souvent en énorme quantité) sur leurs téléphones et autres dispositifs électroniques.

### ► ALGORITHME

Les algorithmes des principaux réseaux sociaux publics comme YouTube, TikTok ou Facebook constituent un problème supplémentaire. Ils créent un effet d'attraction en proposant de plus en plus rapidement et de manière de plus en plus extrême des vidéos ou d'autres contenus à des personnes effectuant des recherches en ligne sur des sujets radicaux. Par ces méthodes, les individus se retrouvent parfois, sans en être pleinement conscients, dans un véritable *rabbit hole* numérique dont il est très difficile de s'échapper.

Une autre tendance problématique est le phénomène où des utilisateurs, souvent jeunes, sont dirigés vers des groupes de discussion ou des canaux sur des plateformes comme Telegram, où un narratif extrémiste plus spécifique est partagé. Dans les cas les plus préoccupants, des matériels de propagande violente et des manuels terroristes sont explicitement partagés dans ces groupes de discussions privés.



# LES CONFLITS AU MOYEN-ORIENT ET LEUR IMPACT EN BELGIQUE



En 2024, la guerre entre le Hamas et Israël s'est aggravée et a ravivé le conflit entre Israël et le Hezbollah au Liban. La chute fin de l'année du régime du dictateur syrien Bachar al-Assad ouvre la porte à des mutations considérables dans la région, avec des implications possibles pour notre pays.

## ► SYRIE

L'implosion soudaine et inattendue du régime de Bachar al-Assad le 8 décembre 2024 en Syrie, à la suite de la progression des rebelles de Hayat Tahrir al-Sham, pourra entraîner des changements rapides dans l'ensemble de la région au cours des mois à venir. Cette situation risque d'impacter le sort des *Foreign Terrorist Fighters* liés à la Belgique se trouvant dans des prisons et des camps au nord-est de la Syrie, mais également les aspirations territoriales de plusieurs groupements djihadistes en Syrie. Une résurgence de l'EI n'est pas complètement à exclure. Avec son réseau de partenaires internationaux et le SGRS, la VSSE suit de près la situation sur place.

## ► GAZA ET LIBAN

L'escalade du conflit entre Israël et le Hamas à Gaza et en Cisjordanie ainsi que la résurgence de la guerre entre Israël et le Hezbollah libanais influencent également les sociétés belge et européenne. Les événements survenus au Moyen-Orient sont un catalyseur de la radicalisation, et sont déjà à l'origine d'actions violentes dans plusieurs pays européens, telles que les rixes qui ont opposé le 7 novembre 2024 les supporters de football israéliens et de jeunes propalestiniens dans les rues d'Amsterdam. Quelques jours plus tard, une poignée de jeunes qui prévoyaient une action violente contre la communauté juive ont été arrêtés à Anvers. En Suède et au Danemark, les ambassades israéliennes ont été la cible de coups de feu ou de lancements de grenade à main.

Des organisations terroristes telles que l'EI et Al-Qaïda exploitent le conflit au Moyen-Orient dans leur matériel de propagande afin de renforcer leur message djihadiste et recruter des sympathisants. Cela pourrait également inciter des personnes à commettre des actions violentes en Belgique.

## ► HAMAS ET HEZBOLLAH

Le Hamas figure sur une liste européenne des organisations terroristes, la VSSE estime cependant qu'il est très peu probable que le Hamas commette un attentat sur le sol belge. Si le risque de violence existe, il émane plutôt de *lone actors* radicalisés, motivés par le conflit à Gaza.

Le Hamas est, certes, actif également en Belgique, mais ses actions consistent principalement à faire du lobbying au sein d'institutions belges et internationales et à chercher un financement. Il s'agit d'activités qui ne présentent pas une menace directe de violence, mais qui n'en sont pas moins problématiques et qui constituent même parfois une infraction pénale lorsqu'il s'agit de financement d'une organisation terroriste.

Aucune menace terroriste directe pour la Belgique n'émane non plus du Hezbollah libanais. Dans notre pays, le Hezbollah est principalement actif au sein de la diaspora libanaise dans le but de récolter des fonds. La VSSE et ses partenaires nationaux et internationaux suivent de près ces activités. ■

# MENACE DE L'EXTRÉMISME RELIGIEUX ET IDÉOLOGIQUE

Outre le terrorisme, l'extrémisme constitue également une menace pour notre société démocratique. Certaines formes d'extrémisme religieux et idéologique peuvent entraîner dans certains cas une radicalisation accrue qui aboutit à la violence.



## ► FRÈRES MUSULMANS

Les Frères musulmans constituent un mouvement hétérogène qui ne représente pas une menace de violence en Belgique. Toutefois, La VSSE constate qu'au sein des sympathisants des Frères musulmans en Belgique, une centaine d'individus tentent de répandre activement une idéologie qui peut conduire à la radicalisation et promouvoir l'extrémisme.

Les Frères musulmans se distinguent des autres mouvements islamistes extrémistes par leurs activités de lobbying destinées à influencer la politique gouvernementale concernant l'islam, et par leur méthodologie basée sur la création d'organisations destinées à avoir une emprise sur la communauté musulmane.

