VSSE
veiligheid van de staat
sûreté de l'état

INTELLIGENCE REPORT 2024

STATE SECURITY

.be

Responsible editor: Francisca BOSTYN
Boulevard du Roi Albert II, 6 - 1000 Brussels

TABLE OF CONTENTS

Francisca BOSTYN
Administrator-General

PREFACE

In keeping with tradition, I present to you the VSSE's annual Intelligence Report. This year, too, we cannot get around the fact that our domestic security was again affected by the international geopolitical context. In the last few years, the Russian aggression has obviously been an important catalyst in this regard. Attempts to interfere in democratic processes continue to crop up. Take, for example, the "Voice of Europe" story that was brought to light last year.

New scenes of battle have also emerged that have not always been on our radar in the past, such as the North Sea. Reports of suspicious activities by ships in the North Sea are omnipresent in the news today and compel the VSSE and its Belgian partners to actively monitor these new evolutions.

Disinformation and polarisation are annually recurring issues, and especially in an election year, these were issues to keep a watchful eye on. I am convinced that this watchfulness should be a standard part of our approach to foreign threats against our Western democracies, as foreign actors can and will use every socially sensitive topic to stir up polarisation. Polarisation, fuelled by disinformation, is subtle and difficult to tackle, but can be very socially disruptive. Monitoring this issue will continue to be a challenge for the VSSE.

Our adversaries are often also very resourceful in their hybrid efforts. For example, together with other European intelligence services we observe that individuals are recruited much more casually, for instance through Telegram – they are, so to speak, freelancers that are brought in ad hoc to carry out espionage or sabotage activities. It goes without saying that this way of working makes it much more complex for intelligence and security services to take action.

In this context, we as an intelligence service must be flexible and must have adequate means at our disposal to protect ourselves. I am therefore very pleased that since 2024, the VSSE has been able to rely on the revised Criminal Code, in which espionage and interference have been made punishable.

Recent attacks in New Orleans and Magdeburg indicate that terror remains one of the most important threats, also for the VSSE. The Islamic State (IS) and its franchise in the Khorasan Province (ISKP) pose the most important threats to our country, not least because their ideology may spur lone actors to action. In July 2024, the ISKP threat led to judicial

intervention among a number of sympathisers in Belgium. Another striking and worrying finding is the fact that one in three individuals involved in the VSSE's terrorism cases is a minor. This is not only a challenge for security services, but also for actors in social prevention focussing on young people. Fortunately, minors have fewer possibilities to take action, which is why they less often end up carrying out their planned attacks.

The developments in Syria in December 2024 pushed the issue of the remaining Belgian foreign terrorist fighters in that area back to the forefront. It is the clearest example of how evolutions abroad can influence our own security: regardless of the envisaged solution, it cannot be denied that these foreign terrorist fighters are indeed a security issue for our country.

Furthermore, I would like to point out that the VSSE is more than just an intelligence service. We are also an organisation with an important assignment with regard to security. This is more than ever the case since the National Security Authority became part of the VSSE in early 2024. This Authority's tasks include issuing security clearances and ensuring the proper handling of classified information – the latter is done, for instance, by actively alerting security officers, which are present in a growing number of organisations. The current security context and the increased security awareness have led to a significantly larger workload. It is important that we acknowledge and communicate this.

Finally, I would like to draw your attention to a number of important challenges for the future.

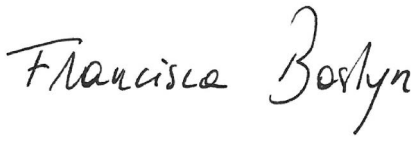
First and foremost, there are the challenges related to cyber threats and to the fast-paced developments with regard to new technologies. In order to keep up, we have to master them quickly. The range of technologies we have to cover, however, is broad and ranges from integrating artificial intelligence into our daily work to finding solutions for gaining access to encrypted communication.

The technological challenge presents three other challenges. Firstly, there is the human challenge. It is not easy to find qualified staff that have a thorough knowledge of this technological complexity. And if we find them, how do we make sure that we can offer them an attractive salary and interesting terms of employment? These specialist profiles are highly sought-after in the private sector, which has much larger financial capabilities than a federal authority.

Secondly, there is the legal challenge: quickly-evolving threats and technological evolutions continuously require adapted legislation, which is a time-consuming process. Thirdly, there is the exponential increase in data. As an intelligence service, we constantly have to find new ways to process these vast amounts of information. At the VSSE, we are still in the process of implementing a new investigative model and a new IT environment, which should eventually enable us to better tackle this issue. This will require further continuous investment in the future.

A final major challenge that I see, is the contribution that the VSSE will have to make in order to make our country more resilient at a time when war in Europe is once again a public topic of discussion. The political world and the security services are increasingly aware of the fact that we have to better prepare our society for war and other crisis situations. How can we keep hospitals and power stations up and running? How can we ensure large movements of troops? And how should the VSSE adapt its intelligence work when Belgium is involved in an armed conflict? Another question is how to protect our economic prosperity. This does not only relate to protecting our intellectual property, but also to physically protecting our critical infrastructure. The pressure on our economy is something that Belgium and Europe need to be even more mindful of, especially given the increased assertiveness of countries such as China.

Together with our Belgian and international partners – cooperation is key in a world that knows no borders when security is concerned – we continue to do our utmost every day to protect our democracy and our country's inhabitants. In the last few years, we have been given the chance to significantly expand our service with regard to staff and budget. I would like to take the opportunity to thank all members of staff, new or experienced, for their daily efforts, their drive and their belief in our mission. I am convinced that, collectively, we are ready to take our responsibility in the new reality in which we live.

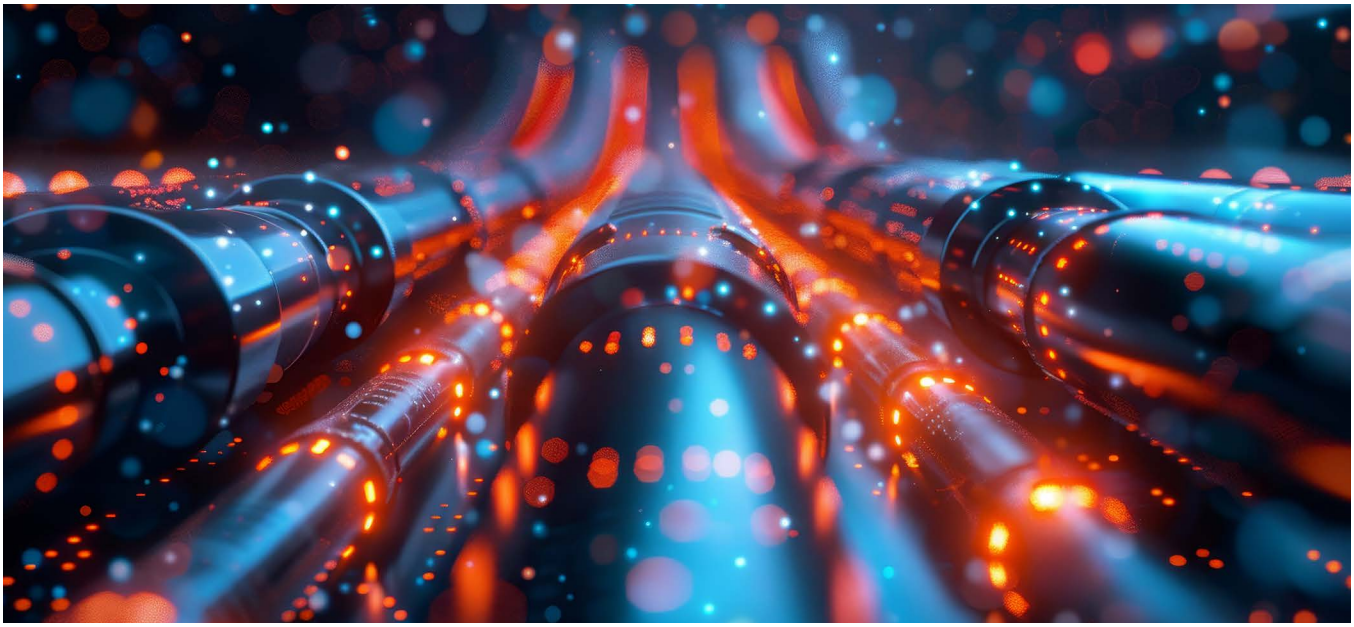


01

THE VSSE AS AN INTELLIGENCE SERVICE

ESCALATION OF HYBRID THREATS IN BELGIUM AND EUROPE

Exploding parcels in the sorting centres of a mail service at European airports, sabotage of railway lines, reconnaissance drones flying over military barracks, cyberattacks, ship anchors severing undersea internet cables, polarising disinformation campaigns designed to influence elections. 2024 was the year of escalating hybrid threats, which can generally be attributed to hybrid warfare with Russia.



The concept of hybrid threat refers to a combination of activities carried out by state and/or non-state actors, with the aim of negatively influencing or causing damage to an opponent or its institutions in a way that goes unnoticed. The term "unnoticed" is of paramount importance here. A hybrid threat may be just as tangible as a conventional kinetic attack, but it is never clear on whose behalf it was carried out. This is a deliberate strategy, as it prevents any coordinated response, from NATO for example. This hybrid approach – adopted by perpetrators who are difficult to identify – complicates the task of reliably attributing responsibility for these actions to any perpetrator, and therefore sometimes precludes any response.

Therein lies the success of hybrid threats, given the sheer damage that can be wrought, with little risk of response. There are many indications that Russia has intensified its hybrid actions in Europe over the past year, both geographically, from Eastern to Western Europe, and methodologically. Russia is well-versed in hybrid warfare and works with hacker groups (cyber threat), criminal organisations (attacks on critical infrastructure) and freelance agents to disguise their activities wherever possible.

While, over the past two years, the focus has been on actions attributable to Russia, other players – state and non-state actors – are also busy behind the scenes. China, for example, continues to use a broad range of hybrid methods.

