ADIV • SGRS
MAY 2025 / WWW.SGRS.BE

ANNUAL REPORT 2024

56° 30' 0" N, 31° 43' 15" E

DEFENCE

.be

COVER: Ammunition depot in Toropets (RUS) after Ukrainian bombing.

The world is changing, but our mission remains the same.

CONTENT

MAJOR GENERAL STÉPHANE DUTRON

HEAD OF THE SGRS

Quaero et Tego is our motto; protecting our country, our companies and our expats through our intelligence is our primary mission; advising the authorities wisely is our duty to our country, society and our fellow citizens.

“We work for you, for our country, for peace.”

Major General
Stéphane Dutron

RESPONSIBLE EDITOR

M. Van Hecke Bernard

Queen Elisabeth Barracks
Rue D'Evere 1, 1140 Evere

Images : DG StratCom and personnel SGRS

Layout : ADIV-SGRS

THE ARRIVAL OF THE F-35

The arrival of F-35 fighter jets to the Air and Space Component poses a number of technological challenges to the Cyber Component, especially in the area of weapon system protection.

Introduction

The Service's Agility in Response to Changes in the Security Environment

The year 2024 once again failed to bring peace to the world, as two major conflicts continued to unfold, with increasingly concerning geopolitical consequences. In February 2025, it will be three years since Russia launched its devastating invasion of Ukraine. In the Middle East, 2024 was marked by the intensification and geographical spread of the conflict between Israel and Hamas, reignited by the tragic events of 7 October 2023.

In Ukraine, although the front line has remained relatively stable, Russian forces have continued a slow but steady advance, incurring massive losses and prompting the adoption of new doctrines for resource deployment – not least the shift towards a full war economy. Ukraine, supported logistically by numerous allied nations, has demonstrated remarkable resilience, both at the front and deep within its territory, notably achieving a symbolic and striking breakthrough in the Kursk region, inside Russian territory. The deployment of North Korean troops to this region has further internationalised the conflict and raises serious questions about the long-term implications of emerging alliances and their potential impact on other crisis-prone areas.

In the Near East, alongside operations in Gaza and the West Bank, the Israeli army has carried out intense bombardments of Hezbollah positions in southern Lebanon and conducted strikes in Syria and Iran. The service is closely monitoring the expansion of Tzahal operations, as well as the erosion of Iranian influence via its proxies. The sudden collapse of the Assad regime in Syria last December has created new uncertainty and triggered a reshaping of power dynamics and spheres of influence in the region.

Naturally, my service is following these developments closely – not only in these two theatres of conflict. Our analysts, supported by a wide range of intelligence-gathering tools, produce in-depth assessments aimed not only at establishing facts but also at identifying trends to better anticipate future developments. This work informs both military and political decision-makers and feeds into exchanges with our national and international partners – always with the ultimate objective of safeguarding our citizens and national interests.

Most regional confrontations have repercussions in Europe and Belgium. This is particularly evident in the worrying rise in antisemitism and radicalisation, which has led to a significant increase in workload for intelligence and security services. The threat level – particularly in terms of espionage and foreign interference – has continued to rise, requiring the implementation of targeted countermeasures.

In this context, my service has had to demonstrate agility. Our personnel have shown exceptional adaptability and commitment in responding to the evolving security landscape. One of my priorities during my first year as head of the service has thus been achieved.

In the same spirit, we have continued our recruitment drive, both for civilian and military personnel, with the aim of doubling our workforce by 2040. I have placed particular emphasis on developing our training programmes and supporting new colleagues. Significant resources will continue to be dedicated to this effort, as well as to infrastructure improvements.

Finally, we will continue the digital transformation of our directorates and ensure that we are equipped with state-of-the-art capabilities to conduct intelligence operations – both in the physical world and in cyberspace. In 2024, we launched new joint projects with national partners such as the VSSE and the Federal Police, and I have personally worked to strengthen our relationships with international partners.

Enjoy reading!

MAJOR GENERAL

Stephane Dutron

ADIV - SGRS / CYBER COMMAND

Cyber Command

Cyber Force Through Partnerships

The year 2024 has been particularly intense for Cyber Command - and this has been the case since January.

As part of Belgium's Presidency of the Council of the European Union, cyber commanders and cyber ambassadors from Member States gathered for the first time in the so-called 'Egmont format', culminating in an unprecedented joint declaration underlining the importance of a strong cyber defence policy. The security challenges in cyberspace – across its physical, logical and virtual layers – are immense. Strengthening cooperation at the strategic, operational and tactical levels is therefore essential. One concrete application of this European cyber defence policy was our participation in the deployment of the Cyber Rapid Response Teams (CRRT) in Moldova. These multidisciplinary teams, drawn from several European countries, played a vital role in safeguarding the Moldovan presidential elections. This year, we will chair the planning mechanism for the continued implementation of this new European capability.

Meanwhile, 2024 was also an election year in Belgium, with elections at all levels of government. We contributed to the security of the June and October elections through our cyber defence capabilities and our expertise in detecting disinformation from foreign sources. Over time, we have observed a growing wave of increasingly sophisticated and malicious information manipulation and interference campaigns. While Belgium has so far avoided the large-scale disinformation operations observed in France, Germany, the Baltic States and parts of Central Europe, we remain a key target due to our central location in Europe and the presence of numerous international institutions.

In October, a series of cyberattacks targeting several federal, regional, and local government websites was all over the news. These so-called "denial of service" attacks, carried out by hacktivist groups, flooded the websites with traffic, making them intermittently inaccessible for several days. Basic protection measures generally held up well, and the overall impact remained limited. The modus operandi of these hacktivist groups is to publicise their actions to encourage other actors or individuals to join them and amplify the climate of fear they aim to create. It's worth noting that the less media coverage their actions receive, the less effective they are.

Given the current geopolitical situation, we are also contributing to the development of NATO-requested plans related to military defence, national defence, military enablement and resilience. In this context, we also must address hybrid threats in cyberspace – including electromagnetic warfare, cyberattacks, sabotage and disinformation – aimed at critical infrastructure. As part of our efforts, we organised a Tabletop Exercise (TTX) – the first of its kind in Belgium – with key infrastructure

stakeholders essential to military operations. The Centre for Cybersecurity Belgium (CCB) and the National Crisis Centre (NCCN) participated as observers.

To respond effectively to these threats, we continue to build up the Cyber Force within Defence while reinforcing SGRS' mission in cyberspace. The measures outlined in the Strategic Vision and the STAR Plan are being progressively implemented. We are continuously developing and deepening our human capital, notably through innovative initiatives such as the Cyber Defence Factory®, and through national and international partnerships. These include collaborations with the European Space Agency (ESA), the Federal Judicial Police, Agoria's Cyber Made in Belgium initiative, and our structural partner in applied research, the Royal Military Academy. Since the creation of Cyber Command just over two years ago, we have increased our workforce by 65%, with the objective of doubling it again by the end of the current term.

I remain firmly convinced that investments in human capital, innovation and partnerships are the right response to current and emerging threats. True to our motto Cyber Force Through Partnerships, we will continue developing our capabilities in support of the missions of SGRS, Defence and the nation.

MAJOR GENERAL

Signing the application form for one of our partners (Eric Van Cangh of Agoria) to become a candidate reservist at Cyber Command

How Long Can a War Economy Last?

After nearly three years of war, Russia's objectives in Ukraine appear to have changed little, if at all.

Although Russia frequently claims to be open to a ceasefire or peace negotiations, the Kremlin's long-term goal still seems to be the total subjugation of Ukraine. To pursue this goal, Russia transitioned to a war economy at the end of 2022, injecting enormous amounts of money into the production of weapons, fuel, food, clothing, and other key supplies.

This shift initially led to short-term economic growth and rising wages. However, the longer this situation continues, the greater the structural damage to Russia's economy is likely to be. Still, it is clear that the Kremlin prioritizes its geopolitical ambitions over economic sustainability. Moreover, it remains convinced that Ukraine will ultimately lose this war of attrition if Western military and economic support begins to falter.

Although neither side has achieved a decisive breakthrough along the front, both Russia and Ukraine continue to believe that military victory is possible. Russia has therefore maintained a steady offensive across the entire front, with a particular focus on the Donbas region (notably Donetsk and Luhansk). Despite making some westward advances, Russia is once again being forced to slow down, as it did in Bakhmut and Avdiivka in 2022 and 2023, due to well-known limitations such as a lack of heavy equipment, personnel, and ammunition.

Ukraine's Defensive Turn

Following a largely unsuccessful counteroffensive in 2023, Ukraine has shifted toward a more defensive strategy. Both President Zelensky and General Syrsky have framed this as part of a broader plan to avoid a permanent stalemate. Although a kind of military stagnation has emerged in southern Ukraine, Ukrainian forces have nevertheless succeeded in breaking through weak Russian defenses near the border with Russia's Kursk Oblast – exposing vulnerabilities in the Russian military.