De manière clandestine, des groupements faisant

partie de la sphère d'influence des Frères musulmans tentent d'exercer un lobbying afin qu'une place plus importante soit accordée à l'islam dans la société. Pour ce faire, ces groupements dissimulent leurs liens avec les Frères musulmans en se faisant passer pour des représentants légitimes de la communauté musulmane en Belgique. Ils souhaitent ainsi s'arroger une place au sein des institutions belges et obtenir un financement pour leurs diverses initiatives.

L'objectif à long terme des Frères musulmans consiste à instaurer une société dans laquelle chaque aspect de la vie est régi par la norme religieuse. À court et moyen termes, leur discours participe à l'instauration d'un climat de ségrégation et de polarisation, qui constitue à son tour un terrain propice à la radicalisation.

Bien que le soutien étranger que reçoivent les Frères musulmans en Belgique se soit affaibli, on peut supposer que le mouvement y poursuivra ses activités.

### ► **LONE ACTORS D'EXTRÊME DROITE**

La principale menace qui émane à l'heure actuelle de l'extrémisme de droite en Belgique est la diffusion de sa propagande. À long terme, ce phénomène pourrait potentiellement saper la confiance dans les institutions, l'ordre et les processus démocratiques du pays.

La VSSE estime que le risque d'attentat terroriste diligenté par des groupements d'extrémisme droite est plutôt faible.

Si une action violente devait malgré tout être commise par les milieux de l'extrémisme de droite, celle-ci serait probablement l'œuvre de jeunes *lone actors* qui se radicalisent généralement en ligne. Certains d'entre eux trouvent leur inspiration dans la doctrine de l'accélérationisme. Cette doctrine part du principe que la lutte raciale ou la guerre religieuse est inévitable à terme, et que cette guerre doit idéalement être déclenchée ou accélérée par la violence terroriste. En effet, les militants accélérationnistes d'extrême droite croient inébranlablement que la race blanche finira par l'emporter en raison de sa supposée supériorité. Le nombre de partisans de l'accélérationisme reste néanmoins limité en Belgique.

### ► **FORTE MOBILISATION DE L'EXTRÊME GAUCHE**

D'expérience, nous savons que les groupes d'extrême gauche peuvent être impliqués dans des actes de sabotage et des tactiques de *black block*. Cependant, au cours de l'année écoulée, ce sont principalement des occupations de bâtiments, des actes de vandalisme et d'intimidation qui ont été constatés, souvent dans le contexte de leur engagement accru et de leur mobilisation autour du conflit à Gaza. Les élections se sont également révélées être un thème mobilisateur pour les extrémistes de gauche. Pour élargir leur base de soutien, ils tentent généralement de s'emparer de sujets d'actualité, tels que la question climatique.

Les actions des extrémistes de gauche en Belgique se concentrent actuellement principalement sur le recrutement, les manifestations et la diffusion de leurs messages via leur propagande en ligne et hors ligne. Cependant, certains au sein du milieu d'extrémisme de gauche considèrent la violence comme un moyen légitime pour atteindre leurs objectifs. Sur base des informations disponibles, la VSSE évalue cependant comme improbable la préparation et la planification d'attentats par ce milieu.



# LA VSSE ET LE SGRS TRANSMETTENT CHAQUE SEMAINE DES DOSSIERS TERRORISME À LA POLICE ET AU PARQUET



Dans le cadre de la lutte contre le terrorisme et l'extrémisme, la VSSE et le SGRS coopèrent étroitement et depuis plusieurs années déjà au sein d'une plateforme commune. Pratiquement chaque semaine, cette plateforme soumet des dossiers de terrorisme à la police et au parquet. En 2024, les deux services de renseignement ont été désignés en tant qu'« assistant technique » dans 33 enquêtes pénales liées au terrorisme.

Depuis les attentats de mars 2016 et la commission d'enquête parlementaire constituée dans la foulée, le monde du renseignement et de la sécurité a basculé pour passer du *need to know* au *need to share*. Des *Joint Centers* ont été ainsi mis en place ces dernières années afin d'assurer une circulation fluide des informations entre les différents services actifs dans les domaines du renseignement et de la sécurité, tels que l'OCAM, les services de police, le ministère public et les services de renseignement.

Si la police et le parquet se concentrent sur la recherche d'infractions, la collecte de preuves et la poursuite de personnes, les services de renseignement se focalisent sur les menaces et la collecte de renseignements avant qu'il ne soit question d'infractions. Ces finalités n'en demeurent pas moins complémentaires et mènent à une interaction permanente entre les différents acteurs.

## ► LA PLATEFORME CECT : LE POINT DE CONTACT CENTRAL EN MATIÈRE DE TERRORISME ET D'EXTRÉMISME DU SGRS ET DE LA VSSE

Depuis plusieurs années déjà, les collaborateurs de la VSSE et du SGRS luttent ensemble contre la menace terroriste djihadiste, au sein de la Plateforme CT ou Plateforme contre-terrorisme. Depuis 2024, cette collaboration s'est étendue à l'ensemble des dossiers d'extrémisme et terrorisme d'inspiration religieuse et idéologique. L'ancienne plateforme CT s'est ainsi muée en 2024 en une nouvelle plateforme, intitulée Plateforme CECT (Plateforme contre-extrémisme et contre-terrorisme).