▶ A WHOLE-OF-SOCIETY APPROACH

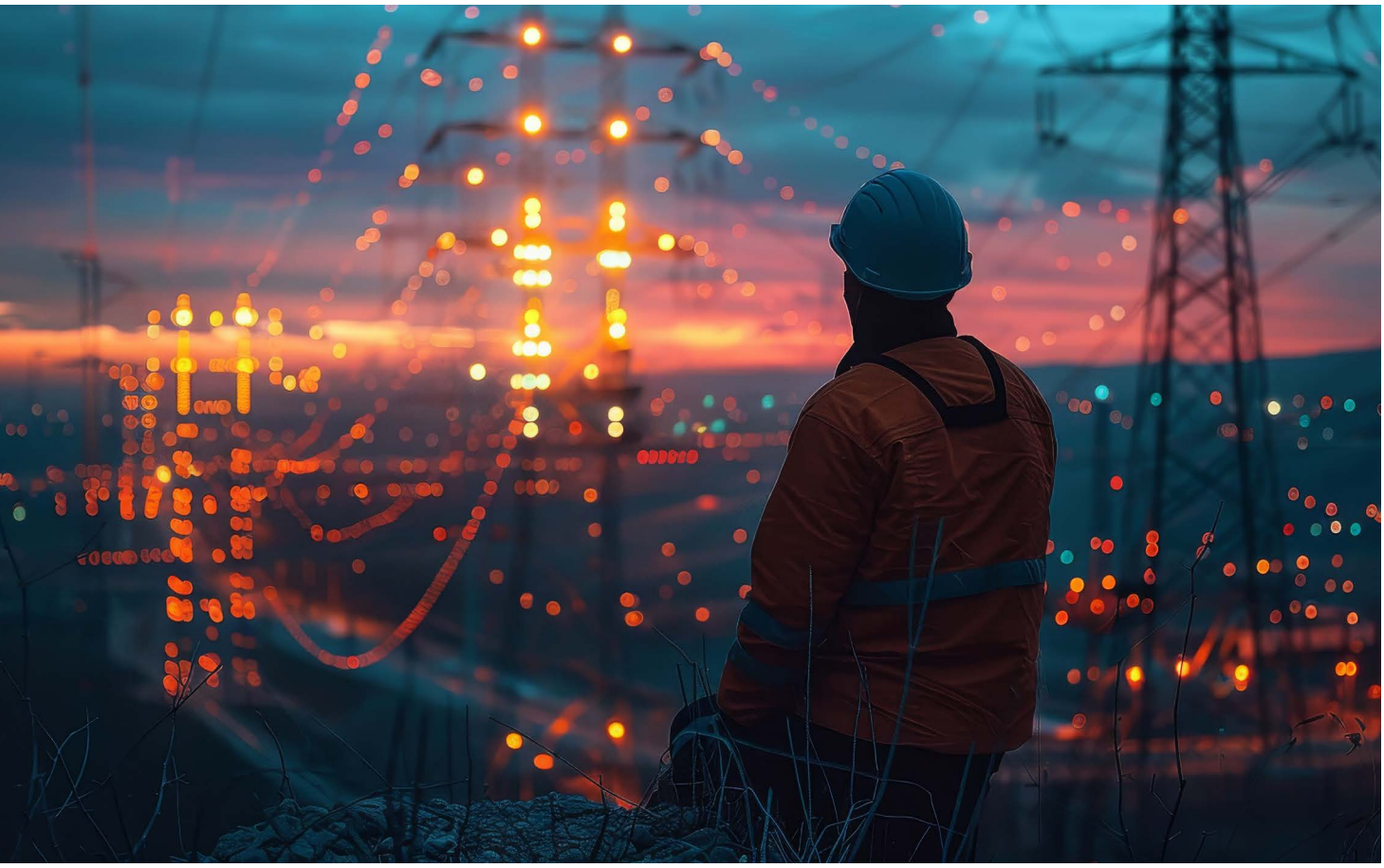
Today, one of the major challenges facing intelligence services is to anticipate these attacks, identify them (commercial players do not particularly like to boast about their weaknesses) and be able to attribute them to a specific actor. This is a specialist task, and one in which the VSSE cooperates at both national and international level.

Each player has a specific role to play in this area. In Belgium, the VSSE works closely with the National Crisis Center (NCCN), the General Intelligence and Security Service (GISS), the federal police, the Coordination Unit for Threat Analysis (CUTA) and the Centre for Cybersecurity Belgium (CCB), as well as with private sector companies. Our collective response will determine whether we emerge from this period weaker or stronger.

■

RUSSIA OPTING FOR AGGRESSIVE STRATEGIES TO DESTABILISE THE WEST

The mass expulsions of Russian intelligence officers under diplomatic cover from European countries have put Moscow in a delicate position. It has seriously undermined the Russian intelligence services' capacity on European soil, although their ambitions remain unchanged. To overcome this obstacle, Russian intelligence services are getting creative.



Since Russia's large-scale invasion of Ukraine in early 2022, hundreds of "traditional" Russian intelligence officers have been forced to leave the European Union and its partner countries, such as the UK and Norway. These officers generally had official diplomatic status within Russian representations. In Belgium, they had to leave the Russian embassy, the Russian mission to the EU in Brussels and the Russian consulate general in Antwerp (the Russian mission to NATO had already closed on its own initiative in 2021). Most of the officers expelled in 2022 and 2023 have been declared "persona non grata". Our country has thus ensured that dozens of Russian intelligence officers return to Moscow.

While these expulsions have severely curbed the capacity of Russian intelligence services and their freedom of movement on European territory, Russia's intelligence needs have not just gone away. Far from it. The war is raging on, and by describing its offensive as a fight against "the West as a whole", Russia is opting for an aggressive hybrid strategy. On the one hand, it is keen to obtain specific information, for example on the military and financial support granted to Ukraine by European countries, or on sanctions packages. On the other hand, it also aims to destabilise and discredit "the West as a whole", by creating and even stoking a climate of social unrest, or through the dissemination of its own ideological narratives.

In the past year, it became clear that, in their quest to find new ways to collect intelligence and conduct operations, Russian intelligence services have switched to an innovative way of recruiting and task-

ing agents. This takes its inspiration from the "gig economy", an economic model based on flexible, temporary or freelance contracts: assignments are widely distributed via social networks (Telegram, in particular) by one or more intermediaries. These missions are aimed at whoever is interested, just as anyone can moonlight as a cab driver with Uber or supplement their income as a bike courier with Deliveroo. The Russian services also increasingly use criminal networks, which complicates the detection of their activities.

The missions entrusted to these "freelancers" or to criminal organisations range from gathering intelligence, propaganda actions to military reconnaissance and sabotage (see box). In London, for example, a warehouse housing material aid for Ukraine was set on fire; the fate of the perpetrators is currently in the hands of the courts. In Belgium, no espionage or subversive activities carried out by freelance agents or criminal organisations by order of the Russian intelligence services have yet been recorded, but this definitely does not mean that we should not prepare for such actions.

What's more, the application of the principles and lessons of the gig economy is not the prerogative of Russian intelligence services. The use of individuals with no obvious direct link to the intelligence community for well-defined intelligence operations is a phenomenon that is gaining in interest and scope. This modus operandi reduces the risk of compromise for professional intelligence officers during an operation, and reinforces the plausible deniability sought by hostile intelligence services (and their political leaders).

So by using freelancers and criminal organisations, foreign intelligence services kill two birds with one stone: they create the impression that they are (or are able to be) active everywhere, whereas the activities can rarely be attributed to them with certainty.

▶ FREELANCERS AS AGENTS FOR RUSSIA

Recruiting freelance agents via social media is a step-by-step process: as with conventional recruitment, potential agents have to prove themselves, on the one hand, and put themselves increasingly at risk, on the other.

- A classified ad for a simple mission appears in a Telegram group: "Put up anti-Ukrainian stickers and receive 20 euros." One person expresses interest. A bot asks a series of basic questions.
- The candidate answers the test questions correctly. A Russian intelligence officer takes over the conversation and provides further instructions. The agent carries out the mission and transmits a photo as proof. They are paid in cryptocurrency.
- A second, riskier and even illegal mission follows: "Go and photograph this military infrastructure."
- One mission follows another, each tougher than the last. The perpetrator sinks increasingly into illegality, and is finally entrusted with a request for sabotage.

This is an abstract example.

▶ NO NEED TO PANIC

Russia intends not only to block support for Ukraine, but also to destabilise Western societies. Although it is tempting to systematically see Moscow's fingerprint on every incident, giving way to this line of reasoning would play into the Kremlin's hands. One of the aims of this new modus operandi is precisely to sow panic by giving the false impression that Russia can strike anywhere, at any time. This is why the VSSE and its partners must be careful not to create unnecessary controversy when monitoring this phenomenon. ■

THE NORTH SEA: A PERFECT AREA OF OPERATION FOR HYBRID WARFARE

The North Sea is an ideal area of operation for hybrid warfare. At sea, hostile actors can operate relatively unnoticed, especially if they deploy not only warships, but also container ships, research ships or even unassuming sailing boats. Why worry about a sailing boat cruising peacefully on the North Sea, or a cargo vessel whose anchor is dragging along the seabed a little too long?

Criss-crossed by data cables, energy cables and gas pipelines, the North Sea provides the ultimate strategic environment. Hence the increasing number of incidents involving these kinds of cables and pipelines, particularly in the Baltic Sea. The part of the North Sea off the Belgian coast is also a potential target. An increasing number of suspicious movements of ships, which sometimes also follow illegal routes, have been detected in recent months.

It is clear that these suspicious movements are closely monitored by the various Belgian services of the Maritime Security Centre. The Maritime Security Centre is part of the Coast Guard Centre in Belgium. In this centre in Zeebrugge, Customs, the Maritime and River Police, the Armed Forces and the Maritime Security Unit of the Federal Public Service Mobility combine their strengths and their powers to collect, analyse and share information. Their work is preventative as well as reactive to increase security in ports and at sea. This is an important task given that the Belgian coast is next to one of the busiest shipping routes in the world. The VSSE interacts continuously with the Maritime Security Centre and also exchanges information on the issue in international forums. ■

▶ SOMETHING IS UP IN THE NORTH SEA

In April 2024, on the initiative of the Belgian Minister for the North Sea, Paul Van Tigchelt, the competent ministers of six countries bordering the North Sea signed a cooperation agreement stating that they will work together on the protection of critical undersea infrastructure from sabotage and attack. Part of this agreement involves the development of a secure system for exchanging information on incidents.

In August 2024, in the margins of an energy conference held in Stavanger, Norway, the intelligence services of eight countries bordering the North Sea called for increased security of North Sea subsea infrastructures.

In December 2024, the Port of Antwerp-Bruges invited representatives from the Belgian industry, the maritime sector, banking institutions, academia and the security sector to an interactive evening on the theme of maritime security.

DISINFORMATION AND POLARISATION IN A DOUBLE ELECTION YEAR

2024 was an unprecedented year when it came to elections. More than two billion people were able to cast their votes worldwide. Elections were held in Belgium too, at all levels of power: from local to European. To ensure that these elections were free and fair, the VSSE not only conducted its own investigations, but also worked closely with its Belgian and foreign partners.

Elections are always a sensitive period, during which disinformation and interference activities can have a greater impact. A fact not lost on hostile actors. This is why a lot of disinformation circulated in the Belgian information landscape in the election year 2024.

However, Belgian politicians and parties or, more generally, our electoral process were rarely explicit targets. This observation served as a common thread throughout the Belgian election year.

A few extremist and anti-establishment voices were nevertheless raised within our own country, calling into question the fairness of the elections, for example, with unfounded insinuations about voting computers. Anarchist and Salafist groups also called on people not to vote. However, the number and scope of these messages remained very limited. Moreover, there was never any question of disinformation being used to disrupt the elections or alter the results.

▶ ONGOING POLARISATION

This does not solve the problem, though. Hostile actors such as Russia inundate the Western – and therefore also the Belgian – information landscape with polarising, anti-democratic messages on an almost continuous basis. Sometimes these messages are completely false, but more often than not they are simply an attempt to inflame sensitive issues, or to amplify and exploit sudden polarising incidents.

In addition to "classic" themes such as migration and the rights of LGBTQI+ people, issues such as farmers' protests, the conflict in Gaza and Western support for Ukraine have also been addressed in 2024. All with the same objective: to divide our society and undermine confidence in our democracy. No department can tackle this phenomenon alone. The intelligence services are just one link in the fight against disinformation, in which the media, education and civil society have a vital role to play.

▶ THE SPREAD OF DISINFORMATION IS PUNISHABLE UNDER CERTAIN CIRCUMSTANCES

The VSSE is not a thought police. Nor are we fact-checkers.