This operation was also part of Ukraine's broader effort to establish an eastern buffer zone and to slow or stop Russia's advance in the Donbas. However, the imbalance in manpower between the two sides remains Ukraine's greatest disadvantage. The ongoing need to revise and adapt mobilization strategies is placing increased pressure on President Zelensky's controversial conscription policies, the delicate balance between military readiness and economic stability, and–perhaps most crucially–the unity of the Ukrainian people.

Air Campaigns

In addition to the ongoing fighting on the front lines, both sides are increasingly focusing on their air campaigns to destabilise the adversary as much as possible. Russia is primarily targeting Ukraine's energy infrastructure and elements of the Ukrainian military establishment – including Western military support – in an effort to overwhelm Ukraine's air defence systems. Meanwhile, Ukraine continues to strike targets within Russian territory, mainly focusing on military objectives such as airports, ammunition depots, and logistical hubs, to apply maximum pressure on Russian operational planning.

Although Ukraine remains at a numerical disadvantage compared to Russia in terms of military equipment, a military-industrial battle is unfolding between the two sides. Each is racing to develop and produce increasingly innovative and disruptive weapons systems, as illustrated by the numerous drone attacks seen throughout 2024.

How long can this war economy be sustained? The outcome of this conflict will depend not only on battlefield victories but also on the resilience of Ukraine and the continued support of the international community.

Electromagnetic Warfare At Its Peak

> **The conflict in Ukraine is marked by the particularly effective and disruptive use of unconventional, innovative, and often improvised means**

A largely unfamiliar form of combat – based on the intensive use of the electromagnetic spectrum – is raging between the two sides on all fronts: electromagnetic warfare.

On one side, telecommunications and electromagnetic navigation systems, including satellites, are being jammed. Radar is used both for defence and offence, and communication systems (including mobile phones) are exploited to locate and strike the adversary. A direct consequence of this war in the airwaves is a return to basic tools that had barely been used since the Cold War. Operations are now being conducted using maps, compasses, and even wired communication systems that are independent of power supplies.

On the other side, both parties are making extensive use of UAVs (Unmanned Aerial Vehicles). The trend toward medium- and large-scale military systems has faded, giving way to the use of commercial or custom-built micro and mini drones assembled from parts sourced globally. These drones are often equipped in an improvised fashion with a wide variety of payloads, such as sensors, jammers, explosives, and more. Their roles now span a wide range of missions on land, at sea, and in the air. Among other things, these UAVs are used for intercepting and spying on communications, detecting and identifying the enemy through electromagnetic or visual means, and conducting direct or indirect strikes to physically destroy targets.

New Challenges For Satellite Imagery Analysts

In modern warfare, it is no longer realistic to assume that a ground manoeuvre can escape satellite surveillance. While this provides a major advantage in terms of global coverage and access to information, it also presents new challenges.

Less restrictive legislation, lower launch costs, and the rise of technologies such as miniaturisation and 3D printing have democratised access to space for both state and non-state actors. This has led to an exponential increase in the number of low-orbit observation satellites and is paving the way for near-permanent coverage in the coming years.

Armed Conflicts

In the context of armed conflicts, this growing accessibility to satellite imagery for strategic, operational, and tactical purposes presents new challenges that intelligence and defence services will need to address in the future.

For example, the Russian-Ukrainian conflict shows that both sides are making use of this growing wealth of information and that countermeasures like optical decoys and digital camouflage are increasingly employed to avoid constant surveillance.

Space, an Operational Area

Space has long become an operational domain, and the volume of imagery to be analysed continues to grow. Since the late 1990s, the SGRS has developed its satellite imaging capabilities, with sensors playing a key role in achieving information superiority. Given these developments, it will be important to further strengthen our human analysis capacity – which will eventually be supported by artificial intelligence – and to enhance collaboration with our partners.

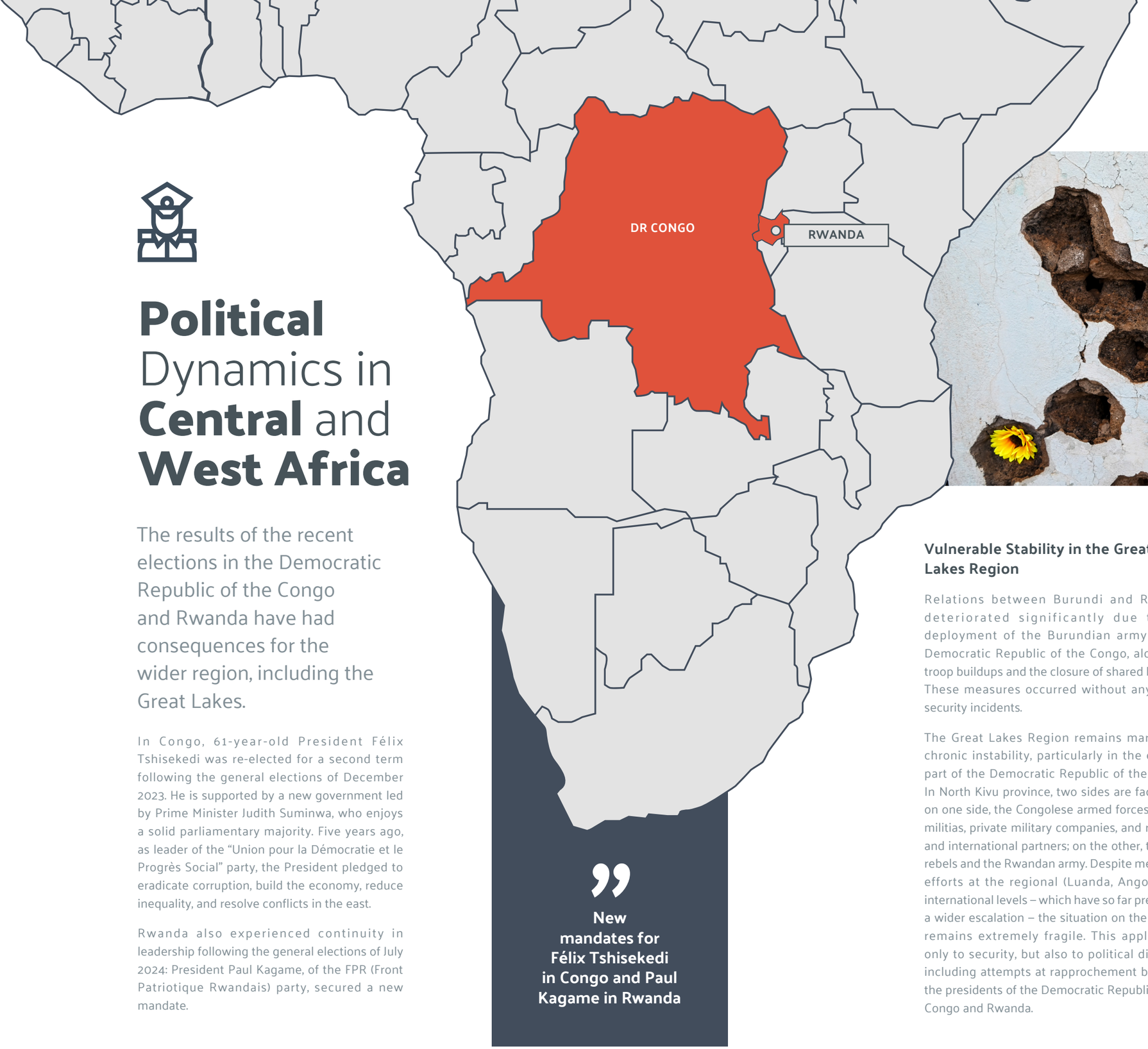
Improved global coverage is a clear advantage, and the "Alliance Persistent Surveillance from Space" (APSS), signed by 16 NATO countries including Belgium in 2023, illustrates this shared recognition. Integrating government and commercial sensors into a virtual constellation for coordinated and effective surveillance is essential to the continuation of our intelligence operations, among other goals.

Political Dynamics in **Central** and **West Africa**

The results of the recent elections in the Democratic Republic of the Congo and Rwanda have had consequences for the wider region, including the Great Lakes.

In Congo, 61-year-old President Félix Tshisekedi was re-elected for a second term following the general elections of December 2023. He is supported by a new government led by Prime Minister Judith Suminwa, who enjoys a solid parliamentary majority. Five years ago, as leader of the "Union pour la Démocratie et le Progrès Social" party, the President pledged to eradicate corruption, build the economy, reduce inequality, and resolve conflicts in the east.

Rwanda also experienced continuity in leadership following the general elections of July 2024: President Paul Kagame, of the FPR (Front Patriotique Rwandais) party, secured a new mandate.