La plateforme CECT constitue un *single point of contact* pour les partenaires nationaux impliqués dans ces matières. Via cette plateforme, la VSSE et le SGRS envoient des analyses et notes de renseignement communes aux services partenaires nationaux et internationaux. Les deux services de renseignement s'expriment ainsi d'une seule et même voix en matière de terrorisme et d'extrémisme. Parallèlement, la plateforme commune CECT peut exploiter la capacité et les moyens de collecte propres à chacun de ces services.



Dans la pratique, cette coopération se traduit par un partage de renseignements en lien avec le terrorisme et l'extrémisme par le biais de notes de la Plateforme CECT adressées à la police et au ministère public. Ainsi, des renseignements qui permettent d'ouvrir des enquêtes judiciaires ou de contextualiser des enquêtes en cours sont fournis.

Lorsque de nouvelles informations pertinentes en matière de terrorisme sont disponibles, le service concerné en informe le *Joint Intelligence Center* (JIC). Ce dernier se compose de membres de la police judiciaire fédérale, de l'unité centrale anti-terrorisme de la Police Fédérale, de l'OCAM et de la Plateforme CECT. Ces services examinent ensuite ensemble les nouvelles informations, procèdent à une évaluation commune et formulent ensuite une proposition de suivi adéquat : une enquête pénale, une enquête de renseignement ou un autre type de suivi. Cette décision doit enfin être validée par le *Joint Decision Center* (JDC). Celui-ci se compose des mêmes membres que le JIC, complétés par des membres du parquet local, du parquet fédéral et du directeur-coordonateur administratif de la Police Fédérale.

## ► 50 DOSSIERS TERRORISME

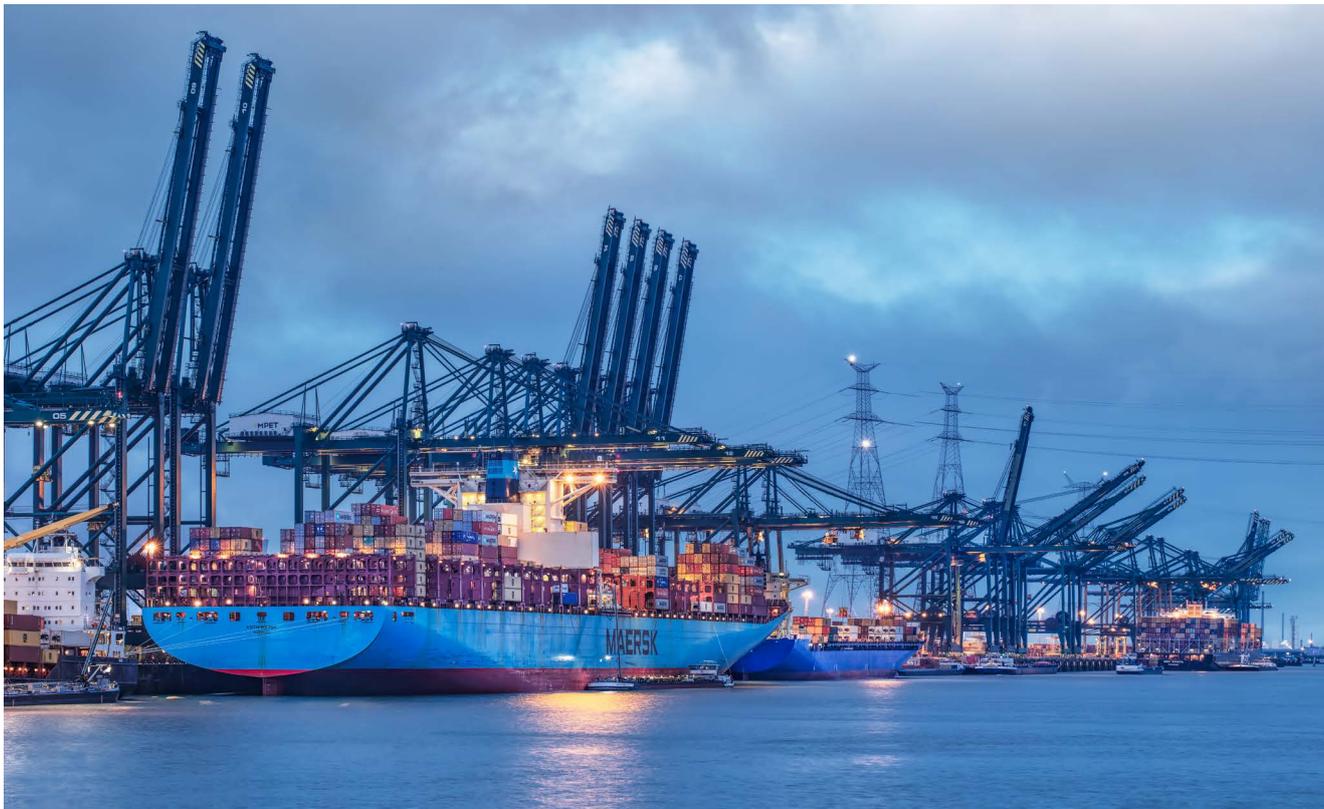
En 2024, la Plateforme CECT a signalé aux JIC 50 dossiers de renseignement en lien avec le terrorisme. Au total, 114 JIC ont été organisés l'année dernière. En d'autres termes, une petite moitié des dossiers terrorisme traités par un JIC ont été introduits par la VSSE et le SGRS. La plupart des autres dossiers ont été soumis par les différentes entités de la Police Fédérale. Il n'est pas surprenant que le pourcentage de dossiers issus des services de renseignement y soit relativement élevé ; leur finalité est en effet précisément de détecter les menaces à un stade précoce.