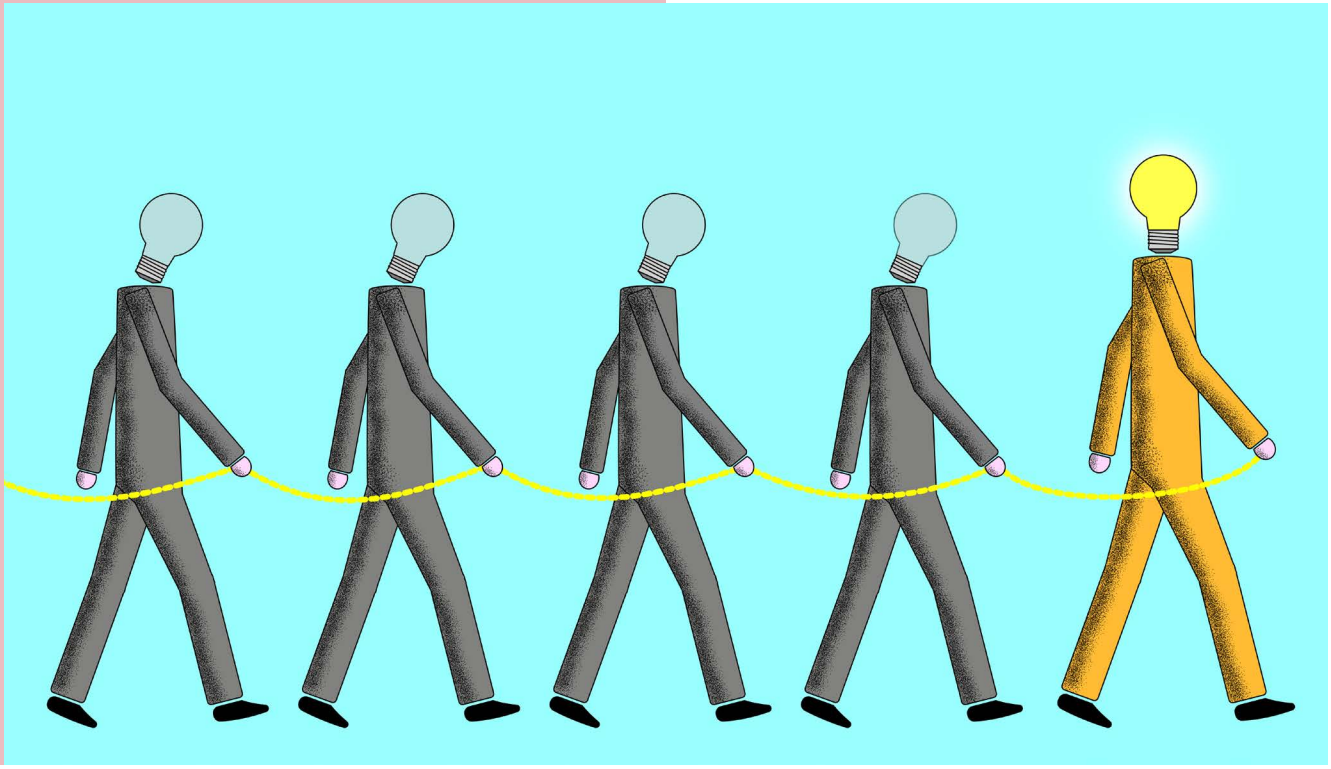
We detect false information when hostile actors exploit our openness and fundamental freedoms to promote their own strategic interests.

It is worth noting that providing incorrect essential information to Belgian authorities with the aim of deceiving them and therefore harming the essential national interests, is a criminal offence. This is partly because of new criminal legislation, in force since April 2024.

▶ ARTIFICIAL INTELLIGENCE

The use of artificial intelligence had only a minor impact on the Belgian elections. Previously, there were fears that artificial intelligence would be a catalyst for all forms of disinformation. Deepfakes – fake video and audio clips broadcast to compromise political figures – are just one example. Fears on this subject have proved unfounded – for Belgium at least.

But vigilance is still called for. Even outside an election context, there is always a risk that false videos, memes and other messages will continue to erode the cohesion of Belgian society and confidence in our democratic institutions. And artificial intelligence is a vehicle for creating and disseminating this kind of content ever more rapidly, at an ever lower cost and ever more attuned to its audience. ■



BELGIUM IS NOT IMMUNE TO CYBERATTACKS

In the light of the attacks led by a group of pro-Russian hackers against dozens of Belgian websites in the run-up to the municipal elections in October 2024, it has become clear that our country is not immune to large-scale cyberattacks. This attack was primarily conducted for propaganda purposes. In other cases, attacks can also involve the theft of confidential data.

Between 7 and 13 October 2024, the pro-Russian hacktivist group NoName057(16) targeted various Belgian websites. These were Distributed Denial of Service (DDoS) attacks, involving the flooding of websites/online services with traffic, with the aim of overloading their capacity and rendering them temporarily unavailable or disrupting their operation. This type of attack does not involve data theft or system intrusion.

▶ RETALIATION FOR SUPPORT TO UKRAINE

According to information communicated by the group, the attacks were carried out in retaliation for Belgium's planned arms deliveries in support of Ukraine, in particular the delivery of CAESAR artillery units. Despite the timing of the attacks – a week before the local elections – and the admittedly limited reference to the elections in the group's communication, the focus was not on the elections. The DDoS attacks were aimed at a variety of targets: mainly local government websites (municipal and provincial), but also sites of various federal authorities (FPS Finance, FPS Economy), seaports, bpost, industry federations (Febelgra, Febelfin), the Belga news agency, and so on. While the overall impact was largely limited, several websites remained unusable for some time.

The group in question, active since 2022, had already carried out a series of cyberattacks against Belgian websites in the past. In January 2024, sites linked to the Chancellery of the Prime Minister, the Chamber of Representatives and the Senate were targeted. NoName057(16) is active internationally, and has already levelled DDoS attacks against the websites of government agencies, media companies, critical infrastructure and private enterprises in several European countries, as well as outside the European Union (USA, UK).

In the event of such incidents, the VSSE remains in constant contact with partner services with a lead in the fight against cyberattacks, such as the Centre for Cybersecurity Belgium (CCB) for technical analysis and the Armed Forces' General Intelligence and Security Service (GISS) for the operational work. The VSSE aims to shed light on the issue of counter-intelligence in cyber investigations. The aim is to collect more information on what state and non-state hackers are looking for, which information was compromised and which conclusions need to be drawn about the intentions of our adversaries.

■

THE VSSE FIGHTS AGAINST THE CIRCUMVENTION OF SANCTIONS AGAINST RUSSIA

Among the world's geopolitical and security challenges, nuclear, biological, chemical and radiological weapons of mass destruction and their delivery systems represent a crucial challenge for the security of our country and of our allies. That is why preventing certain state actors from acquiring goods and technologies covered by sanctions packages is also one of the VSSE's missions.

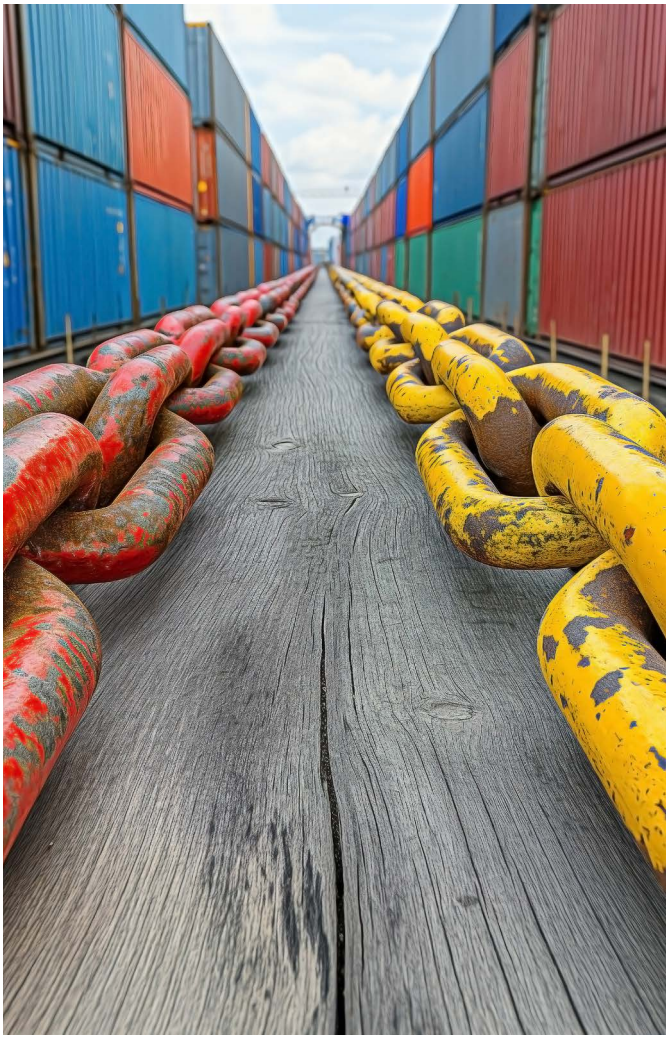
The VSSE supports the international strategy, which has two clearly identified objectives: on the one hand, to counter the capabilities of the Russian military-industrial complex supporting the incursion into Ukraine and, on the other hand, to impose far-reaching structural consequences on Russia in response to its actions against its Ukrainian neighbour.

The evolution of the war in Ukraine and the various series of sanctions imposed on Russia are forcing the country to adapt and find new channels to procure the goods needed for its unconventional and highly advanced weapons programmes. These are often considered dual-use goods, i.e. goods that can be used for both civilian and military purposes. As well as high-tech components, they may also be relatively rudimentary goods, which could be used in the manufacturing process of certain weapons.

In concrete terms, Russian companies, often controlled by the State and its intelligence services, attempt to acquire goods and technologies in or via Belgium that are useful to the Russian war effort. These acquisitions may be carried out with the help of companies based in third countries across Asia, the Middle East, Europe or Africa.

The VSSE actively helps enforce international sanctions against Russia, in particular by identifying and disrupting mechanisms for circumventing sanctions against this country, in collaboration with national and international partners.

Furthermore, with the assistance of these partners, the VSSE is fully committed to preventing other actors from acquiring the materials, technologies, know-how and knowledge needed to develop programmes related to weapons of mass destruction and their delivery systems, such as missiles and drones. These include states such as Iran and North Korea, which are subject to international sanctions. ■



THE VSSE CONTRIBUTED TO AN INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE EUROPEAN PARLIAMENT

The VSSE watches out for any clandestine foreign interference in the Belgian decision-making process, but also assumes this role in its capacity as the intelligence and security service of the host nation of European and international institutions such as the EU and NATO. In this role, over the past year, the VSSE has helped the investigation into a pro-Russian interference network hinged around the "Voice of Europe" media outlet.

As part of its mission to help prevent interference activities in and around the European Parliament, the VSSE, in close collaboration with various European partner services, has investigated a pro-Russian interference network run and financed via a number of intermediaries by a pro-Russian, Ukrainian oligarch and media magnate.

These kinds of networks try to rally "friendly" MEPs to their cause, with or without financial compensation. They also strive to increase the number of pro-Russian MEPs in the European Parliament, using parliamentary assistants, among others, to better organise and coordinate their activities.

This interference network was supported by its own media organisation, "Voice of Europe", that was led by a front man in the Czech Republic.

A number of European services (including the VSSE) cooperated intensively to expose this network. In March 2024, the Czech authorities decided to place the oligarch, his front man in the Czech Republic, and "Voice of Europe" on a sanction list, due to their interference activities.