New mandates for Félix Tshisekedi in Congo and Paul Kagame in Rwanda

Vulnerable Stability in the Great Lakes Region

Relations between Burundi and Rwanda deteriorated significantly due to the deployment of the Burundian army in the Democratic Republic of the Congo, alongside troop buildups and the closure of shared borders. These measures occurred without any major security incidents.

The Great Lakes Region remains marked by chronic instability, particularly in the eastern part of the Democratic Republic of the Congo. In North Kivu province, two sides are facing off: on one side, the Congolese armed forces, armed militias, private military companies, and regional and international partners; on the other, the M23 rebels and the Rwandan army. Despite mediation efforts at the regional (Luanda, Angola) and international levels – which have so far prevented a wider escalation – the situation on the ground remains extremely fragile. This applies not only to security, but also to political dialogue, including attempts at rapprochement between the presidents of the Democratic Republic of the Congo and Rwanda.

New Alliances and Growing Insecurity in the Sahel

In the Sahel, the military juntas of Mali, Burkina Faso, and Niger have strengthened their ties through the creation of a confederation – the Alliance of Sahel States (AES). In doing so, they have formally distanced themselves from the Economic Community of West African States (ECOWAS).

As relations with Western countries weakened, the AES countries forged closer ties with Russia, which has also become militarily active in West Africa amid the global power struggle.

Despite these new alliances, security in the Sahel continues to deteriorate. Terrorist activity is spreading further north into neighbouring countries such as Benin, Togo, Nigeria, Côte d'Ivoire, and Ghana. In addition, the risk of new coups remains high in the AES junta-led states.

The Near and Middle East Remain Volatile

7th October 2003

More than a year after the Hamas attack on Israel on 7th October 2003, the war in the Middle East continues to intensify and, above all, to spread.

After a continuous escalation between Israel and Hezbollah, in which the red lines on both sides have been pushed back several times, Tel Aviv has launched a series of air strikes against Lebanon since September 2024. Israeli troops began incursions into the south of the country in early October, marking the launch of Israeli ground operations in the Land of the Cedars.

These strikes not only caused the exodus of many inhabitants of South Lebanon, but they also prompted many Belgians living in Lebanon to leave the country. Thanks to the information gathered through both our human and technical resources, we provided an accurate and continuous security assessment, particularly for the crew responsible for the assisted repatriation of Belgians.

Louise-Marie (LoMa) in the Red Sea
121 days

Axis of Resistance

The ongoing conflict in the Middle East is not limited to Gaza and Lebanon. It is defined by the confrontation between Israel and Iran, which has led to the mobilisation of several actors under the umbrella of the "Axis of Resistance." This anti-American and anti-Israeli alliance–comprising Iran, Syria, Hezbollah, the Houthis, Hamas, and Iraqi-Syrian Shiite militias–is central to the region's security dynamics.

The Houthis soon distinguished themselves by threatening global maritime traffic with their operations in the Red Sea against Israeli targets or those identified as allies of Israel. These actions disrupted transit through the Bab-el-Mandeb Strait and the Suez Canal, both vital to international trade. Belgium contributed to operations aimed at ensuring freedom of navigation in the region. The frigate Louise-Marie (LoMa) completed a 121-day mission in the Red Sea as part of Operation ASPIDES and in the Strait of Hormuz under Operation AGENOR. The SGRS supported this intelligence mission from the preparatory phase through the entire operation.

Syria and Iraq

In the wake of the conflict between Israel and Hamas–and later Hezbollah–Syria, which hosts numerous pro-Iranian militias, found itself in the eye of the storm and has increasingly been targeted by Israeli strikes. In addition, since October 2023, multiple drone, rocket, and short-range ballistic missile attacks have hit American bases in Iraq and Syria. These bases are tasked with fighting the Islamic State under Operation Inherent Resolve (OIR).

In Syria, the Islamic State has taken advantage of growing instability due to the ongoing conflict in Gaza and South Lebanon. Although the group has established franchises across various continents–notably Islamic State Khorasan in Afghanistan, which also has international ambitions–its core remains in Syria and Iraq. Several thousand fighters are still active there, while a few thousand more are in captivity, often held by the Syrian Democratic Forces.

Role of Belgium and the SGRS

While Belgium has previously repatriated women and children in carefully coordinated operations with the SGRS, others remain detained in Syrian camps and prisons. There is a real risk that these facilities could once again become targets for Islamic State members attempting to free fighters and sympathisers. Although Belgium no longer participates in Operation Inherent Resolve with F-16s or Special Forces, the country still maintains several liaison officers within the operation. The data we collect through our various sources on the ground is analysed by our specialists to provide accurate and forward-looking intelligence. This information helps ensure that our political decision-makers are kept as well-informed as possible about developments in the field and their broader security implications–both regional and international.

Security Clearances and Verifications: An Ever-Increasing Workload

Military security involves not only defence infrastructure but also personnel and national interests. Security verifications and clearances are conducted for Defence and the defence industry in cooperation with various partners, including the the VSSE Service and the Federal Police.

Civilian and military applicants–those who have not yet started working for Defence–undergo a security verification before potentially obtaining their clearance, should they require access to classified information.

Verification is also necessary for individuals or companies outside Defence that require regular access to Defence quarters or installations. Examples include cleaning companies and consultants contracted by Defence.

Verification involves cross-checking various partner databases (local and federal police, the Federal Public Service, Justice, etc.) to determine whether the person is known, either positively or negatively, to these services.

The SGRS also handles verification requests from other partners. These concern, for example, personnel from Brussels Airport and regional airports, the Port of Antwerp, or the Federal Agency for Nuclear Control (FANC).

300.000

security verifications are carried out each year.

70%

The number of requests has increased over the past two years.

A security clearance is essential for all military and civilian Defence personnel who have access to classified information. It confirms that the necessary guarantees of loyalty, discretion, and integrity are met by the new employee. This clearance also grants access to classified areas or classified IT networks.

Clearances are also required for private companies (legal entities) contracted by Defence and needing privileged access. This applies, for instance, to companies working on various weapons systems such as the Land Component's CaMo (Motorised Capability) programme, the Navy's new frigates, or the F-35 fighter-bomber of the Air and Space Component.

Clearances are valid for up to five years and are based on the results of a security screening. The scope and duration of this screening depend on several factors, including the required level of security (confidential, secret, or top secret), and are guided by the principle of 'need to know'–meaning individuals are granted access only to the information necessary to perform their duties.

The applicant must consent to the screening being conducted. The screening concerns not only the applicant but also their broader environment (spouse, adult children, household members).

The SGRS also issues clearances for other companies, such as aerospace firms (e.g. SABCA or ASCO), which may not have a direct relationship with Defence.

Security screenings take time to conduct thoroughly. Delays can be caused by personal circumstances such as the number of people in the household, a new partner, or multiple moves. Information may also need to be obtained from abroad or through foreign services–for example, in the case of cross-border workers or international assignments – which adds to the processing time.

15.000

Each year, on average, 15,000 screenings are conducted, 6,000 to 9,000 of which are industry-specific.

More than **20.000**

Over 20,000 of Defence's 27,000 civilian and military personnel have been authorised.

15.000

In 2024, 15,000 screenings were conducted – a 33% increase – mainly due to the number of ongoing projects, particularly the new Defence weapons systems.

The **SGRS** as an Indispensable Link in the Future of the **Air and Space Component**

Belgium's 2024 F-35 programme was heavily prepared in part by the SGRS. To ensure an efficient and centralised approach, the Directorate of Security set up the Special Access Program Central Office (SAPCO). This cell is ultimately responsible for all security aspects of the Belgian F-35 programme, including military security, cyber security and counter-intelligence. In the future, this unit will also monitor the security of other advanced weapon systems within Defence.

The top speed is approximately

1900 km/h

Progress of the F-35 Programme in 2024

A major achievement was the drafting and implementation of the « Construction Security Plan » for the high-security operational buildings of the new F-35 complex at the Florennes and Kleine Brogel air bases. Thanks to this plan, the security of the construction work can be guaranteed.

In preparation for the reception of the first F-35 aircraft in autumn 2025, the build-up and reinforcement of specific F-35 security personnel at Florennes was carefully managed and supervised by the SAPCO. This was done in close cooperation cooperation with the relevant services of the Air component, and included the recruitment and training processes for specialised security teams. These teams of general security experts and cyber security specialists will be responsible for protecting both the infrastructure and operations surrounding the F-35 aircraft. A specific training plan was prepared and implemented in preparation for the preparation for the reception and operational deployment of the first aircraft.

At the end of 2024, the « Building Occupancy Date » for the operational building of the F-35 complex at Florennes was achieved. This important milestone marked not only the delivery of the building, but also the full operational functioning of all safety systems. It also forms the basis for the smooth installation of all networks, information systems and flight simulators later this year. The SAPCO played a crucial role in this by coordinating between the various services involved within Defence and private partners.