Parmi les 50 dossiers de renseignement en matière de terrorisme amenés par la plateforme CECT en 2024, il a été question, dans 22 cas, d'informations concernant une menace violente. Les 28 autres dossiers concernaient plutôt la propagande ou le financement du terrorisme. Les 50 dossiers soumis par la Plateforme CECT ont mené à l'ouverture de 29 enquêtes pénales. 15 autres dossiers sont restés au niveau d'enquête de renseignement.

Une fois l'enquête pénale initiée, les services de renseignement peuvent être désignés en tant qu'assistant technique. Cela est automatiquement le cas pour chaque dossier terrorisme du parquet fédéral. Cela signifie que les services de renseignement ont accès au dossier judiciaire et peuvent mettre leurs connaissances et expertise au profit de l'enquête. En 2024, la VSSE et le SGRS ont ainsi été désignés en tant qu'assistant technique dans 33 dossiers terrorisme.

Toutefois, le travail des différents services ne s'arrête pas au terme de l'enquête pénale. Il est en effet nécessaire d'assurer le suivi adéquat de ces dossiers par le biais des différentes plateformes de concertation. Ce suivi s'effectue notamment au niveau de l'arrondissement judiciaire. La plateforme CECT fournit ainsi un input permanent aux *Task Forces* locales dans le cadre de la stratégie TER, la stratégie commune contre le terrorisme et l'extrémisme. ■

# LA VSSE CONTRIBUE À LA LUTTE CONTRE LE CRIME ORGANISÉ



**L'approche du crime organisé en Belgique implique en premier lieu une perspective policière et judiciaire, à laquelle se greffe de plus en plus souvent une approche administrative au niveau local. En tant que service de renseignement, la VSSE fournit un appui supplémentaire aux partenaires nationaux.**

La VSSE enquête en premier lieu sur des individus et des réseaux qui déploient des activités susceptibles de porter atteinte à l'État, à savoir la violence ou la corruption visant des agents de l'Etat ou des secteurs vulnérables, tels que les infrastructures critiques de notre pays. Elle partage ainsi les informations pertinentes avec la police et la justice, via les procédures habituelles de collaboration.

En 2024, des signaux positifs ont permis d'observer que la lutte contre le crime organisé lié à la drogue commençait à porter ses fruits. Toutefois, les victoires engrangées par la justice, qui ont conduit à de nombreuses condamnations, ont exercé une grande pression sur notre système pénitentiaire. La VSSE fait valoir son expertise spécifique du milieu carcéral pour détecter les menaces susceptibles d'y émerger. En coopération avec ses partenaires tels que l'administration pénitentiaire, elle tente par ailleurs de déceler les menaces que le crime organisé fait peser sur le personnel pénitentiaire.

Avec l'appui de ses partenaires, la VSSE anticipe également l'extradition vers la Belgique de grands barons de la mafia internationale de la drogue. Plusieurs *High Value Targets* (HVT) ont ainsi été arrêtées à l'étranger au cours des derniers mois de 2024. Les autorités judiciaires demandent leur extradition dans le cadre des poursuites judiciaires et de l'exécution de leur peine dans notre pays, mais cette extradition éventuelle implique également des risques pour la sécurité. En collaboration avec la Police Fédérale, notre service examine dès lors la meilleure manière de contenir ces risques, en cherchant prioritairement à prévenir la poursuite de ces activités criminelles en prison. Nos services s'attèlent notamment à trouver l'établissement pénitentiaire et le régime de détention adaptés pour ces HVT.

La VSSE a également renforcé sa présence dans les ports belges afin d'accroître la résilience des acteurs et des processus utilisés face aux aspects subversifs du crime organisé.

# 02

**LA VSSE COMME SERVICE DE SÉCURITÉ**

## LA VSSE TRAVAILLE AU RENFORCEMENT DE LA CULTURE DE SÉCURITÉ



**La VSSE, ainsi que l’Autorité Nationale de Sécurité (ANS) qui fait partie de la VSSE depuis le 1<sup>er</sup> janvier 2024, travaille à renforcer la culture de la sécurité, tant à l’intérieur qu’à l’extérieur de ses murs.**

Au niveau national, la VSSE est en contact permanent avec un réseau d’officiers de sécurité aussi bien au sein d’administrations ou d’organismes publics que d’entreprises privées. C’est l’ANS qui, avec d’autres départements de la VSSE, a la tâche de leur fournir des avis, de la guidance et des directives sur les différentes dimensions de la sécurité. De cette manière, ils travaillent au renforcement de la culture de la sécurité.