▶ A FINE LINE

It is not unusual for individuals, groups, organisations and states to try to defend their interests through diplomacy, economic representation, public relations campaigns, cultural associations and so on. These strategies are part and parcel of political and diplomatic life. To return to the example of "Voice of Europe": Russia still has extensive diplomatic representation in the EU and Belgium. As such, it does not need the network revolving around the Ukrainian media magnate to legitimately defend its interests.

Interference differs fundamentally from lobbying or diplomacy in that it uses "illegal, fraudulent or clandestine means".

■

ESPIONAGE AND INTERFERENCE IN THE CRIMINAL CODE

Since April 2024, Belgium has new tools to combat espionage and interference by foreign countries. Until then, espionage and interference activities were only punishable if they took place in a military or war context. In reality, therefore, interference and espionage were rarely criminal offences.

So could interference and espionage be carried out with impunity before April 2024? Of course not. Administrative measures were always a possibility. Moreover, interference and espionage are generally accompanied by other punishable acts (corruption or criminal conspiracy, for example).

As these measures were not sufficient in today's reality, the legislator has decided to bring forward the entry into force of the penalisation of the offences relating to interference and espionage, originally planned for the new Criminal Code of 2026. Belgium is thus fully assuming its responsibilities to tackle espionage and interference on its territory effectively, not only against Belgian interests, but also against those of the international institutions located on its soil.

▶ STATE SECRET

These new stipulations make it possible to prosecute espionage activities, whether for the transmission, disclosure, reproduction or reception of a state secret. The same applies to attempted espionage and activities carried out in preparation for the transmission of a state secret. To this end, the notion of "state secret" has also been defined in the law. In addition to classified information, this term refers to any information which is not accessible to the public and plays a significant role in protecting Belgium's interests.

Moreover, anyone who actively engages in interference activities with the intention of influencing democratic decision-making processes (election results, voting in parliament, awarding of a public

▶ THE VSSE AND GISS WORK TOGETHER IN THEMATIC "HOUSES"

In 2024, cooperation between the VSSE and the GISS on counter-espionage and foreign interference was also stepped up. Since the spring of 2024, the VSSE and the GISS have been regularly pooling their intelligence on these issues within the framework of thematic "Houses", which focus on a single geographical region or a particular theme. This makes it possible to better coordinate the two services' investigations and prevents duplication of work.

procurement contract) may henceforth be prosecuted if these activities are carried out clandestinely, i.e. without the knowledge of the Belgian authorities and with the aim of seriously harming national interests.

▶ COOPERATION PLATFORM

In practical terms, the services responsible for these areas meet to discuss the files within a discussion platform. For each file, they assess which follow-up method has the greatest chance of success. If it is possible to prove a sufficient number of offences, this may lead to criminal proceedings. If it is not yet clear that enough offences can be proven or if more information can be obtained for the intelligence services, then it is preferable to continue with the intelligence work. This system is comparable to the method used by the JIC/JDC in terrorism cases.

Whatever option is chosen, it must be considered in the light of the context and a nuanced picture of the situation sought. Criminal proceedings can serve as a signal or be a great deterrent. This is the most effective response in some cases. In other dossiers, no offences have been committed, and administrative measures are in order.

▶ NOT LIMITED TO USUAL SUSPECTS

It is clear that including espionage and interference in the new Criminal code impacts all foreign actors engaging in espionage or interference activities to influence the democratic decision-making process. The VSSE has observed that countries other than Russia and China are also engaging in espionage and interference in Belgium. ■

CHINA: A DELICATE BALANCING ACT BETWEEN INTERESTS AND RISKS

In a tense geopolitical context, the – mainly economic – relationship between China and Belgium or between China and Europe remains important. Nevertheless, China poses various threats to Belgium and Europe in terms of cyber, espionage or interference, risks to our economic and scientific potential, attempts to control the diaspora, and so on. The VSSE is tasked with detecting these threats, reporting them to decision-makers, and raising awareness of the risks to which the various Belgian players – from the public, academic or economic sector – are exposed. Based on this information, it is up to the decision-makers to then strike the right balance between Belgium's economic interests and security risks.

In 2024, China adopted a more assertive stance towards Europe than before, mainly to defend its political and economic interests. In this respect, there is a relative alignment with Russia; "relative" in the sense that the People's Republic of China does want to maintain trade relations with Europe, which remains a major Chinese economic partner.

One of the ways in which this assertive behaviour becomes apparent is through hybrid threats against Belgium and Europe. And perhaps even more than other adversaries, China carries out these threats in a subtle manner, through all possible vehicles – be they diplomatic, economic, social, cultural or, of course, intelligence-related. This is what we call China's global approach. As part of this global approach, where the concept of national security has been further broadened under Xi Jinping, the role of the intelligence services has recently been

expanded. China's intelligence services – including the main civilian intelligence service, the MSS – are already present in all areas of society. And as their capabilities have grown, so has the pressure to deliver results.

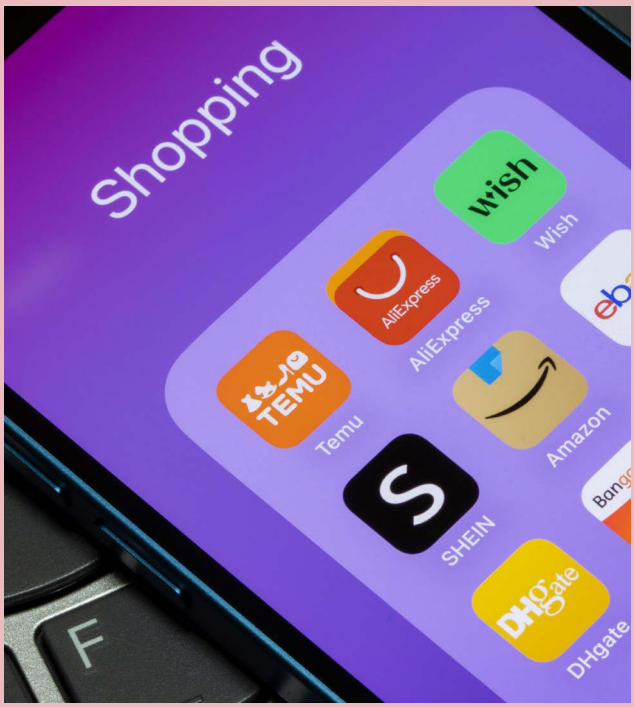
As part of this approach, a combination of legitimate and clandestine activities is often observed. With regard to interference, China's objectives are, on the one hand, to create and support groups of decision-makers in Europe, who can in turn attempt to influence the decision-making process to China's advantage, and on the other, to divide Western allies, in particular by attempting to damage transatlantic or intra-European relations.

While the general behaviour has evolved, the VSSE has seen no recent changes in the modus operandi used by Chinese intelligence services in Belgium. The recruitment or even handling of individuals of interest to them is often carried out in China or from China, as we were able to observe in a file partly made public at the end of 2022. This system reduces the risks for Chinese intelligence officers, who do not have to travel to 'hostile' countries.

The above-mentioned global approach, in which all Chinese players, whether State or non-State, are obliged to collaborate with the intelligence services – added to a subtle modus operandi that is difficult to identify – complicates the work of our service in detecting Chinese intelligence activities. This makes it all the more important to raise the threat awareness of Belgian players in order to shore up our resilience and enable everyone to assess the threat correctly. ■

▶ THE RISK OF CHINESE APPS

A good example of how the People's Republic of China operates are the Chinese applications that have attracted attention several times over the past year. Through a seemingly innocent application (online shopping, watching funny videos), a mass of user data is collected and stored. Is the damage directly visible to users? No, but this data can be used over the long term. For example, it can be used to infect smartphones, to spread disinformation more effectively, to reinforce or repress certain narratives, or to provide input for certain tools that rely on large quantities of data, such as artificial intelligence tools. Under China's legal framework, there are no obstacles to the use of this data by the Chinese intelligence services. They can use it, for example, to target individuals or their relatives for the purposes of espionage or interference. Caution therefore remains essential. That is why it is advisable not to install unnecessary applications on your business devices, or devices on which sensitive information is stored.



THE HYDRA-HEADED JIHADIST TERRORIST THREAT

In 2024, the main terrorist threat in our country continues to come from jihadist terrorist organisations. This observation – one the VSSE has made for several years – is backed up by major developments and changes.

▶ IS IN THE KHORASAN PROVINCE

In Belgium, the main source of the threat of jihadist terrorism is still the Islamic State (IS), and in particular its subsidiary in Central Asia, the Islamic State – Khorasan Province (ISKP). The historic province of Khorasan is located in the Central Asian region bordering Afghanistan, Pakistan, Iran, Tajikistan, Uzbekistan and Turkmenistan.

As feared, in 2024, ISKP made itself known by emerging as an organisation capable of carrying out more complex terrorist operations in its own region as well as beyond. The attack perpetrated by ISKP on 3 January 2024 in Kerman (Iran), which killed 96 people at a rally organised in memory of the commander of the Iranian Revolutionary Guard, did not augur well. Later that month, a smaller attack in Turkey killed two people. On 22 March 2024, it was Russia's turn to be hit by an attack that killed 145 people at Crocus City Hall. It was one of the bloodiest attacks on European soil since the Paris attacks of 13 November 2015.

ISKP has thus emerged as the most dynamic branch of the entire IS network. Although the organisation does not control any territory in Pakistan or Afghanistan, its reputation built on its actions on Russian, Turkish and Iranian soil enables it to continue to attract new financial resources and sympathisers.

While, over the past year, ISKP has demonstrated its willingness and ability to conduct operations through centralised cells, ISKP and IS in general also remain perennial sources of inspiration for lone actors via their online propaganda. This violent propaganda incites individuals to commit violent acts, for which they then claim responsibility. Planned terrorist attacks by ISKP sympathisers have also been foiled in Western Europe in the past year, such as in Austria. In Belgium there were house searches and arrests among ISKP sympathisers on the eve of the opening of the Paris Olympic Games in July 2024.

▶ IS IN SYRIA AND IRAQ

Despite the defeat of the physical caliphate in Syria and Iraq in 2019, "Foreign Terrorist Fighters" (FTF) are still present in various locations in the region. Some of them also have links with our country: they are Belgian nationals or they left Belgium to take part in the jihad, for example. In the vast majority of cases, they left at the time with a view to joining the ranks of IS, although many of these 'Belgian' FTFs ultimately fell in with a host of separate jihadist groupings.

The sudden implosion of Bashar al-Assad's regime in Syria on 8 December 2024, following the rapid and unexpected advance of the Hayat Tahrir al-Sham (HTS) rebels, may also have repercussions for the Belgian security situation in the weeks and months ahead.

According to information at the VSSE's disposal, at the end of 2024, 13 male FTFs with links to Belgium are said to be held in prisons in north-eastern Syria controlled by Kurdish fighters. The Al-Hol and Al-Roj camps, located in the same region, are said to house 8 female FTFs and 9 children. Twenty-four other fighters with links to Belgium and 43 children are said to be present in north-west Syria. A handful of these fighters are said to support or be members of the HTS rebel movement. It goes without saying that the VSSE is keeping a close eye on the whereabouts of these FTFs. A rapid change in the situation that would allow them to return to Belgium unnoticed and uncontrolled would have an impact on the security situation in our country.