An Important Step in Infrastructure

In addition, a « Design Review Process » for the future deployable infrastructure for F-35 operations abroad was also successfully completed. This process ensures compliance with various pre-construction safety requirements. The US security authority has now granted permission to proceed to the implementation phase, marking an important step forward in the realisation of this infrastructure.

Strict Control by the United States

The Belgian F-35 programme is closely monitored by the United States as a Special Access Program (SAP). These oversight measures are necessary to ensure and protect the high-tech features of this weapon system. Access to information, facilities and operational procedures is strictly regulated to ensure the integrity and security of the programme.

Moreover, in autumn 2024, the US security authority conducted a successful inspection of the F-35 facility at its headquarters in Evere.

The Programme's Success

The SAPCO always played an active role in various working groups and symposia throughout 2024, with safety always playing a central role. Participation in these events is essential for the success of the programme. They provide an opportunity to cooperate with European and American partners, exchange experiences and build expertise. In this way, The SGRS, and by extension Defence, contribute to the further development of the international F-35 programme and strengthen interoperability among all F-35 partner nations.

These achievements underscore SGRS' undiminished commitment to the highest security standards within the F-35 programme and to ensure the deployment and protection of this strategic weapon system to the maximum.

Protecting Classified Systems from TEMPEST Attacks

Every CIWS (Communication, Information, and Weapon System) emits a certain level of unintended radiation. This radiation can reveal information about the data being processed by the CIWS at that moment. If the information is classified, and the radiation is intercepted and analyzed, it could lead to a serious security breach. Using antennas, hardware, and software, it is possible to reconstruct images and documents displayed on the CIWS screens without any physical connection. TEMPEST targets these vulnerabilities and provides countermeasures. Daily fare for SGRS' Cyber Command.

The Nature of TEMPEST Attacks

TEMPEST attacks are considered the "ideal" cyberattack because they do not require physical access to the classified data or the CIWS itself. The sensitive information is unintentionally broadcasted, and its capture leaves no trace. TEMPEST security measures focus on assessing how much this radiation is attenuated, either by the building's structure (zoning) or by the CIWS' own features (profiling).

TEMPEST Zoning: Shielding Through Building Design

TEMPEST zoning measures the effectiveness of a building's ability to block or reduce this radiation. Factors such as construction materials, window presence, and wall thickness contribute to this attenuation. The goal is to define an "inspectable space," a three-dimensional area around the CIWS where a TEMPEST attack is unlikely because it can be easily detected or prevented by local security measures. Zoning involves placing a transmitter in the room with the CIWS and a receiver at a strategic point where radiation could be captured. The captured data is then analysed to assess how well the building shields against the radiation. Periodic zoning assessments are required whenever a classified CIWS is newly installed or when the building's exterior changes.

Challenges in Zoning Assessments

One of the main challenges of TEMPEST zoning is identifying the most advantageous location for a potential interceptor. Weather conditions can also affect these measurements, as rain or other environmental factors can temporarily alter the strength of the signal. Zoning assessments are critical in any location where classified information may be at risk, including military bases, international institutions like NATO and the EU, and private companies that work closely with the defence sector.

TEMPEST Profiling: Assessing System-level Protection

TEMPEST profiling takes a different approach by measuring the CIWS's built-in ability to limit radiation. This involves setting up the system in an anechoic chamber, a controlled environment that blocks all external radiation, allowing only the CIWS' emissions to be measured. The captured data is then analysed to determine the TEMPEST level of the CIWS, which indicates how effectively it can shield itself from leaking sensitive information.

The combination of TEMPEST zoning and profiling is key to minimising the risk of a TEMPEST attack. For instance, a CIWS with low internal protection against radiation (poor TEMPEST level) should be placed in a highly shielded building (good TEMPEST zone). Conversely, a system with a high TEMPEST level can afford to be placed in a location with lower shielding because its own design limits radiation leakage.

The Growing Importance of TEMPEST Security

The importance of TEMPEST is expected to grow significantly soon. Almost every military system–from tanks and ships to aircraft and weapons systems–relies on sophisticated processors. As these systems increasingly adopt wireless technologies, the risk of TEMPEST attacks becomes even greater. Rapid advances in electronics, with ever-smaller components and greater processing power, also add to this challenge.

TEMPEST is a concern not only for system designers but also for end users. Designers must incorporate TEMPEST considerations from the outset, while users must remain vigilant and strictly follow security protocols to ensure that sensitive information remains protected from eavesdropping.

The **SGRS** and the **Protection** of **Belgian Industries**

Belgium, strategically located in the heart of Europe, boasts a diverse industrial sector that is vital to its economy and security. Protecting these industries from escalating threats–whether cyber, economic, or physical–has become a national priority. The Bureau of Industry plays a central role in safeguarding this sensitive sector and collaborates closely with the National Security Authority (NSA) and other national and international organisations.

The Bureau of Industry is a key player in Belgium's economic and industrial security system. Its primary missions include:

1 **Overseeing the Security of Defence-related Companies:**

The Bureau manages the security clearances of around a thousand companies. This is achieved through both conducting security checks and advising companies on protective measures, security standards, and regulations.

2 **Raising Awareness and Providing Information:**

The Industry Department possesses significant expertise in industrial security, which it uses to inform companies about best practices. This includes raising awareness of cybersecurity, safeguarding classified information, and securing sensitive infrastructures.

3 **Collaborating With the National Security Authority (NSA):**

Since January 1, 2024, the NSA has become a decision-making body under the guidance of the VSSE. In this context, the Industry Service and the NSA are working together to harmonise security standards for Belgian companies active in strategic sectors. This includes strict rules for protecting sensitive information and managing security incidents.

4 **Safeguarding the Role of the Military Designated Security Authority (DSA):**

On the international stage, relationships with the NSA and/or foreign DSAs are essential for exchanging transport plans and Requests for Visit (RFVs), drafting Programme Security Instructions (PSI) and Security Aspect Letters (SALs), and collaborating in international working groups.

5 **Coordinating Security Checks:**

As part of its contracts with Belgian Defence, the Bureau ensures that each individual undergoes security checks. This process protects personnel on military bases, controls information flow, and prevents TESSOC (Threats to Security of Communications and Data) risks.

Thanks to enhanced cooperation with the National Security Authority in 2024, the NSA and the Industry Service will jointly strengthen the security of classified information, critical infrastructure, and risk prevention for Belgian industries. In the future, this cooperation will be increasingly crucial to adapt to technological and geopolitical changes and to maintain a high level of protection for Belgium's industries.

Technology at the Forefront

Protecting our economic and scientific potential

Technology plays a pivotal role in the global power struggle. A fierce race for innovation and advanced technologies is underway, and the winners of this race gain not only economic but also strategic and military advantages. Some superpowers and malicious actors have been using a "harvest now, decrypt later" strategy for several years. This approach involves storing large quantities of highly sensitive encrypted data that are temporarily inaccessible, with the aim of decrypting them once quantum technology makes it possible.

New Security Systems

The major Western powers are gradually recognising the importance of protecting their economic and scientific potential. Europe (in 2023) and the United States (in 2022) introduced regulations to encourage semiconductor production and innovation, while safeguarding their industries from the threat posed by certain hostile states. Europe has also implemented a screening system for Foreign Direct Investments (FDI), which has been adopted into Belgian legislation and has just completed its first year of operation. The SGRS is an integral part of this screening system and has initiated several FDI projects that underwent specific measures (conditions and guarantees). Overall, this screening process covered a total investment amount estimated at 173.3 billion euros, including 2.06 billion euros for Belgium.

Moreover, the war in Ukraine has underscored the importance of technological superiority in military conflict. Despite its numerical inferiority and limited strategic depth, Ukraine has been able to stand firm thanks to advanced Western equipment. This technological advantage also serves as a deterrent, as any potential adversary will hesitate before engaging in armed conflict if it believes it is technologically inferior. This situation is evident in contemporary regions of tension, such as Taiwan.

Protection of Technological Development

This is one of the reasons why Belgium is strongly committed to technological development through DEFRA (Defence-Related Research Action) projects and collaborations between universities, the public, and the private sectors. The SGRS plays a key role in protecting these defence industries and research projects from espionage, interference, and disruption. The SGRS has successfully prevented companies controlled by hostile nations from participating in these research projects.

Its efforts in this regard not only prevent unwanted technology transfer but also safeguard the reputation of our defence industry and research centres as reliable partners who prioritise the security of their research.

Information Warfare: **A Bull's Eye**

For the Information Warfare department, 2024 marked the convergence of several previously launched initiatives, including its leading role in a Federal Interdepartmental Working Group monitoring Foreign Information Manipulation and Interference (FIMI [1]).