- **Politique de sécurité** : la VSSE soutient le développement de politiques de sécurité robustes au sein des organisations publiques et privées permettant une gestion des risques. La VSSE effectue également régulièrement des sensibilisations autour de cette problématique. L’ANS a ainsi organisé en 2024 des événements à destination des officiers de sécurité. Ces événements ont vu la participation de près de 500 d’entre eux issus tant du secteur public que privé.
- **Sécurité de l’information** : l’ANS s’assure de la protection des informations sensibles et des informations classifiées, réagit en cas d’incident de sécurité et établit des directives de gestion de ces informations.
- **Sécurité du personnel** : l’ANS – avec d’autres départements de la VSSE – accompagne ses partenaires dans les demandes d’habilitation de sécurité. La VSSE mène avec le SGRS les enquêtes de sécurité

sur les personnes demandant une habilitation afin de s’assurer de garanties suffisantes de loyauté, d’intégrité et de discrétion dans leur chef.

- **Sécurité physique et technologique** : l’ANS joue un rôle dans la certification de certains systèmes d’information et de communication, de bâtiments ou de zones sensibles. Par ailleurs, l’ANS conseille ses partenaires sur la protection de leurs informations, par exemple lors de voyage dans des pays à risques.

Ces différentes missions, qui ont déjà été renforcées suite à l’intégration de l’Autorité Nationale de Sécurité au sein de la VSSE, ne feront que s’accroître dans les années à venir.

La VSSE a également fait un travail de renforcement de la culture de sécurité au sein de ses propres murs, pour son propre fonctionnement. Cela a certainement eu des conséquences pour le personnel, par exemple pour ce qui concerne l’utilisation de matériel électronique personnel ou en lien avec la nécessaire discrétion que les collaborateurs d’un service de renseignement doivent nécessairement avoir, y compris dans leur cercle familial proche.

Via sa politique de sécurité, la VSSE souhaite être un exemple pouvant inspirer les partenaires des secteurs public et privé.

# L'ANS A DÉLIVRÉ PRÈS DE CINQ FOIS PLUS D'HABILITATIONS DE SÉCURITÉ EN CINQ ANS

L'Autorité Nationale de Sécurité (ANS) fait partie de la VSSE depuis le 1<sup>er</sup> janvier 2024. Avec l'intégration de l'ANS, la VSSE entend améliorer sensiblement la culture de sécurité en Belgique. Dans ce contexte, l'ANS a délivré près de 12.000 habilitations de sécurité en 2024, soit pratiquement cinq fois plus qu'en 2020.

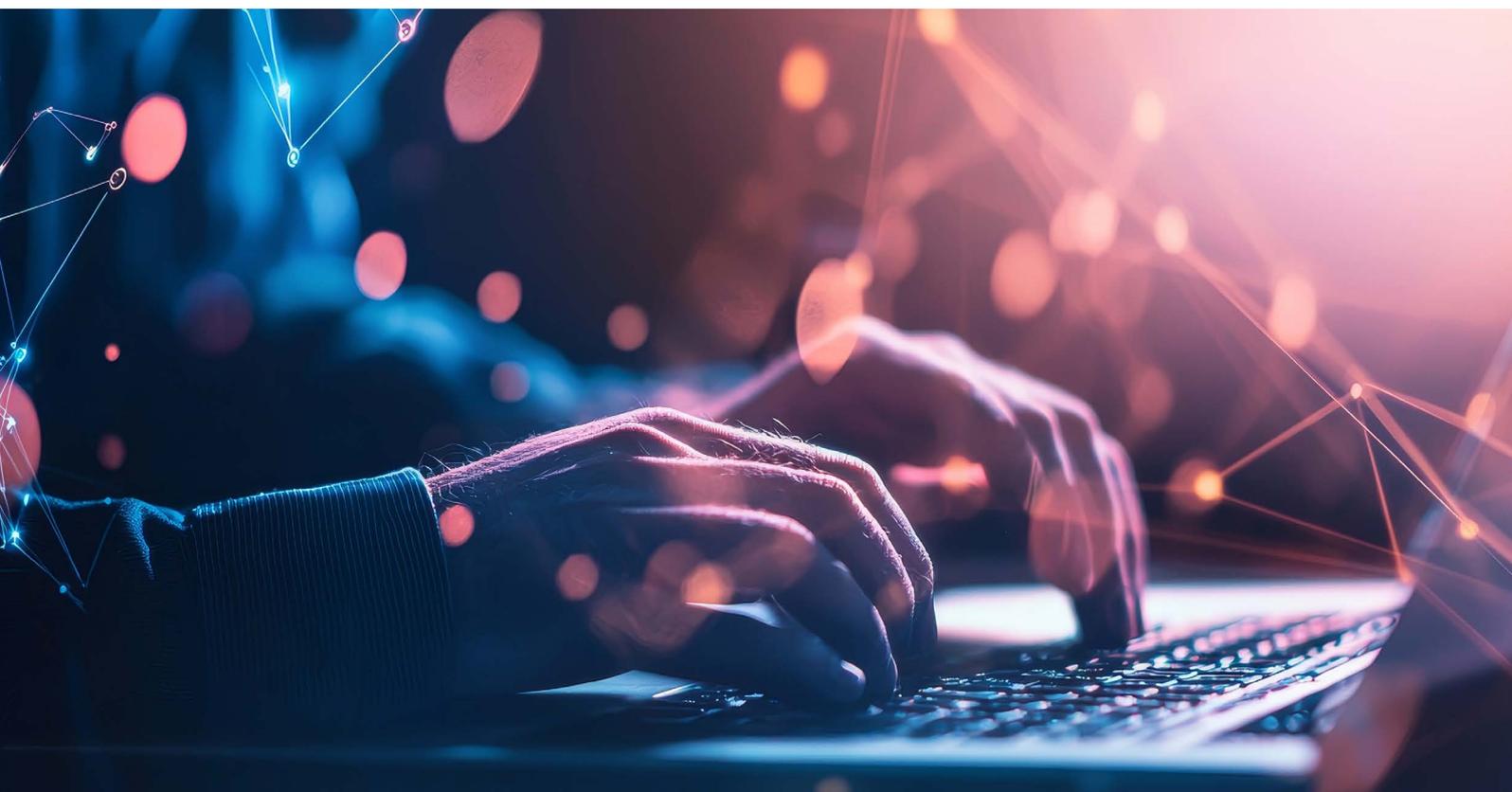
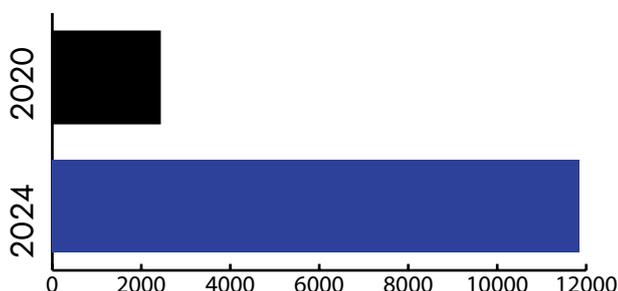
La VSSE est un service de renseignement et de sécurité. Ce pilier sécurité a été considérablement renforcé ces dernières années, notamment par l'intégration de l'ANS. Celle-ci a longtemps fait partie du SPF Affaires étrangères, mais en février 2022, le Conseil National de Sécurité a décidé de la réformer. Cette réforme prévoyait que la compétence de l'ANS liée aux vérifications de sécurité soit octroyée à la Police Fédérale. L'ANS en tant que telle, le personnel (une vingtaine de personnes) et les autres compétences – entre autres donc la délivrance d'habilitations de sécurité aux personnes et sociétés qui traitent des informations classifiées – a été transférée à la VSSE.