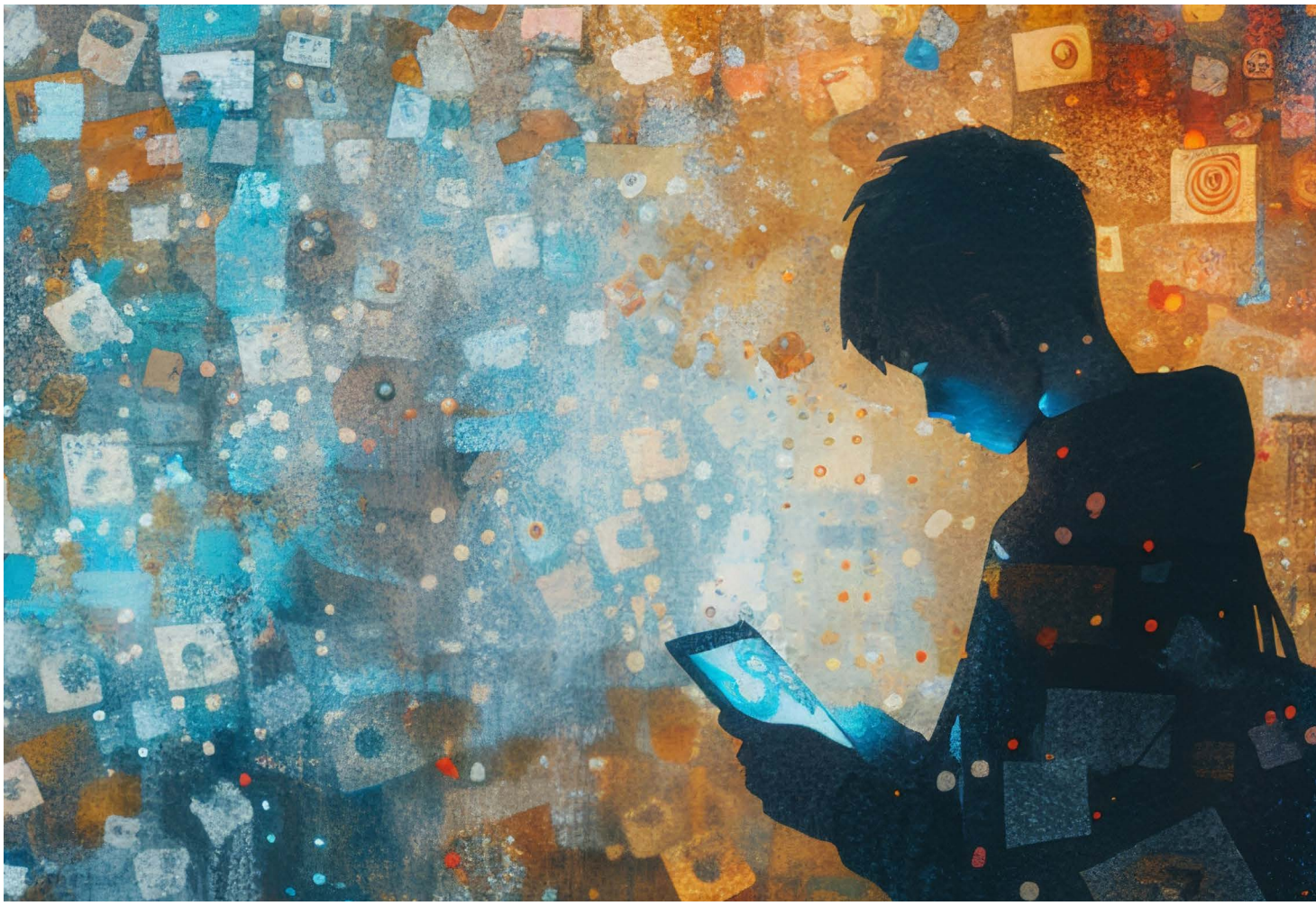
At the end of 2024, there was no indication that IS is fully engaged in the Syrian operations, even though the organisation can still count on many supporters in the wider region and a resurgence of IS cannot be entirely ruled out.

▶ IS IN THE SAHEL AND SOMALIA

On the African continent, namely in the Sahel region and in the Horn of Africa, terrorist organisations are gaining in strength. In these regions, groups linked to IS and al-Qaeda control a significant amount of territory, enabling them to regroup and strengthen their capabilities. The coordinated attack by IS in Somalia on 31 December 2024 is a recent example. The VSSE currently has no indication that the regional situation could have a direct impact on the threat in Belgium. With the help of its Belgian and foreign partners, the VSSE is monitoring the situation.

■

ALMOST A THIRD OF THE INDIVIDUALS NAMED IN THE VSSE'S TERRORISM FILES ARE MINORS



Between 2022 and 2024, almost a third of the people who plotted attacks in Belgium were under 18. Their online radicalisation process is nothing short of meteoric, which is why identifying and tackling these threats in time is a real challenge for the VSSE and its partners.

The Belgian intelligence and security services are increasingly confronted with the presence of minors in threat-related files. This is nothing new, but the phenomenon seems to be gathering in intensity.

A look back at the VSSE's terrorism files for the last three years (from 2022 to 2024) tells us that just under a third of the people who hatched plans for attacks were minors. The youngest suspect arrested in 2024 was 13 years old. These individuals have an average age of around 16. All the minors planning violent actions were boys.

3 IN 4 DRIVEN BY RADICAL ISLAM

In some three-quarters of cases, these minors were motivated by a radical version of Sunni Islam. A quarter of minors were driven by right-wing extremism or anti-establishment sentiments.

The radicalisation process of these minors takes place online, and is generally particularly rapid. In today's hyper-connected society, extremist and terrorist propaganda material is just a click away for young people in search of an identity or a purpose in life. The VSSE notes that, in some cases, minors not only consume extremist and terrorist propaganda material, but also produce and distribute such material themselves.

Social pressure is a key factor in the radicalisation of minors. The VSSE observes that radicalised minors are often members of an (online) network or group of people sharing the same ideology. Young people in these networks regularly and increasingly tend to encourage each other to consume ever more content, and ever more extreme content at that. It is also very difficult to distance themselves from this trend without cutting off social ties with the other members of the group.

The speed of the radicalisation process means that the intention to commit a terrorist act often has little ideological basis. However, this absence of an elaborate ideological framework in no way weakens the motivation of those involved. The VSSE often observes a glorification of violence. People are routinely introduced into problematic (online) groups because of their fascination with violence and violent subjects. After a while, minors perceive violence as the only way of achieving their extremist goals.

Fortunately, due to their inherent situation of dependency, parental control and lack of access to certain platforms, these minors generally find it far more difficult than adults to obtain the means they need to carry out their planned attacks. However, this situation does not prevent terrorist organisations from inciting these impressionable young people to commit violent acts.

Detecting these threats in time is therefore also a difficult task for the intelligence and security services, as the minors in question are usually completely unknown to the authorities before they appear on the radar of the intelligence services. It remains a very difficult and time-consuming assessment for an intelligence service to distinguish between loudmouthed keyboard warriors and those who pose a real threat.

Apart from the VSSE and other security actors, social prevention partners such as the Local Integral Security Cells (abbreviated to LIVC in Dutch) and the Communities play an important role.

■

EXTREMIST PROPAGANDA ENCOURAGES LONE ACTORS TO RESORT TO TERROR

Extremist propaganda is a significant catalyst that spurs on lone actors to commit violent acts. Despite the loss of its caliphate, the Islamic State (IS) remains the main source of inspiration for planned attacks in Belgium, thanks to its online propaganda machine. An analysis conducted by the VSSE reveals that the seized phones of jihadists in Belgium often contain alarming quantities of extremist propaganda.

In terms of scale, Sunni jihadism remains by far the biggest threat of violent terror in Belgium. This threat can come from outside Belgium, but it can also come from within our borders. In both cases, extremist propaganda often acts as a major catalyst. This became evident from an investigation by the VSSE into some fifty phones and other electronics that were confiscated from individuals involved in jihadi terrorism cases. 72% of those devices contained vast amounts of IS propaganda. Propaganda linked to al-Qaeda was also found, but to a lesser extent.

In 2024, both the Islamic State and al-Qaeda still have a strong and extensive propaganda apparatus. The end of the physical caliphate has not prevented IS from strengthening the mobilising power of its ideology. IS continues to exist as an 'online' caliphate. This means that the organisation remains the main source of inspiration for planned attacks in Belgium and elsewhere in the West, as demonstrated by the New Year's Day attack in New Orleans in the United States.

Al-Qaeda also remains active on the internet and social media, with an ever-growing propaganda network. Both IS and al-Qaeda are very adept at recycling and reusing old propaganda material, but are also still producing new material. Both organisations use official and unofficial media to disseminate their propaganda. Each in its own way has built up an online ecosystem which, even in 2024, continues to attract visitors from all over the world. While, in terms of content, al-Qaeda opts for in-depth ideological narratives, IS generally chooses violent and shocking images.

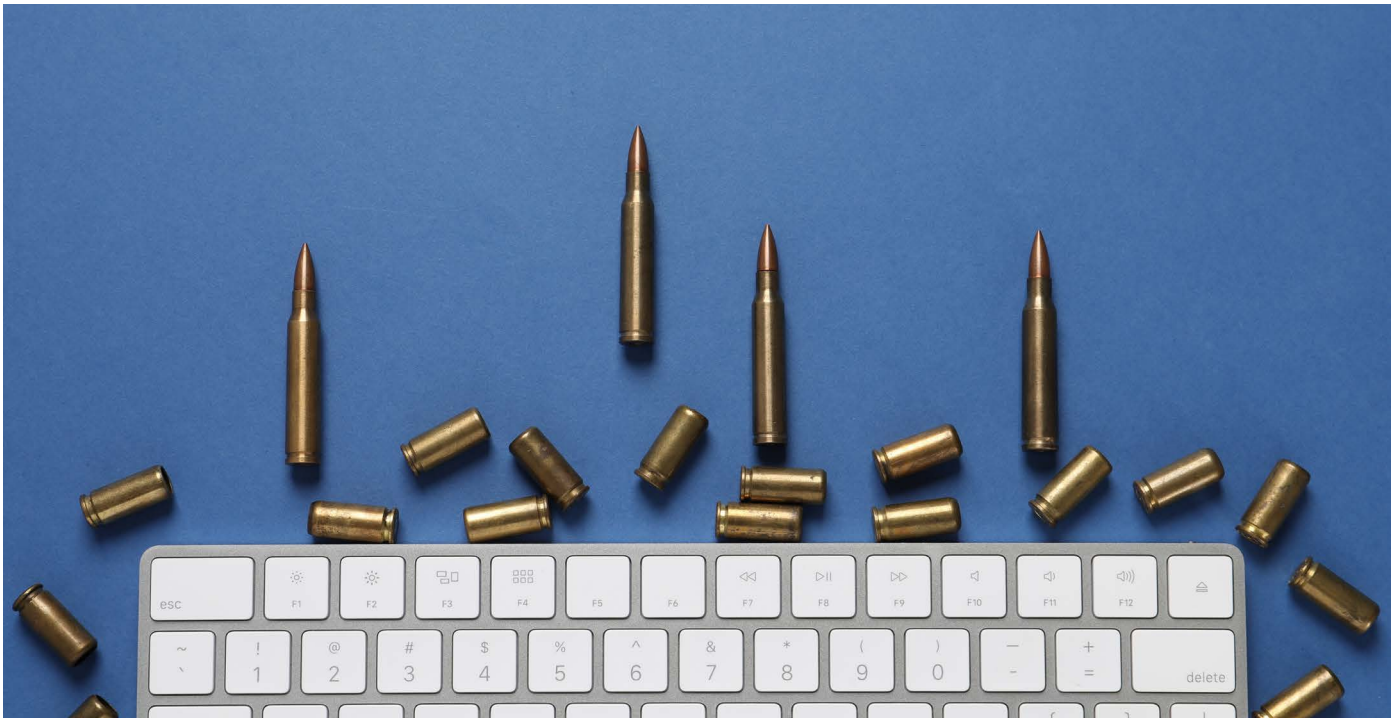
Terrorist groups such as al-Qaeda and IS use their propaganda to achieve a number of objectives: spreading their ideology, radicalising and recruiting individuals, raising funds and, above all, inspiring young people to commit terrorist attacks.