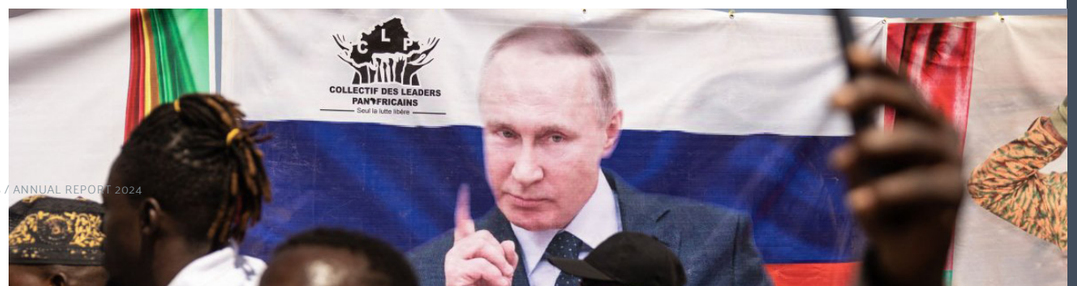
This monitoring extended beyond the various elections and was further challenged by Belgium's EU Presidency.

In the lead-up to both events, the working group established procedures and designated structures –both within the SGRS and at the federal level – to ensure coordinated detection, analysis, and reporting. One example was the early warning "Red Flag System."

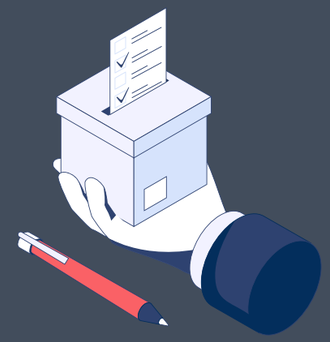
On both election days–9 June for the Belgian federal, regional, and European elections, and 13 October for the municipal elections–our service observed certain FIMI activities. However, Cyber Command stresses that these actions were minor compared to the longstanding disinformation campaigns conducted by certain state and non-state actors and their proxies, targeting Belgian, EU, and broader Western audiences. In early January 2024, the World Economic Forum's Global Risk Report ranked misinformation and disinformation as the top short- and long-term global threats. The Belgian federal government has recognised the need for coordinated FIMI monitoring since 2021.

Particularly following Russia's invasion of Ukraine in February 2022, our service observed a sharp increase in digital influence activities. The evolving geopolitical context has since only intensified FIMI activities directed at Western and Belgian audiences. Recently, FIMI has taken a central place among hybrid threats. Events in the Middle East, as well as in Africa, are increasingly being instrumentalised for influence purposes. These efforts have not only international repercussions, but also economic and social effects on Belgian society itself.

[1]Foreign Information Manipulation and Interference (FIMI)



Trends Before, During and After the Elections



State actors

The Russian disinformation and propaganda ecosystem intensified its operations. Events in the Middle East were exploited to manipulate perceptions and polarise Western audiences. The war in Ukraine also served as a vehicle for disinformation designed to divide the EU and NATO and weaken allied support for Ukraine.

Russian FIMI efforts remain active in the African information space. On the contrary, by engaging local influencers, Russia continues to expand its influence – including among African diaspora communities in the West.

Belgian information landscape

Belgium's announced delivery of F-16 fighter jets to Ukraine shortly before the European and federal elections triggered an increase in Russian FIMI activity. Similarly, the pledge to send three Caesar howitzers just ahead of the local elections led to unprecedented, persistent DDoS (Distributed Denial-of-Service) attacks targeting Belgian infrastructure.

Leading up to the elections, there was a marked rise in anti-immigration narratives and growing anti-establishment sentiment. January and February 2024 saw coordinated inauthentic activity, particularly during the farmers' protests. Various influence operations also exploited the "Gaza context" to inflame public emotion.

AI & Platforms

Artificial intelligence (AI) has become a game changer in FIMI, enabling the rapid creation of memes, avatars, fake accounts, and more. Its accessibility has driven a steady increase in AI-enabled disinformation.

On social media–particularly X–disinformation, propaganda, and extremism continue to grow.

TikTok also raises growing concerns for security services due to the lack of transparency around its algorithms, its dissemination of Russian propaganda, and its polarising effects.

Telegram, which gained attention during the COVID period, is attracting a wider audience but remains a hub for conspiracy theorists and anti-establishment content.

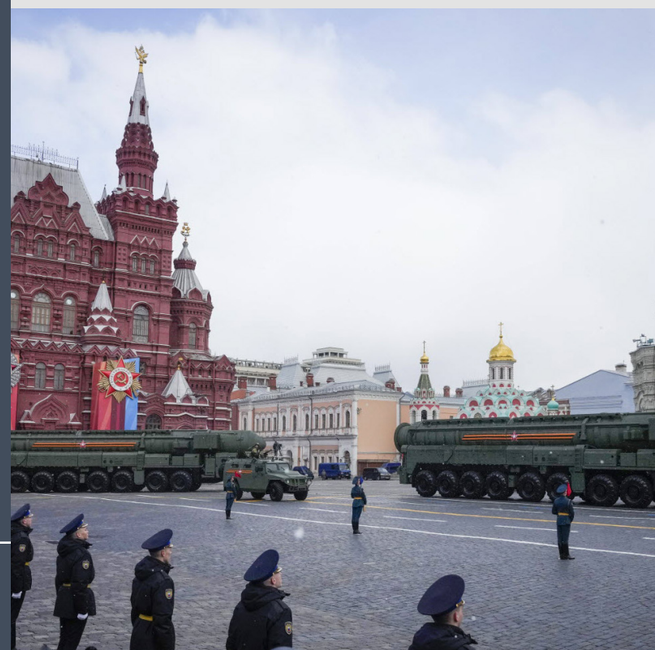
Proliferation: **the Dangerous Acceleration**

The proliferation of weapons of mass destruction (WMD) and of related technologies, a trend already noticeable in 2023, further continued in 2024 and even accelerated.

Russia is still constantly using nuclear coercion as part of its confrontation with the West and to influence the course of the conflict in Ukraine in its favour.

This coercion goes hand in hand with openly stated intentions to launch or revive strategic programmes. It also aligns with a global acceleration in the spread of strategic weapons systems and related technologies – trends that are reshaping the global norm and undermining the historical WMD non-proliferation architecture.

Technological and capability developments in other countries – particularly China, North Korea, and Iran – are also concerning, especially where they involve WMD and the proliferation of related technologies in breach of existing international standards. This trend, unfolding against a backdrop of heightened tensions in various regions, risks accelerating the arms race and increasing the likelihood of miscalculation.



A launch system for the RS-24 Yars ballistic missile is displayed in Moscow's Red Square.

Photo: Sipa/Ap/Alexander Zemlianichenko

ADIV - SGRS / PART II

Belgium in the **Spotlight**

The situation in Belgium is inextricably linked to this international context, exposing the country to a wide range of threats–many of which are interconnected. Adversaries increasingly resort to hybrid tactics to achieve their objectives and gain strategic advantage. International developments can incite violent acts on Belgian soil, carried out by radicalised extremist individuals or groups. Belgium's role as a member and host of EU and NATO institutions makes it an attractive target for espionage and interference activities.

Geopolitical Tensions and Their Impact on Belgium

The current geopolitical climate – marked by international tensions and conflicts, alongside a society that is increasingly globalised and polarised – presents several threats. The war in Ukraine and Belgium's position on the matter are provoking responses from Russia toward our country.

For example, Belgium has been added to a list of so-called 'unfriendly countries' by Russia. While Russia's nuclear doctrine may not be cause for immediate alarm, it does explicitly target Belgium. Growing global polarisation complicates relations with African states, where military collaborations have, in some cases, been suspended or cancelled. Internationally, these threats materialise in the form of armed conflicts and terrorism.

The concept of 'hybrid warfare' refers to activities that remain below the threshold of the traditional approach to warfare but which could cause harm to Belgium. This year, for example, cyber attacks such as the DDOS campaign against government institutions, disinformation targeting extremist groups, espionage and sabotage were observed.

Threats to Defence

Defence must also address these threats. As Defence personnel are a reflection of society, they too can be vulnerable to extremist ideologies and to foreign influence and interference. Geopolitical tensions have led to heightened vigilance against sabotage targeting critical infrastructure – both civilian and military. Moreover, due to its missions, Defence remains an appealing target for espionage. In that respect, 2024 followed the same trend.

The SGRS plays a multifaceted role in countering these threats. On one hand, it focuses on prevention by raising public awareness wherever possible. On the other hand, its personnel actively detect potential risks and, when necessary, implement appropriate measures.

Our Partnerships, **Vitally Important!**

The globalised and sophisticated nature of contemporary threats–such as terrorism, cyberattacks, disinformation campaigns, and disruptive technologies – necessitates a joint approach based on partnerships. By pooling resources, expertise, information, and intelligence, we can improve threat analyses, enhance operational capabilities, and broaden our understanding of the challenges. This will enable us to better anticipate, prevent, and respond to new threats.