## ► 40 COLLABORATEURS

Depuis que l'ANS opère sous la bannière de la VSSE, le service a été sensiblement renforcé. Ainsi l'ANS compte à ce jour 40 collaborateurs, qui ont travaillé d'arrache-pied au cours de l'année écoulée pour améliorer la réactivité et actualiser le cadre légal très obsolète, les directives et les procédures.

En 2024, l'ANS a traité pas moins de 15.366 demandes d'habilitation de sécurité individuelles. Au final, 11.840 habilitations ont été délivrées. Le nombre d'habilitations de sécurité octroyées a plus que doublé en l'espace de deux ans. À titre de comparaison, seules 2.428 habilitations de sécurité individuelles avaient été délivrées cinq ans plus tôt, en 2020.

En outre, en 2024, l'ANS a traité 1.271 demandes d'habilitation de sécurité pour des personnes morales privées et publiques et 485 habilitations de sécurité ont été délivrées afin de leur permettre de traiter des informations classifiées.



## LES VÉRIFICATIONS DE SÉCURITÉ EFFECTUÉES PAR LA VSSE EN HAUSSE DE 36 %

En 2024, la VSSE a réalisé 327.608 vérifications de sécurité, soit une hausse de 36 % par rapport à l'année précédente. Et la sensibilité accrue aux questions de sécurité laisse supposer que le nombre de vérifications ne cessera d'augmenter à l'avenir.

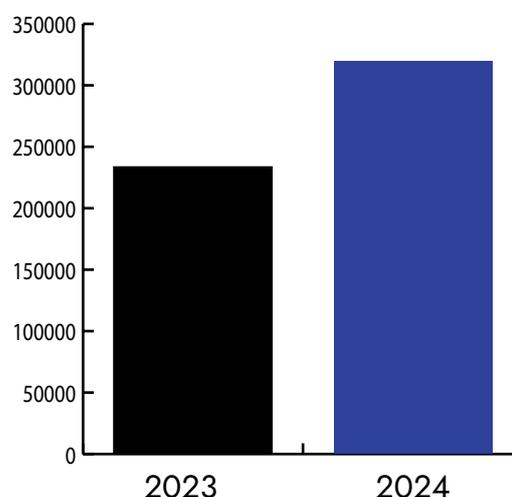
Les vérifications de sécurité consistent en une série de contrôles préalables pour exclure les personnes qui constitueraient un potentiel risque de sécurité des fonctions sensibles, ou leur interdire l'accès à des zones sensibles. Des exemples classiques sont les personnes qui travaillent dans les zones de sécurité des aéroports ou dans le secteur nucléaire. De telles vérifications interviennent également dans le cadre des demandes de nationalité belge, d'asile ou de regroupement familial.