▶ ALGORITHMS

An additional problem is that the algorithms of the main public social media channels such as YouTube, TikTok or Facebook are creating a pull effect by suggesting more and increasingly extreme videos or other content ever more quickly to people who have looked up radical topics online. These methods plunge these people, sometimes unconsciously, into what is known as a digital "rabbit hole", from which it is very difficult to extricate oneself.

Another problematic trend is the phenomenon of users – mostly young people – being directed through certain interests to discussion groups or channels on apps such as Telegram, in which more specific extremist right-wing narratives are being shared. In the most worrying cases, very explicitly violent propaganda material and terrorist manuals are shared

■



CONFLICTS IN THE MIDDLE EAST AND THEIR IMPACT ON BELGIUM

In 2024, the war between Israel and Hamas escalated, reigniting the conflict between Israel and Hezbollah in Lebanon. The fall of Syrian dictator Bashar al-Assad's regime at the end of the year opens the door to considerable change in the region, with possible implications for our country.

▶ SYRIA

The sudden and rapid implosion of Bashar al-Assad's regime in Syria on 8 December 2024, following the advance of the Hayat Tahrir al-Sham (HTS) rebels, may also trigger fast-moving developments in the region in the months ahead. This situation is likely to have an impact not only on the fate of "Foreign Terrorist Fighters" with links to Belgium held in prisons and camps in northeastern Syria, but also on the territorial aspirations of several jihadist groupings in Syria. Nor can a resurgence of IS be completely ruled out. Together with its network of international partners and the GISS, the VSSE is closely monitoring the situation on the ground.

▶ GAZA AND LEBANON

The escalation of the conflict between Israel and Hamas in Gaza and the West Bank, and the resurgence of the war between Israel and the Lebanese Hezbollah, are also having an impact on Belgian and European society. Events in the Middle East provide fertile ground for radicalisation, and have already led to violent actions in several European countries, such as the brawls between Israeli football fans and young pro-Palestinian supporters in the streets of Amsterdam on 7 November 2024. A few days later, a handful of youths planning violent action against the Jewish community were arrested in Antwerp. In Sweden and Denmark, the Israeli embassies were the target of gunfire or hand grenade fire.

Terrorist organisations such as IS and al-Qaeda use the conflict in the Middle East in their propaganda material to reinforce their jihadist message and recruit sympathisers. This phenomenon could also encourage people to commit violent acts in Belgium.

▶ HAMAS AND HEZBOLLAH

Although Hamas is mentioned on a European list of terrorist organisations, the VSSE considers it highly unlikely that Hamas would carry out an attack on Belgian soil. If there is a risk of violence, it is more likely to come from radicalised lone actors spurred on by the conflict in Gaza.

Although Hamas is active in Belgium too, its actions consist mainly in lobbying Belgian and international institutions and seeking funding. These activities do not present a direct threat of violence, but they are nonetheless problematic and sometimes even constitute a criminal offence when it comes to financing a terrorist organisation.

There is no direct terrorist threat to Belgium from the Lebanese Hezbollah either. In our country, Hezbollah is mainly active within the Lebanese diaspora for fundraising purposes. The VSSE and its national and international partners are closely monitoring these activities. ■

THE THREAT OF RELIGIOUS AND IDEOLOGICAL EXTREMISM

Alongside terrorism, extremism also poses a threat to our democratic society. In some cases, certain forms of religious and ideological extremism can lead to increased radicalisation, culminating in violence.

THE MUSLIM BROTHERHOOD

The Muslim Brotherhood is a heterogeneous movement that does not pose a threat of violence in Belgium. However, the VSSE noted that among the sympathisers of the movement in Belgium, about a hundred individuals are actively trying to spread an ideology that can lead to radicalisation and promote extremism.

The difference between the Muslim Brotherhood and other extremist Islamist movements lies in its lobbying activities, aimed at influencing government policy on Islam, and in its methodology, which is based on the creation of organisations designed to keep the Muslim community in check.

In a clandestine fashion, groups within the Muslim Brotherhood's sphere of influence are attempting to exert pressure for Islam to be given a more prominent place in society. To this end, these groups conceal their links with the Muslim Brotherhood by posing as legitimate representatives of the Muslim community in Belgium. This way they hope to gain a foothold in Belgian institutions and obtain funding for their various initiatives.

The long-term aim of the Muslim Brotherhood is to establish a society in which every aspect of life is governed by religious practices. In the short and medium term, their rhetoric contributes to a climate of segregation and polarisation, which in turn provides fertile ground for radicalisation.

Although foreign support for the Muslim Brotherhood in Belgium has waned, the movement can be expected to continue its activities in our country.

▶ RIGHT-WING EXTREMIST LONE ACTORS

At the moment, the main threat posed by right-wing extremism in Belgium is the dissemination of its propaganda. In the long term, this phenomenon could potentially undermine trust in the country's democratic institutions, processes, and rule of law. The VSSE deems the risk of a terrorist attack by right-wing extremist groupings to be rather low.

If a violent act were nevertheless to be committed by right-wing extremists, it would mainly be the work of generally very young lone actors, who usually become radicalised online. Some of them find their inspiration in the accelerationist doctrine. This doctrine assumes that racial or religious warfare is inevitable in the long term, and that such warfare should ideally be triggered or accelerated by terrorist violence. This is because extreme right-wing accelerationist activists unshakeably believe that the white race will eventually win out because of its supposed superiority. Nevertheless, the number of accelerationists in Belgium remains limited.

▶ STRONG MOBILISATION OF LEFT-WING EXTREMISTS

We know from experience that left-wing extremist groups can be involved in acts of sabotage and employ black block tactics. However, in the past year, the VSSE mainly observed occupations of buildings, acts of vandalism and intimidation, often in the context of their increased engagement and mobilisation with regard to the conflict in Gaza.

The elections also demonstrated to be a mobilising theme for left-wing extremists. To broaden their support base, they are increasingly trying to exploit topical matters such as the issue of climate change.

At present, actions by left-wing extremists in Belgium mainly focus on recruitment, protests and the dissemination of their messages via online and offline propaganda. Nevertheless, some within left-wing extremist circles see violence as a legitimate means to their ends. Based on the available information, the VSSE considers the preparation and planning of attacks by left-wing extremists as unlikely.

■

VSSE AND GISS TERRORISM FILES SENT WEEKLY TO THE POLICE AND PUBLIC PROSECUTOR'S OFFICE

As part of the fight against terrorism and extremism, the VSSE and the GISS have been cooperating closely for several years now within a joint platform. Every week, this platform submits terrorism files to the police and the Public Prosecutor's Office. In 2024, the two services were designated as 'technical assistants' in 33 terrorism-related criminal investigations.

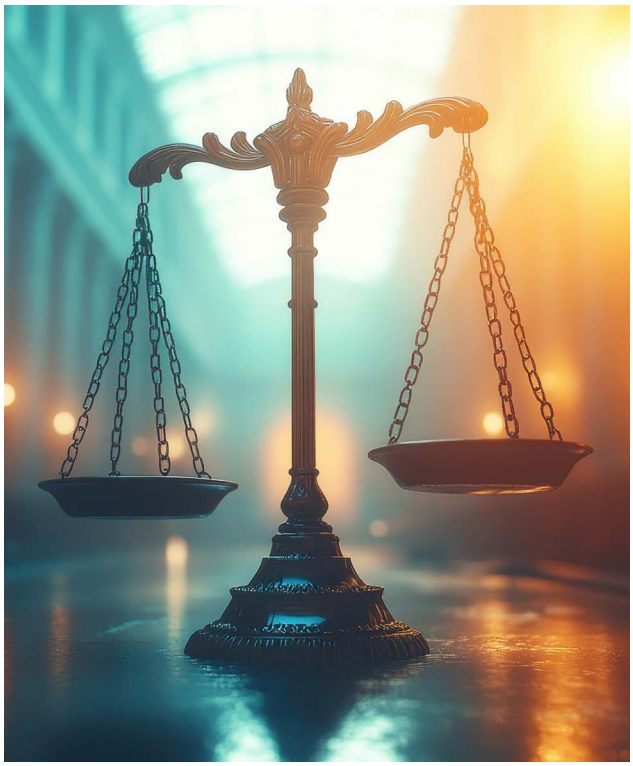
Since the March 2016 attacks and the parliamentary committee of enquiry set up in their wake, the entire intelligence and security world has shifted from the need to know to the need to share. Over the past few years, platforms have been set up to ensure a smooth flow of information between the various services active in the fields of intelligence and security, such as the intelligence services, the Coordination Unit for Threat Analysis (CUTA), the police and the Public Prosecutor's Office.

While the police and the Public Prosecutor's Office concentrate on investigating offences, gathering evidence and prosecuting individuals, the intelligence services focus on threats and intelligence gathering before any offences are committed. These aims are nonetheless complementary and allow ongoing interaction between the various players.

▶CECT PLATFORM: CENTRAL POINT OF CONTACT FOR TERRORISM AND EXTREMISM FOR THE VSSE AND THE GISS

For several years now, VSSE and GISS staff have been working together to combat the threat of jihadist terrorism within the CT Platform, also known as the Counter-Terrorism Platform. Since 2024, this collaboration has been extended to cover all files related to religious and ideological extremism and terrorism. In 2024, the former CT platform was therefore transformed into a new platform called the CECT Platform (Counter-Extremism and Counter-Terrorism platform).

The CECT Platform serves as a single point of entry for national partners involved in these matters. From this platform, the VSSE and the GISS send joint analyses and intelligence notes to national and international partner services. This makes it possible for the two intelligence services to speak with one voice on terrorism and extremism. At the same time, the joint CECT Platform can harness each service's own intelligence-gathering capacity and resources.



In practice, this cooperation takes the form of intelligence sharing (in relation to terrorism and extremism) through joint reports sent to the police and the Public Prosecutor's Office via the CECT platform. This makes it possible to exchange intelligence that could lead to a criminal investigation or could contextualise an investigation.

When new relevant information regarding terrorism becomes available, the service involved informs the Joint Intelligence Center (JIC). The JIC is made up of members of the Federal Judicial Police, the federal police's Central Anti-Terrorism Unit, the CUTA and the CECT Platform. These services then examine the new information together, make a joint assessment and draw up a proposal for appropriate follow-up, whether by means of a criminal investigation, a continuation of the intelligence investigation or another type of follow-up. This decision must then be validated by the Joint Decision Center (JDC). This is made up of the same members as the JIC, as well as members of the local Public Prosecutor's Office, the Federal Public Prosecutor's Office and the director-administrative coordinator of the federal police.

▶ 50 TERRORISM FILES

In 2024, the CECT Platform reported 50 intelligence files relating to terrorism to the JICs. A total of 114 JICs were organised last year. In other words, just under half of the terrorism files handled by a JIC were referred by the VSSE and the GISS. Most of the other files were submitted by the various entities of the federal police. The fairly major contribution of the intelligence services in this regard, is not surprising, as, after all, detecting threats at an early stage is a central part of their remit.