To this end, the SGRS has both an international relations office and, more recently, a national relations office, which serve as the points of contact for official relations and activities with various partners.

Some of these partnerships are traditional yet extraordinary due to their substantive depth, such as the one with the VSSE. But beyond such traditional security partners, there is a growing need for less conventional partnerships.

The SGRS faces a highly dynamic landscape of security challenges, ranging from new military threats to rapidly evolving cyber and hybrid techniques and tactics, which demand innovative solutions.

The SGRS aims to stay ahead of these developments by leveraging advanced technology and fostering a culture of continuous training and development. Partnerships are essential in this regard.

A Fragment of SGRS' Collaboration Network and the Cyber Command

The Service's network spans a wide range of partners and collaborations. For instance, the SGRS and the Cyber Command now work regularly with professors from a dozen universities and colleges. These collaborations often focus on highly specialised topics, such as future-oriented technologies or very specific fields of knowledge like cryptography. Moreover, the SGRS and the Cyber Command share their intelligence expertise with students, for example at the Universities of Ghent and Liège.

The Service also works regularly with around twenty companies, usually – but not exclusively – in the defence industry. Examples include collaborations with companies specialising in artificial intelligence or language technologies.

EU and NATO

The EU and NATO are multinational organisations with their own intelligence services. The intelligence services of their respective member states work together within the EU and NATO frameworks. The SGRS actively participates in this cooperation, which includes the exchange of information and analyses. Experts take part in specialised working groups and help develop joint threat analyses, assessments, and potential future scenarios. As part of Belgium's commitment to national and international cooperation and security, the SGRS thereby contributes to broader peace and stability.

Our Sister Service, Our « Partner in Crime »
The SGRS and the VSSE: Stronger Together

The SGRS and the VSSE have a long history of close collaboration. In the field of counterespionage, for instance, this cooperation is certainly nothing new, yet in recent years it has been particularly strengthened within an increasingly formal framework.

In addition to the official cooperation agreement of 2004, two joint strategic plans were drawn up in 2018 and 2022: the National Strategic Intelligence Plan (NSIP). Its objective was to develop many synergies between the two services.

Joint platform

Both services have not been idle in the meantime. The platform for the fight against extremism and terrorism was officially launched in April 2024. The sister services had already been working together on counterterrorism since 2018, following the attack, at the request of the parliamentary commission. This collaboration primarily focused on Sunni-inspired terrorism. The issue of counter-extremism was added this year, making the platform an expansion of the previous collaboration, with a current focus on both religious and ideological terrorism and extremism – regardless of the origin or target of the threat, whether military or civilian.

According to the platform coordinator:

"The combination of both intelligence services allows us to pool our capabilities and have easier access to our respective partners. Within our platform, we no longer distinguish between military and civilians. Everyone on the team is aware of all the files; nothing is kept secret. In the end, we are all working towards the same end goal."

ADIV - SGRS / PART III

Results of cooperation

These joint efforts with the VSSE have not only resulted in a common platform but also in additional achievements.

In the field of counterespionage and counter-interference, there is increasing cooperation, including joint operations. Both services will be able to share their information sources, according to clear and defined procedures, and gain mutual access to data held by the other. In addition, they will work together on the development of digitisation projects, with a strong focus on the use of common information and communication technologies to improve the efficiency and effectiveness of both organisations.

This cooperation between the two Belgian intelligence services reinforces their complementarity and guarantees the efficient and effective execution of their respective legal missions, in accordance with their specific characteristics: the SGRS as a military and externally oriented service, and the VSSE as an internally oriented service.

A joint sensitisation session with the VSSE to raise awareness among members of parliament of digital risks on 10 December 2024

Partnerships at the Heart of **Europe's Digital Defence Strategy**

The Belgian presidency of the European Union in 2024 comes at a critical time for European security, marked by escalating digital threats and geopolitical tensions. Cyberattacks and digital destabilisation are growing concerns for the EU and its member states.

Egmont-format

During its presidency, Belgium convened European defence experts, cybersecurity specialists, and diplomats in the so-called Egmont format to address pressing issues. This platform facilitates strategic development, information exchange, and stronger partnerships among member states.

A key takeaway from the Egmont meetings was the vital role of robust partnerships in confronting complex cyber threats. It underscored the need to view national security through a broader European lens. No single member state can tackle these challenges alone – collective resilience is essential.

Current Threats and Partnerships

Europe's increasing digitalisation makes it more vulnerable to cyberattacks targeting critical infrastructures such as energy supply, financial systems, and communication networks. The Belgian presidency recognises that supranational cooperation is indispensable. Tools like the EU Cyber Diplomacy Toolbox enable member states to respond in a coordinated manner to large-scale cyber incidents.

Both bilateral and multilateral collaborations–such as the EU Cybersecurity Act, which outlines guidelines for enhancing cyber resilience and cooperation with NATO allies–play a vital role. Strategic partnerships with countries like the US and Canada are equally crucial, given the cross-border nature of cyber threats. Platforms such as the EU-US Trade and Technology Council foster this transatlantic cooperation.

Cyber Ambassador Pierre Gillon and former Minister of Defence Ludivine Dedonder

Cyber Defence

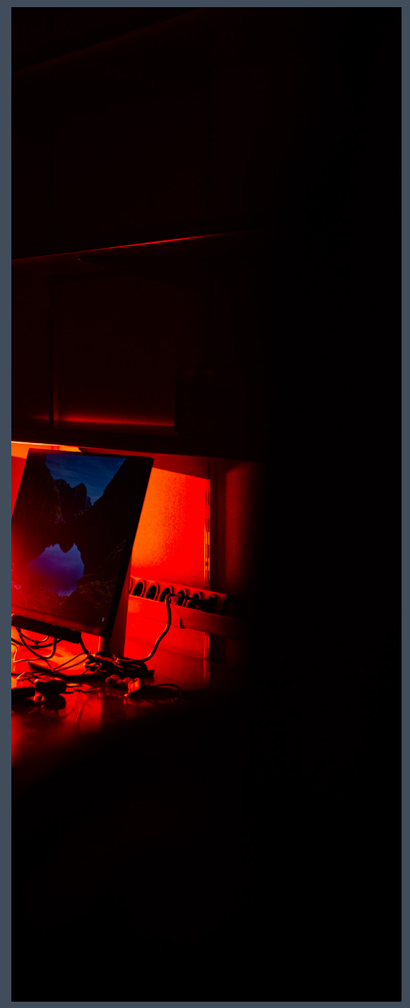
The EU Conference of Cyber Commanders (CyberCo) provides a forum for senior defence officials designated by the EU as cyber cyber commanders at the national level in their member states and other permanent members. The main aim of the conference is to improve cooperation, exchange of relevant information and coordination among member states. CyberCo is organised by each EU Council Presidency, with the support of the European Defence Agency (EDA) and the participation of the European External Action Service (EEAS), including the EU Military Staff (EUMS). CyberCo provides operational guidance for the implementation of EU cyber defence policy, validated and approved by the Council of the EU.

Cyber Diplomacy

Cyber diplomacy is rapidly becoming a cornerstone of international relations. Diplomatic engagement is needed to define global standards and norms for responsible state behaviour in cyberspace. The Belgian presidency has called for closer cooperation with the United Nations and other international bodies to establish a normative framework that unequivocally condemns cyberattacks on critical infrastructure.

Open Source Intelligence (R)evolution

The war in Ukraine has reignited attention on OSINT (Open Source Intelligence) as a key intelligence discipline. Thanks in part to the 2022 STAR plan, investments in the SGRS have been ramped up, with particular emphasis on OSINT as a vital source of information throughout the conflict in Ukraine. This has led to a significant expansion of capabilities within the SGRS and Defence, in terms of personnel, equipment, technology, and operational scope.



From Traditional Methods to OSINT 2.0 and 2.1

Although OSINT has existed for centuries, the rise of the internet and technologies such as machine learning have given it a new dimension, often referred to as "OSINT 2.0." Today, large volumes of data can be processed more efficiently and accurately. While traditional open sources–like newspapers, reports, public speeches, and maps–are long-established tools in intelligence gathering, modern sources such as social media, blogs, scientific databases, and online news outlets are now equally essential.

The integration of these technologies has turned OSINT into a critical pillar of intelligence work, alongside other disciplines like HUMINT (Human Intelligence) and SIGINT (Signals Intelligence).