En raison de la diversité des types de vérification de sécurité, la VSSE est sollicitée par un grand nombre de partenaires pour les effectuer. Le partenaire le plus important est toutefois la Police Fédérale qui est responsable depuis le 1<sup>er</sup> janvier 2024 du traitement des vérifications sur base de la loi sur la classification de 1998.

En 2024, la VSSE a effectué au total 327.608 vérifications. C'est une augmentation d'environ 36 % par rapport aux 241.197 vérifications de 2023.

D'où provient cette augmentation considérable avoisinant les 36 % ? Pour les badges aéroportuaires, une nouvelle vérification a désormais lieu chaque année contre tous les cinq ans auparavant. De plus, le nombre de demandes de vérifications dans le cadre des procédures pour obtenir la nationalité belge est en forte progression, à l'instar des demandes de vérifications dans le cadre des demandes d'asile et de regroupement familial. Les vérifications menées dans le cadre de sommets européens ou de l'OTAN continuent également d'augmenter. Enfin, toujours plus de nouveaux secteurs, comme les établissements pénitentiaires ou les ports maritimes, sont soumis à des vérifications de sécurité.

Compte tenu de la situation géopolitique et de la prise de conscience actuelle dans notre société pour traiter la sécurité d'une manière responsable, cette tendance à la hausse devrait se poursuivre au cours des prochaines années.



# LA VSSE A FORMULÉ 86 AVIS SUR DES INVESTISSEMENTS DIRECTS ÉTRANGERS

La procédure de screening des investissements directs étrangers (FDI) est d'application en Belgique depuis 2023. La procédure a connu en 2024 sa première année calendrier complète. Durant celle-ci, la VSSE a rédigé au bénéfice du Comité de Coordination du Renseignement et de la Sécurité (CCRS) des avis rassemblant les positions de chacun des partenaires impliqués. Ainsi en 2024, ce sont 86 avis sur les aspects de sécurité et de renseignement qui ont été remis au Comité de filtrage interfédéral.



Dans un contexte géopolitique toujours plus complexe et volatil, il est essentiel que la Belgique développe des mécanismes contribuant à lui assurer une certaine sécurité et autonomie économique, tout en conservant une ouverture vers l'extérieur.

Bien que la grande majorité des investissements étrangers vérifiés n'ont pas été considérés comme représentant une menace, certains investissements ont nécessité néanmoins de plus amples vérifications afin que le CCRS puisse rendre son avis en toute connaissance de cause. Cela concerne plus particulièrement les investissements dans une société belge par des personnes ou des sociétés extérieures à l'Union européenne. Seuls les investissements dans certains secteurs stratégiques, tels que les infrastructures critiques, la haute technologie ou les fournisseurs de la Défense sont contrôlés. Enfin, le filtrage n'a lieu que si au moins 10 à 25 % des actions de l'entreprise belge risquent de se retrouver dans des mains étrangères.

Dans la pratique, une procédure de filtrage n'a été ouverte que dans un peu moins de 10 % des dos-

## ► PROCÉDURES DE SCREENING FDI

La tâche principale consiste à analyser les investissements directs étrangers et évaluer s'ils présentent des risques potentiels pour la sécurité nationale et les intérêts stratégiques du pays.

siers. Il s'agit de ce que l'on appelle la deuxième phase de filtrage. La VSSE a dévolu des capacités propres spécifiques pour enquêter sur ces investissements. Ce choix stratégique a permis à la VSSE d'être une force motrice dans ce nouvel enjeu de sécurité économique national.

Au total, 86 avis ont été émis en 2024. Plus que jamais, il est primordial d'identifier les menaces potentielles et de prendre des mesures préventives pour contribuer à augmenter la résilience des secteurs nationaux sensibles, tels que les infrastructures critiques, les technologies de pointe et l'énergie.



# 03

**À PROPOS DE LA VSSE**

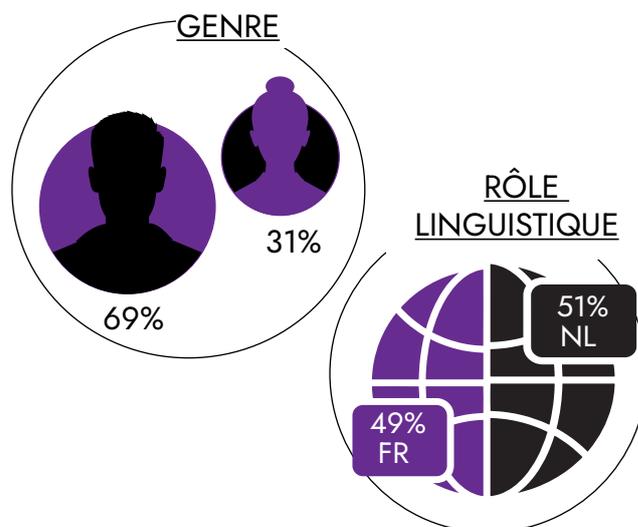
# LES CHIFFRES DE LA VSSE EN 2024

## ► RESSOURCES HUMAINES

# 954

### COLLABORATEURS

Ces dernières années, la VSSE a connu une transformation radicale. En 4 ans, le nombre de collaborateurs a presque doublé. Attirer, accueillir, intégrer et former en interne des centaines de nouveaux collègues s'est apparenté à un véritable « tour de force ».