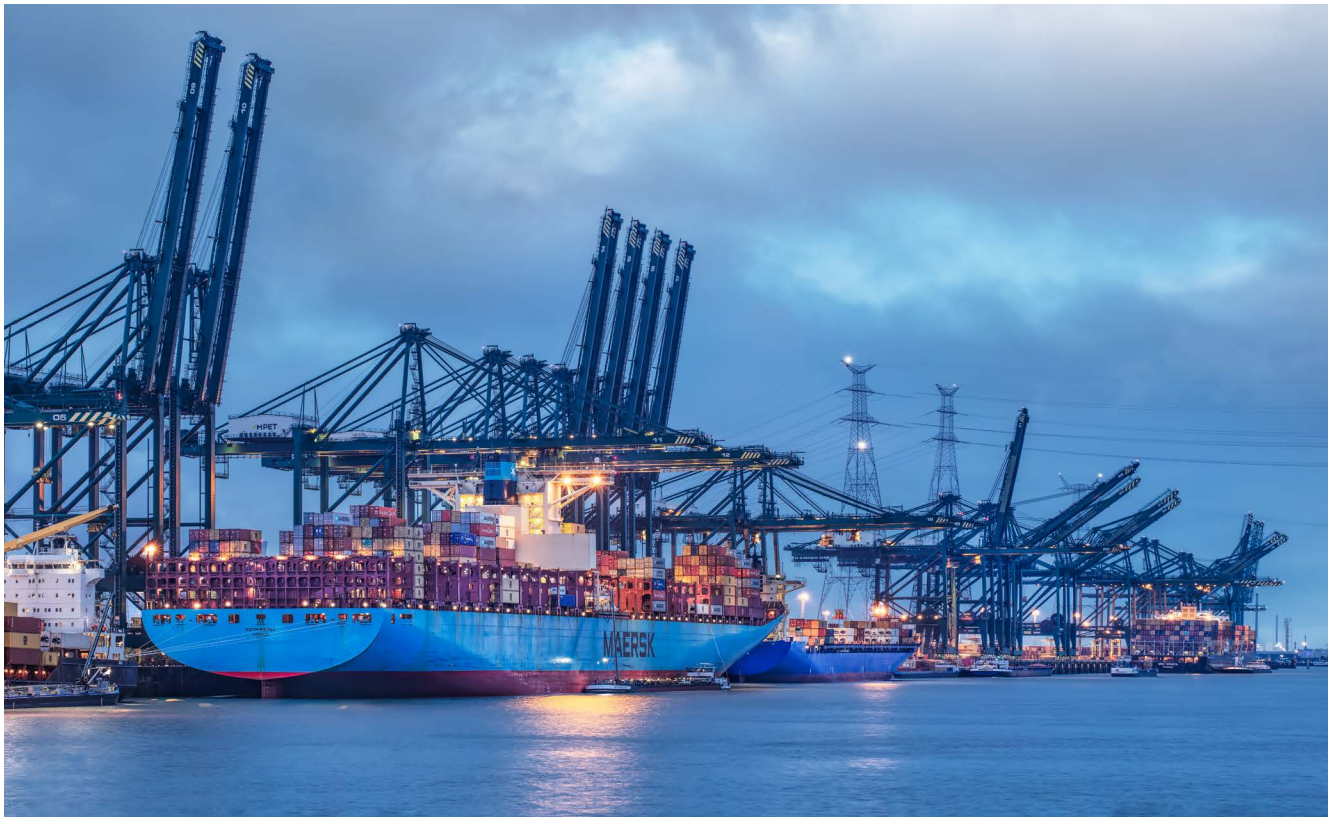
Of the 50 intelligence files on terrorism processed by the CECT Platform in 2024, 22 involved information about a violent threat. The other 28 files concerned terrorist propaganda or financing. The 50 files submitted by the CECT Platform led to the opening of 29 criminal investigations. In 15 cases, these files only entailed intelligence investigations.

Once the criminal investigation has been initiated, the intelligence services can be appointed as technical assistants. This is automatically the case for every terrorist file handled by the Federal Public Prosecutor's Office. In other words, the intelligence services have access to the judicial file and can lend their knowledge and expertise to the investigation. In 2024, the VSSE and the GISS were appointed as technical assistants in 33 terrorist files.

However, the work of the various services does not stop at the end of the criminal investigation. These files must then be the subject of an appropriate follow-up, through the various consultation platforms. This follow-up also takes place at the local district level, with the CECT Platform providing ongoing input to the Local Task Forces as part of the TER strategy, i.e. the joint strategy against terrorism and extremism.

■

THE VSSE PLAYS ITS PART IN THE FIGHT AGAINST ORGANISED CRIME



Belgium's approach to combating organised crime primarily involves the police and the judiciary, increasingly supplemented by a local administrative approach. As an intelligence service, the VSSE provides additional support to its national partners.

The VSSE primarily investigates individuals and networks involved in activities that could be detrimental to the State, i.e. violence or corruption targeting State officials or vulnerable sectors, such as our country's critical infrastructure. Any relevant information is then shared with the police and the judicial authorities, through the usual partnership processes.

In 2024, there were signs that the fight against drug-related organised crime was beginning to bear fruit. However, the victories racked up by the justice system, which have led to numerous convictions, have put a great deal of pressure on our prisons. The VSSE uses its specific expertise of the prison environment to detect threats that may emerge there. In cooperation with its partners, such as the prison administration, it also tries to identify the threats posed by organised crime to prison staff.

With the support of its partners, the VSSE also anticipates the extradition of key figures of the international drug mafia to Belgium. Several High-Value Targets (HVT) were arrested abroad in the final months of 2024. The judicial authorities request their extradition as part of their prosecution and the enforcement of their sentence in our country, but this potential extradition also entails security risks. In collaboration with the Federal Police, our service therefore examines the best way to contain these risks, seeking first and foremost to prevent these criminal activities from being continued in prison. This includes finding the right prison and a suitable detention regime for these HVTs.

The VSSE has also ramped up its presence in Belgian ports in order to increase the resilience of the actors and processes of the ports, in response to the subversive aspects of organised crime. ■

02

THE VSSE AS A SECURITY SERVICE

THE VSSE FURTHER IMPROVES THE SECURITY CULTURE

The VSSE and the National Security Authority (NSA), which has been embedded in the VSSE since 1 January 2024, endeavours to enhance the security culture, both inside and outside the organisation.

On a national level, the VSSE is in constant contact with an entire network of security officers, both within public authorities and private companies. The NSA, alongside other departments of the VSSE, is responsible for providing advice, support and guidance on various aspects of security, thereby helping to reinforce the security culture in Belgium:

- Security policy: the VSSE supports the development of a sound security policy within public and private organisations, enabling them to manage risks. The VSSE also regularly carries out awareness-raising campaigns on this issue. In 2024, for example, the NSA organised events for security officers. Almost 500 security officers, from both the public and private sector, attended these events.

- Information security: the NSA ensures the protection of sensitive and classified information, intervenes in the event of security incidents and draws up guidelines on the management of such information.

- Personnel security: the NSA – together with other departments of the VSSE – assists its partners with requests for security clearance. The VSSE and the GISS also carry out security investigations to ensure that the people who requested these clearances are sufficiently loyal, honest and discreet.

- Physical and technological security: the NSA plays a role in the certification of certain information and communication systems, buildings and sensitive areas. The NSA also advises its partners on how to protect their information, for example, when travelling to high-risk countries.

These various missions, which have already gained in importance following the integration of the National Security Authority into the VSSE, will only become more significant over the coming years.

The VSSE also enhanced the security culture within the organisation, for its own operations. These measures have definitely had an impact on the service's staff, for example with regard to the use of personal electronic equipment or the discretion that employees of an intelligence service must demonstrate, including within their close family circle.

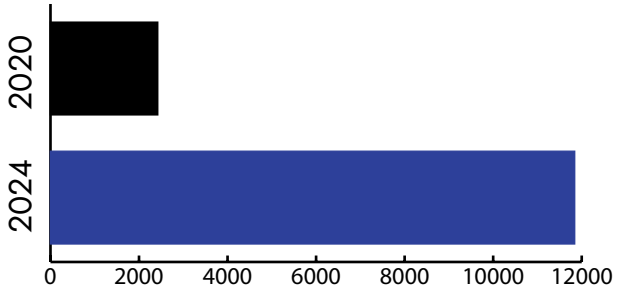
With its security policy, the VSSE sets out to be an example and a source of inspiration for other partners in the public and private sector.

■

THE NSA ISSUED NEARLY FIVE TIMES AS MANY SECURITY CLEARANCES OVER A FIVE-YEAR PERIOD

The National Security Authority (NSA) has been integrated into the VSSE since 1 January 2024. By integrating the NSA, the VSSE aims to significantly improve Belgium's security culture. To this end, the NSA issued almost 12,000 security clearances in 2024, almost five times as many as in 2020.

The VSSE is an intelligence and security service. This security pillar has been considerably strengthened in recent years, notably with the integration of the National Security Authority (NSA) on 1 January 2024. Until then, the NSA was a collegiate body made up of 9 services: the Federal Public Service (FPS) Foreign Affairs, the VSSE, the General Intelligence and Security Service (GISS), the Federal Police, the National Crisis Center (NCCN), the FPS Mobility, the FPS Economy, Customs & Excise and the Federal Agency for Nuclear Control (FANC). The NSA had a permanent secretariat with a staff of around twenty, and was responsible, among other things, for issuing and checking the security clearances granted to individuals and companies handling classified information (at confidential, secret and top-secret levels).