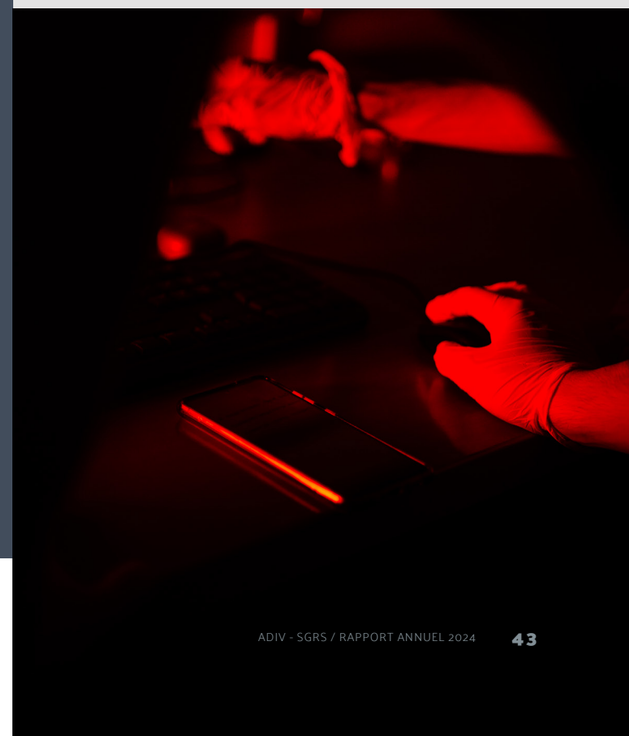
The war in Ukraine has also triggered a resurgence of classic techniques such as disinformation and fake news, which are now being deployed at scale using modern digital tools. The SGRS is closely tracking this evolution. In 2024, it launched an expanded development process for Information Warfare capabilities, aimed at verifying, geolocating, and analysing social media content. This marks the transition to what can be called OSINT 2.1. Initially focused on tactical uses – such as analysing social media posts to track Russian troop movements–this capability is now applied at both operational and strategic levels.

A New Sub-discipline

Over the past year, the SGRS has created a new sub-discipline within the DICU (Digital Influence Collection Unit) to provide stronger support to both operational and strategic intelligence, with a specific focus on Ukraine. This development includes integrating new concepts, allocating resources, and planning for personnel, with the objective of becoming fully operational by 2025.

What Does the Future Hold?

OSINT continues to grow and evolve, constantly adapting to emerging technologies and shifting geopolitical dynamics. Future investments in this field are expected to not only enhance battlefield awareness, but also improve strategic insight into the actions and intentions of governments in an increasingly complex global environment.



China, Champion of **AI-Driven Online Manipulation?**

State actors and cybercriminals are increasingly harnessing Artificial Intelligence (AI) to automate the various stages of cyberattacks. These include identifying vulnerabilities, generating malware, stealing or destroying data, and disrupting systems.

AI tools like WormGPT enable the rapid creation of malicious code and help bypass detection mechanisms. Between 2023 and 2024, companies began taking countermeasures against the misuse of AI by state actors using it for hacking and manipulation. Some of these actors have employed AI to detect software vulnerabilities, debug code, generate scripts, and craft content for (spear) phishing campaigns.

AI for Data Exploitation, Propaganda, and Opinion Manipulation

AI is not only used for technical attacks – it also plays a key role in propaganda and information warfare. Chinese apps such as TikTok, CapCut, Temu, and Shein collect large volumes of personal data and visual content, which are accessible to the Chinese government. These materials are used to train AI systems on how people outside China express emotions and communicate.

This data-driven approach enables the Chinese government to deploy AI-generated content – particularly videos – tailored to influence public opinion abroad. There have already been documented cases where such content was used to sway voter sentiment during (supra) national elections, including in Rwanda, India, and EU member states during the European elections of June 2024.

SGRS' Cyber Command is closely tracking these developments, working alongside national institutions and private-sector partners. It continually adapts its defence posture and awareness efforts in line with emerging threats and technological advancements.

Drones, Explosive Devices, and Electronic Warfare: **Emerging Security Challenges**

The use of commercial or custom-built micro and mini drones has become increasingly widespread. This trend has caught the attention not only of commercial actors but also of terrorist organisations, who are exploring the potential of equipping drones with payloads capable of performing a wide range of tasks.

In response to this concerning development, NATO has restructured some of its analysis groups. In 2024, the team responsible for countering remote-controlled explosive devices was elevated within NATO's hierarchy and received a broader task: to tackle both explosive threats and small, uninhabited radio-controlled systems using electromagnetic countermeasures.

Within this context, a Cyber Command team from the Electromagnetic Warfare Centre (EWC) contributes to NATO exercises and comparative multinational research. It is also involved in Belgian research projects assessing the effectiveness of current national military tools against such threats.

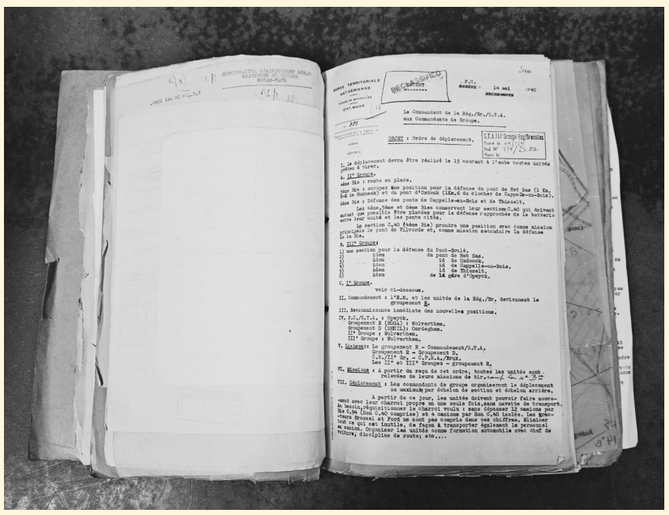
In 2024, the EWC participated in NATO's "Thor's Hammer" exercise–the largest electronic warfare drill to date. It provided an opportunity to test technologies aimed at neutralising improvised explosive devices and small unmanned systems. More broadly, these exercises serve to develop coordinated, interoperable responses to modern electronic threats.

The EWC also plays a role in several ongoing Defence operations, including Baltic air policing missions in support of F-16 deployments (BAP 2024). Defence is currently investing–and will continue to invest – in a wide array of new platforms equipped for electronic warfare.

200 Metres of Archives for the "1940-1945 Campaign" Already Catalogued

For years, classified and historical Defence archives of administrative and legal value have been stored in the vast depot housing the Classified Archives of the SGRS. Among them are military archives created during the general mobilisation of 1939, the 18-day campaign, and the subsequent occupation—collectively known as the "1940–1945 Campaign" archives. This collection spans approximately 500 linear metres, a significant portion of which has already been catalogued.

The "1940–1945 Campaign" archives hold immense historical value for researchers and contain a wealth of information. Despite their age, a large part of the collection remains classified. Politicians, the public, and the State Archives have called for their declassification. However, the process is subject to the 'third-party rule', which stipulates that classified documents originating from other countries or institutions outside Defence may only be declassified with the consent of the relevant third party—sometimes causing delays.



The detailed inventory takes into account all potential sensitivities that might hinder declassification. Archivists at the Classified Archives have no objections to declassifying the documents they have reviewed so far. As a result, the archive collection is being declassified in phases, allowing researchers to access already declassified material. Once the entire collection is cleared, it will be transferred to the State Archives. In the meantime, researchers can consult the documents in the CA reading room.

The Archive Documents that have already been Declassified:

a. I° Army corps
b. II° Army corps
c. Lists Stalags and Oflags

Support and **Development** : SGRS' Dual Commitment

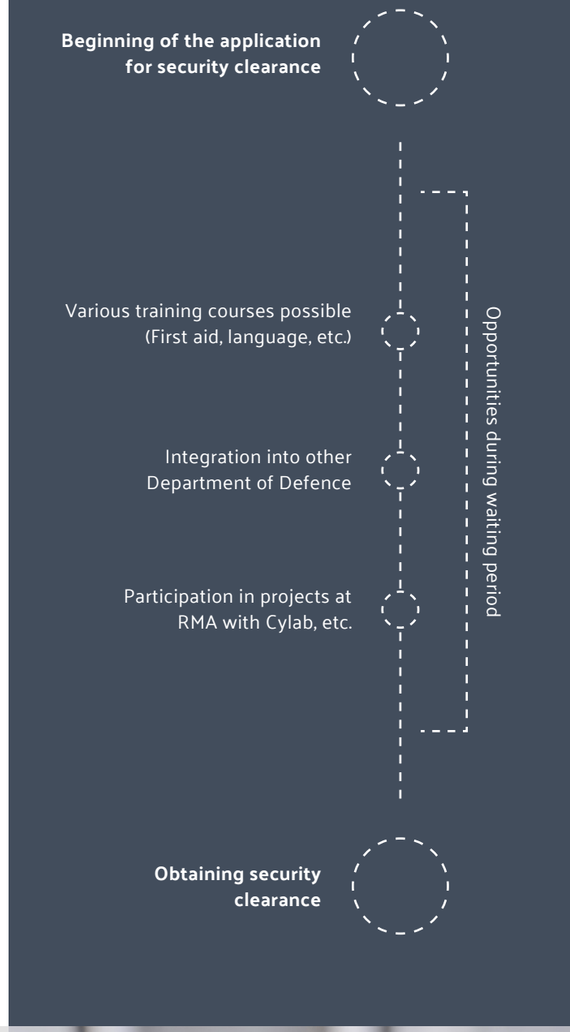
To support integration within the SGRS, the Human Resources department is developing a training programme for new arrivals. General training sessions will present the organisation and its functioning to all incoming personnel, including military personnel transferring internally. Tailored support will also be provided based on each individual's legal status.