## ► ÉCHANGE DE RENSEIGNEMENTS

# 43.366

### MESSAGES ENTRANTS

Les messages entrants émanent de partenaires nationaux tels que le SGRS, la Police Fédérale, l'OCAM, le Centre de crise National (NCCN), le SPF Affaires étrangères, l'administration pénitentiaire ou les parquets. Par ailleurs, une part significative du flux d'informations entrant provient de services de renseignement étrangers. En comparaison, en 2020, la VSSE a reçu 29.148 messages entrants.

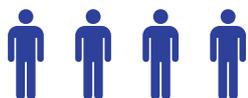
# 1.492

### RÉUNIONS DE COORDINATION AVEC DES PARTENAIRES

En 2024, la VSSE a rédigé 1492 rapports de réunions de coordination où des renseignements ont été échangés avec des partenaires locaux, nationaux et internationaux.

## ► RELATIONS INTERNATIONALES

### OFFICIERS DE LIAISON



À l'étranger



Auprès d'institutions multilatérales (OTAN/EU/Représentation permanente auprès de l'UE)



Le travail de renseignement est plus que jamais un phénomène international : les menaces ne s'arrêtent pas aux frontières nationales et les autres pays sont également confrontés à des défis similaires. Afin d'optimiser l'échange d'informations, la VSSE continue à investir dans son réseau d'officiers de liaison à l'étranger et auprès des institutions multilatérales à Bruxelles.

# LA VSSE DÉCLASSIFIE SES ARCHIVES SUR LA SECONDE GUERRE MONDIALE

Au cours de l'année écoulée, la VSSE a déclassifié en grande partie ses archives concernant la période de la Seconde Guerre mondiale et les a préparées pour leur transfert aux archives générales du Royaume. Les archives de la VSSE sont aussi consultées de manière croissante. C'est ainsi que plus de 250 demandes de consultation ont été introduites en 2024 via le Centre d'Etude Guerre et Société (CegeSoma) et directement à la VSSE.

Dans une société démocratique, un service de renseignement ne devrait pas garder indéfiniment sous clé ses documents classifiés, sous prétexte qu'ils ont un jour été classifiés « confidentiels », « secrets » ou « très secrets ». Ces documents avaient reçu cette classification à l'époque parce que, par exemple, leur divulgation pouvait entraîner l'identification d'une source humaine ou d'une méthode particulière de renseignement, telle qu'une écoute téléphonique. Toutefois, les pièces jadis classifiées ne doivent pas nécessairement le rester ; telle fut également la conclusion du parlement belge en 2022. Depuis le 7 octobre de cette année, la VSSE est ainsi légalement tenue de déclassifier ses archives historiques et d'en faire rapport annuellement à la Chambre des Représentants.

En 2024, le service Archives et Documentation de la VSSE a déclassifié et inventorié 80 boîtes du fonds d'archives relatif aux « Inciviques », avec l'appui de deux membres du personnel détachés des Archives générales du Royaume et d'un grand nombre de collaborateurs du service. Ces dossiers concernent des collaborateurs de la Seconde Guerre mondiale dont les activités ont également fait l'objet d'un suivi de la VSSE après la guerre.

De l'autre côté du spectre se trouve le fonds intitulé « Occupation-Résistance », qui concerne le large éventail de groupes de résistance actifs au cours de la Seconde Guerre mondiale, allant des groupes d'extrême gauche aux groupes de résistance royalistes ou militaires. La VSSE a également gardé un œil sur leurs agissements à l'issue de la guerre. Les 123 classeurs de documents de ce fonds ont également été déclassifiés.

Deux autres fonds d'archives, dénommés « Occupation allemande » et « Occupation-Collaboration », portent sur la collaboration (forcée) avec l'occupant allemand. Ces deux fonds ont été entièrement déclassifiés.

Outre la déclassification, le service Archives et Documentation de la VSSE traite également les

demandes de consultation des archives du service introduites par des chercheurs. En 2024, 20 demandes avaient été adressées à la VSSE. Trois-quarts de ces enquêtes ont reçu un suivi positif ou sont encore en cours de traitement.



## ► RÉSISTANTS

Par ailleurs, 239 autres demandes de consultation des archives relatives aux « Services de Renseignement et d'Action » et aux « Agents de Renseignement et d'Action » ont été introduites en 2024. Ces dossiers de la VSSE sur les résistants se trouvent depuis 1993 déjà au CEGESOMA - le Centre d'Etude Guerre et Société. Le nombre élevé de demandes – 239 demandes concernant pas moins de 1068 dossiers – résulte sans doute du lancement de la plateforme en ligne Wikibase Résistance/Verzet au second semestre de 2024 (<https://resistanceinbelgium.be>). Cette plateforme permet aux personnes intéressées de chercher des données sur pas moins de 150.000 hommes et femmes engagés dans la résistance, en introduisant leur nom, date de naissance, lieu de résidence ou le nom du mouvement de résistance dans lequel ils étaient actifs. ■