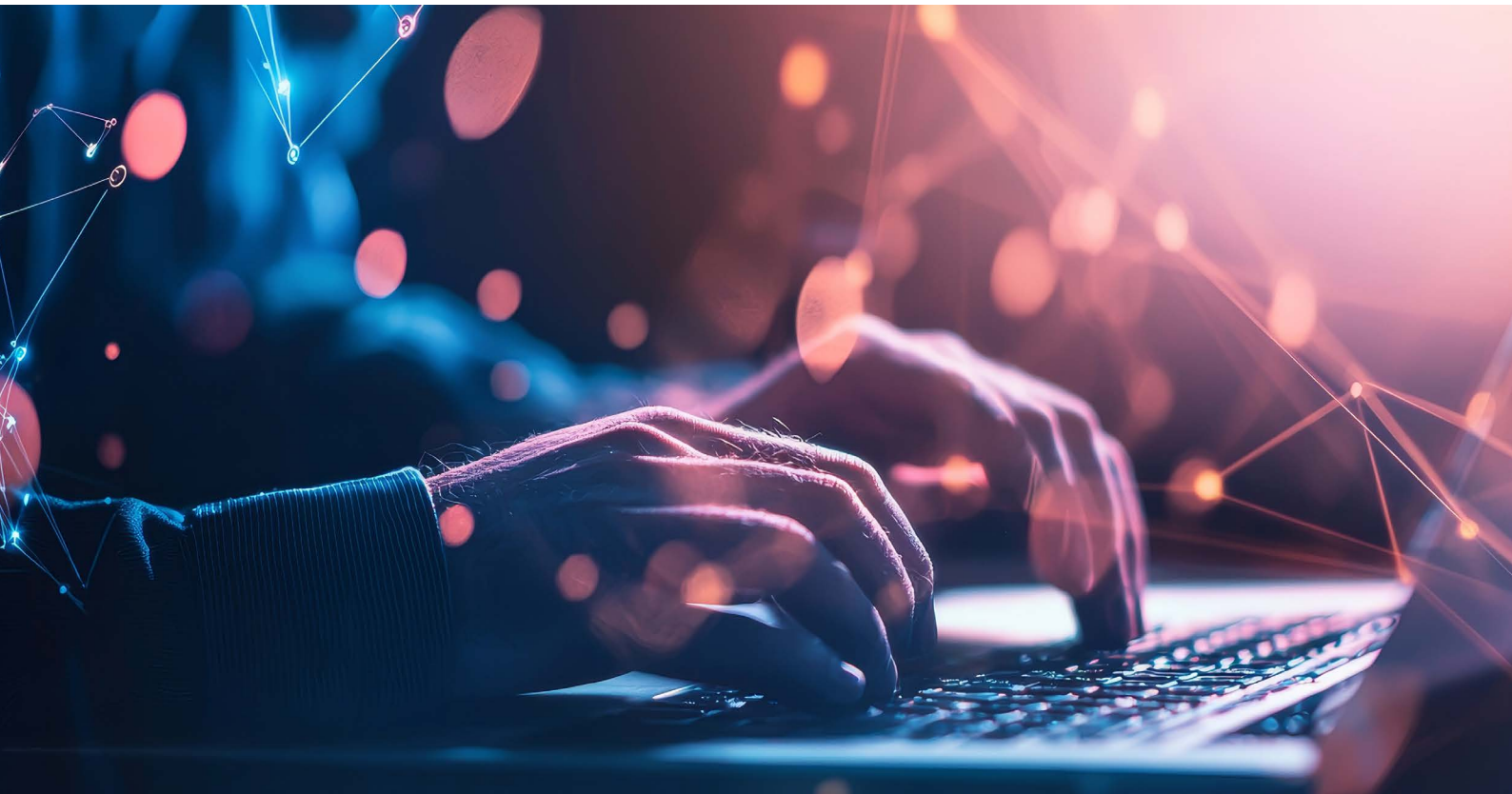


▶ 40 EMPLOYEES

Since the NSA began operating under the VSSE banner, the service has been significantly strengthened. Today, the NSA has a staff of 40. They have worked hard over the past year to improve responsiveness and update the outdated legal framework, guidelines and procedures.

In 2024, the NSA processed no fewer than 15,366 requests for individual security clearances. In the end, 11,840 clearances were issued. The number of security clearances granted has more than doubled in the space of two years. By way of comparison, five years earlier, in 2020, only 2,428 individual security clearances had been issued.

In addition, the NSA processed 1,271 security clearance requests for legal entities (private and public) in 2024, and 485 security clearances were issued to companies or organisations over the past year to enable them to handle classified information. ■



THE VSSE'S SECURITY CHECKS ARE UP 36% IN 2024

In 2024, the VSSE carried out 327,608 security checks, an increase of around 36% on the previous year. Moreover, the increased security awareness suggests that this figure will continue to rise in the near future.

Security checks are a series of prior checks designed to exclude individuals who could form a potential security risk from sensitive duties or from having access to sensitive areas. People working in airport security zones or in the nuclear sector are notable examples. These security checks are also carried out in connection with applications for Belgian nationality, asylum or family reunification.

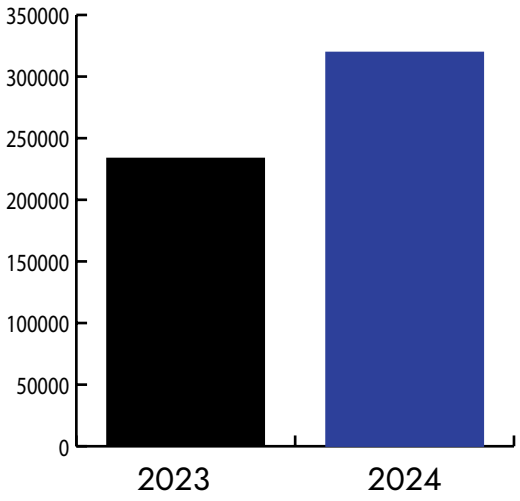
Because of the wide variety of security checks, a range of different partners ask the VSSE to carry out these checks. The main partner, however, is the federal police, which have been responsible for processing checks on the basis of the Classification Act of 1998 since 1 January 2024.

In 2024, the VSSE carried out a total of 327,608 checks. This is some 36% more than the 241,197 checks carried out in 2023.

What explains this considerable 36% increase? For airport badges, a new check now takes place every year (previously every five years). Furthermore, the number of applications for verifications as part of the procedures for obtaining Belgian nationality are on the rise, as are applications for verifications as part of requests for asylum and family reunification. The number of checks carried out in connection with European and NATO summits also continues to increase. In addition, more and more new sectors, including prisons and seaports, are subject to security checks.

And given the geopolitical situation and society's increased awareness that security needs to be dealt with responsibly, the VSSE expects that the number of security checks will continue to rise in years to come.

■



THE VSSE ISSUED 86 OPINIONS ON FOREIGN DIRECT INVESTMENTS

The screening procedure for foreign direct investments (FDI) in Belgium has been implemented since 2023, and completed its first full calendar year in 2024. During this period, the VSSE drafted opinions for the Coordination Committee on Intelligence and Security (abbreviated to CCRS in French), bringing together the positions of each of the partners involved. In 2024, 86 opinions concerning security and intelligence issues were submitted to the Interfederal Screening Committee.

In an increasingly complex and volatile geopolitical context, it is vital that Belgium develops mechanisms to ensure a degree of security and economic autonomy, while maintaining its international outlook.

Although the vast majority of the checked foreign investments were not considered to represent a threat, some nevertheless required further examination to allow the CCRS to issue an informed opinion. These were investments in a Belgian company, by individuals or companies from outside the European Union. Only investments in certain strategic sectors, such as critical infrastructure and cutting-edge technology or suppliers to the Belgian Armed Forces, are subject to screening. Finally, screening is only performed if at least 10% to 25% of the shares in the Belgian company risk being held by foreign entities.

▶ FDI SCREENING PROCEDURE

The main task is to screen foreign direct investments for potential risks to the country's national security and its strategic interests.

In practice, a screening procedure was initiated in just under 10% of the files. This is what is known as the second stage of screening, for which the VSSE deploys its own specific resources to investigate this investment. This strategic choice has enabled the VSSE to become a driving force in this new approach to national economic security.

In 2024, a total of 86 opinions were issued. More than ever, it is vital to identify potential threats and take preventive measures to help increase the resilience of sensitive national sectors, such as critical infrastructure, advanced technologies and energy.

■

03

ABOUT THE VSSE

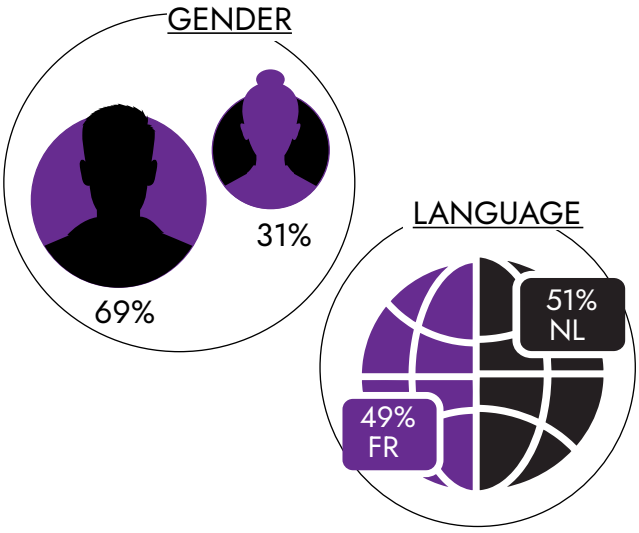
THE VSSE'S FIGURES FOR 2024

▶ HUMAN RESSOURCES

954

EMPLOYEES

The VSSE has undergone a radical transformation in recent years. In four years, the number of employees has almost doubled. It has successfully attracted, onboarded, integrated and trained hundreds of new colleagues internally; a real *tour de force*.



▶ INFORMATION EXCHANGE

43,366

INCOMING MESSAGES

The incoming messages come from national partners such as the General Intelligence and Security Service (GISS), the federal police, the Coordination Unit for Threat Analysis (CUTA), the National Crisis Center (NCCN), the Federal Public Service Foreign Affairs, the prison administration and Public Prosecutors' Offices. In addition, a significant proportion of the incoming flow of information is received from foreign intelligence services. For comparison: in 2020, the VSSE received 29,148 incoming messages.

1,492

REPORTS OF CONSULTATIONS WITH PARTNERS

In 2024, the VSSE wrote 1,492 reports of consultations during which information was exchanged with local, national and international partners.

▶ INTERNATIONAL RELATIONS

LIAISON OFFICERS

Abroad

At multilateral institutions (NATO/EU/Permanent Representation to the EU)

Intelligence work is more than ever an international undertaking: threats do not stop at national borders and countries also have to contend with similar challenges. To optimise the exchange of information, the VSSE continues to invest in its network of liaison officers abroad and at multilateral institutions in Brussels.

THE VSSE DECLASSIFIES ITS WORLD WAR II ARCHIVES

Over the past year, the VSSE has declassified a large part of its archives covering the Second World War period, and prepared them for transfer to the State Archives of Belgium. There has also been a noteworthy increase in the consultation of the VSSE's archives. In 2024, over 250 requests for consultation were made both through the Study and Documentation Centre for War and Contemporary Society (CEGESOMA), the Belgian centre of expertise for the history of 20th century conflicts, and directly to the VSSE.

In a democratic society, there is no reason for an intelligence service to keep its classified documents under lock and key indefinitely, on the grounds that they were once classified as "confidential", "secret" or "top secret". These classifications were justified at the time because the dissemination of the information could have for instance led to the disclosure of a human source or a particular intelligence method, such as wiretapping. However, these once classified documents can now safely be declassified, a conclusion also reached by the Belgian parliament in 2022. This means that, since 7 October 2022, the VSSE has been legally obliged to declassify its historical archives and report annually on the matter to the Belgian Chamber of Representatives.

Last year, the VSSE Archives and Documentation department declassified and inventoried 80 boxes of the "Inciviques" archive, with the support of numerous VSSE staff and under the supervision of two members of staff seconded from the State Archives of Belgium. These files concern World War II collaborators whose activities were also monitored by the VSSE after the war.

On the other side of the spectrum is the "Occupation-Resistance" collection, which concerns the wide range of opposition groups active during the Second World War, from extreme left-wing groups to royalist or military resistance groups. The VSSE also kept an eye on their activities after the war. The 123 folders of documents in this collection have been declassified.

Two other archive collections, entitled "German Occupation" and "Occupation-Collaboration", deal with (forced) collaboration with the German occupiers. These two collections have been declassified entirely.

In addition to declassification, the VSSE's Archives and Documentation department also handles requests from researchers to consult the department's archives. In 2024, the VSSE received 20 requests. Three-quarters of these requests have been approved or are still being processed.

▶ RESISTANCE FIGHTERS

A further 239 requests to consult archives relating to the "Intelligence and Action Services" and "Intelligence and Action Agents" were submitted in 2024. These VSSE files on resistance fighters have been held at CEGESOMA since 1993. The high number of requests – 239 for no fewer than 1,068 files – is no doubt due to the launch of the "Wikibase Résistance/Verzet" online platform in the second half of 2024 (https://resistanceinbelgium.be). This platform enables interested parties to search for data on as many as 150,000 men and women involved in the Resistance, by entering their name, date of birth, place of residence or the name of the Resistance movement in which they were active.

■