A Programme for Support and Development

Military personnel awaiting security clearance are already able to participate in internal or external training sessions, such as first aid or language courses.

Beyond supporting new military staff, the SGRS also provides customised guidance to civilian personnel and reservists. Civilians remain in regular contact with the SGRS before officially taking up their duties. Some may also be assigned temporarily to another Defence department while awaiting the clearance required for work in the intelligence sector. For reservists, dedicated support is available, including monitoring of their training pathway and administrative records.

All these initiatives are designed to ensure new team members adapt smoothly to their new environment. The programme itself is continuously refined based on feedback from participants.



Testimonial Margaux, 24

"ACOS IS was able to offer me a temporary position in a different department to speed up my start. I would cross over in due time.

Now, both departments are involved in my onboarding and development. A handful of superiors of each unit commit to meeting monthly to ensure my alignment - past and present experience included. All allow me the freedom to set my own pace. This type of continuity as well as matching people to their potential - rather than to a job description - is what keeps on reaffirming my inkling towards this unit. Fun fact, my original point of contact remains very much on call, too."

From Integration to Action With an **Innovative** Training Programme

Fourteen military personnel who newly assigned to Cyber Command followed a tailored training programme lasting several months to master the various facets of their future role. The initiative was launched during the period in which they awaited their security clearance, offering them the opportunity to prepare efficiently before joining their respective teams.

The programme began with an introduction to the various services, followed by a speed dating session allowing each participant to express their preferences and aspirations.

Over the course of 17 weeks, the future analysts acquired a solid foundation in intelligence principles and developed critical thinking skills to achieve their goals.

The programme also included a one-day immersive exercise at the Cyber Sigint Missions Centre. This simulation – called the War Game – was designed to help determine the most suitable roles for each participant.

Testimonial Henri, 27

"The training provided an excellent foundation for starting my new role and prepared me for continued learning on the job. It combined both theoretical and practical components, particularly in stress management, offering very actionable tips for navigating new and unexpected situations.

Before attending the training, I had significant experience working on African matters for several years, followed by a career shift into the military. The program not only allowed me to apply my existing knowledge but also helped me expand it in meaningful ways.

We received in-depth training on a variety of topics, including intelligence, cyber operations, management, stress management and briefing techniques tailored to different audiences. One of the most valuable aspects was learning about military culture–how structures are organised, how efficiency is perceived, and even practical guidance on conduct, such as how to present oneself on a military base.

Overall, the training was transformative, equipping me with the tools and knowledge I needed to excel as an analyst."

The War Game: an Innovative Tool

The game is built on a simple concept: recreating battles from the Second World War to place participants in the roles of commanders and section chiefs. This immersive simulation mirrors the operational structure of the department's intelligence centres. Each centre is led by a chief responsible for selecting which weapons systems–such as intelligence collection methods–to deploy. Their mission: to identify and process relevant information in order to accomplish strategic objectives like capturing a village or neutralising enemy forces.

"This simulation helps new analysts acquire the practical reasoning skills that are essential for intelligence operations by allowing them to gain experience with the decision-making challenges they will face," explains M., head of the 'Cyber Sigint Missions Centre' department.

M. points out one of the most important advantages of the War Game: "The game quickly reveals whether the new analysts can demonstrate the necessary creativity and proactivity. In the world of intelligence, it is often crucial to go off the beaten track to gather valuable information. The world of foreign intelligence offers many opportunities, but only the most creative minds can exploit them effectively"

Testimonial Isaac, 25

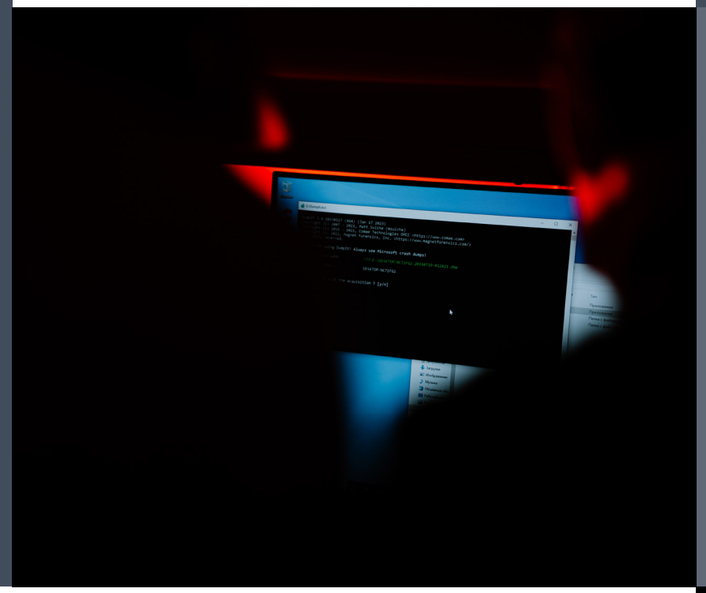
"The War Game was an invaluable experience that taught me how to make sound decisions and visualise the dynamics of military operations. It sharpened my ability to assess situations, recognise opportunities, and leverage what's in front of me to gain an advantage.

One of the most impactful lessons was learning to work effectively within a team. The exercise emphasized the importance of clear communication, especially when balancing differing opinions. We had to collaborate to identify priorities and focus on the most critical aspects to maximise results.

Overall, the War Game not only enhanced my analytical skills but also strengthened my teamwork and communication abilities – tools essential for success in any mission."

Sabrina, 28, Agent Screening

"I have been working at the SGRS for three years, including about a year as a screening agent. My job within the SGRS is to carry out security verifications for, initially, all candidates who want to work at Defence. Secondarily, we also do that for companies that have a contract with Defence and for our partner services. This includes screening people who want to do high-risk jobs, such as employees at airports or nuclear power plants."

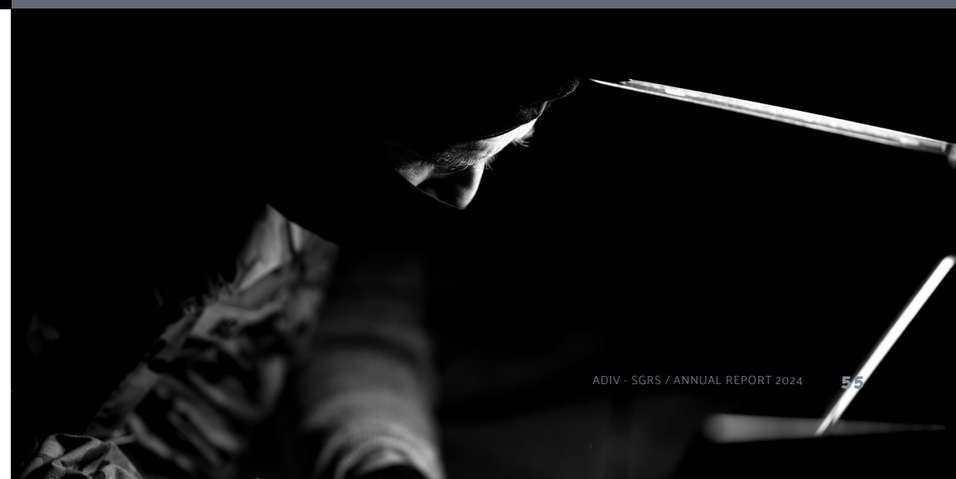


Do not hesitate to visit our website to discover our articles and news within our department.
- www.sgrs.be

ADIV - SGRS / PART V

"We mainly look at background information from databases to determine whether these people have the necessary values and integrity to hold a position at Defence, for example. Drug use, beatings and injuries, theft, etc., for example, are all factors that play an important role in making a decision. We treat each case individually and each case is considered and dealt with separately so that everyone gets an equal chance."

"With our team this year, we faced the challenge of carrying out some 300,000 screenings, often processing 150 to 200 files simultaneously. Keeping that overview is also precisely the hardest part of our job. On the other hand, I get an enormous satisfaction from my work and I really have an impact on the security of our country and of Defence. We contribute to the security of our country by ensuring that people, meet the highest standards of integrity."



ADIV · SGRS

QUAERO ET TEGO

Cyber Force
Through Partnerships

WWW.SGRS.BE