ANNUAL REPORT 2022

SGRS-ADIV

General intelligence and Security Service

Quaero et tego

Decoding
Belgian Military Intelligence, Security and Cyber Defence

DEFENSIE
LA DÉFENSE

.be

SGRS-ADIV

General Intelligence and
Security Service

CONTENTS

Responsible publisher : Vice-Admiral Wim Robberecht
Quartier Reine Elisabeth – rue d'Evere 1, 1140 Evere

Photographs : Patrick Bouillon, DG StratCom and SGRS-ADIV personnel
Graphic design : 2SeeDesign

Vice-Admiral Wim Robberecht © Patrick Bouillon

THE WORLD CHANGES, BUT OUR MISSION REMAINS THE SAME

«Quaero et Tego» is our motto; **Protecting** our country, our companies and our expatriates with our **Intelligence** and expertise is our primary mission; **Advising** the authorities wisely is our duty to our country, society and our fellow citizens.

There is no doubt that the SGRS-ADIV will remember 2022 as the year of change.

On 19 October, the SGRS-ADIV created a new structure with the main objective of better understanding current and future challenges in the fields of intelligence, security and cyberspace. The purpose of our service remains unchanged: to protect our country and our citizens, both in Belgium and abroad, against all possible and imaginable threats, but also to provide the best possible advice to our authorities, partners and industries.

This adaptation was necessary because of the profound changes that have taken place in the world and in Belgium.

It is obvious to anyone interested in intelligence, security or information processing in general that the world today is fundamentally different from the world at the beginning of the 21st century. The mechanisms that were in use 22 years ago are already obsolete in the face of today's threats. Our world has become digital - at every level of society - and requires us to process more and more information at a faster and faster rate. The world may be

changing, but information remains the essential raw material for intelligence and security services.

WE WORK FOR YOU, FOR OUR COUNTRY AND FOR PEACE

At the same time, the world is emerging from the global pandemic, licking its wounds and discovering the consequences of a new social reality. Profound changes have taken place and are influencing our behaviour and habits in almost every aspect of our lives and society.

It was therefore urgent that the SGRS-ADIV learns the right lessons from these changes and adapt accordingly in its areas of competence. These changes are creating new threats that are becoming major concerns for the population. These concerns include a growing sense of insecurity due to an increase in extremes and an increase in fraud against Internet users in cyberspace.

Each of us must be aware that threats follow the changes in our world and constantly adapt to the new realities of our daily lives. The feeling of latent instability and the impression of irreversible degradation of Belgian society are ideal conditions for malicious people to increase their presence and take advantage of this situation, especially as manipulation and disinformation have become commonplace. As a service, we help to inform our citizens about these threats and, with the support of our partners, we try to eradicate or minimise the impact of these scourges.

At the time of writing, we note that espionage and foreign interference have reached levels not seen since the Cold War. In addition to interference, the main threats to national security are violent extremism, terrorism and malicious cyber activity. In addition, war has returned to Europe's borders. In addition, other more distant conflicts are affecting our social model. It is clear that threats are evolving at an accelerating pace and affecting our populations in many ways. Ultimately, these threats pose a direct threat to our democratic system.

As Chief, I am particularly proud of my staff, both military and civilian. Often behind the scenes, they work tirelessly and in sometimes very difficult conditions to ensure that our country is best protected against threats to national security, to our citizens - at home and abroad - and to the vulnerable and critical sectors of the Belgian economy.

Together with our national partners and security actors, we are the eyes and ears of our nation. We look for what our adversaries want to keep hidden. We operate where they hide, usually in the shadows and with the utmost discretion. We study hostile powers to anticipate new threats and ensure the security of our secrets, military operations and knowledge.

We advise our political and military leaders so that they can make the best decisions, independently and sovereignly, to best protect our country and its citizens. We operate around the world, wherever our interests demand. Today, the threats to our society have become more complex, unpredictable and diverse.

ESTABLISHMENT OF THE CYBER COMMAND

CYBERSPACE HAS BECOME THE NEW BATTLEFIELD

On 19 October 2022, we officially launched our Cyber Command at an inauguration ceremony attended by many partners and journalists.

The Cyber Command is now a reality, not only for the military, intelligence and security communities, but also for civil society, academia and industry.

In line with the policy directions of our Minister of Defence, the Cyber Command will play an increasingly important societal role, not only within the sovereign microcosm of cyber security, but also towards society. The acquisition of «dual» capabilities responds to this desire to operate in both military and civilian environments.

GMJ Van Strythem

We expect the Cyber Command to grow while remaining within the intelligence and security family whose missions and legal frameworks it shares. To enable the Cyber Command to grow, the recruitment challenge is obviously our first concern. We have no shortage of assets, be it our training programmes, our military specificity or the diversity of our missions. But to attract potential candidates, we must balance open communication with meeting our security requirements.

Beyond communication, the key to the Cyber Command's success is our ability to build long-term partnerships with our operational partners, as well as with civil society actors. These partnerships are at the heart of our project and take shape with the business, academic and research communities, not to mention associations and training organisations.

They are strategically important for a number of reasons. First, they will enable us to maintain and develop the expertise needed to deal with increasingly sophisticated threats in an ever-changing environment. Secondly, they enable us to anticipate our future needs, as it is essential to have a long-term vision in line with tomorrow's society. Thirdly, they provide recruitment opportunities by creating essential links with associations in circles that are not familiar with the Belgian Defence.

It is with great pride that I will continue to commit myself and use the skills of my staff to develop the Cyber Command into a new cyber component within the Belgian Armed Forces. The challenge is huge, both in terms of personnel and current and future missions, but I am convinced that we have enough resources to face it together.

THE SGRS-ADIV WITHIN THE BELGIAN DEFENCE

Vice-admiral Wim Robberecht,
Head of SGRS-ADIV

Major Adjudant Frédéric Charlot,
Corps Adjudant

1st Corporal Bruno Wilmart,
Corps Corporal

The General Intelligence and Security Service is part of the Belgian Defence. It is the Belgian reference service for **foreign** and **defence intelligence**. The majority of its members are military personnel, although a growing number of civilians work for the SGRS-ADIV.

As the SGRS-ADIV is part of the Belgian Defence, there are some emblematic positions within it, such as Commanding Officer, Regiment Sergeant Major and Corps Corporal.

These positions are mainly concerned with the internal regulations of the service, discipline and the well-being of the personnel as a whole.

The Regimental Sergeant Major and the Corps Corporal are also responsible for the organisation and implementation of military traditions and official visits within the organisation.

The traditional military holidays are :

07 April
Veterans Day

21 July
National Day

11 November
Armistice Day

15 November
King's Day

© SFRS

MISSION

QUAERO ET TEGO
I SEARCH AND I PROTECT

The SGRS-ADIV is the Belgian military intelligence and security service.

Its mission is to collect, analyse and process information relating to any activity that could threaten the integrity of Belgian territory or the Belgian population, military defence plans, the scientific and economic potential related to defence, the performance of the missions of the armed forces and the safety of Belgian citizens abroad, as well as the activities of foreign intelligence services on Belgian territory.

It maintains the military security of defence personnel and military installations, weapons, ammunition, documents and computer systems, and protects the secrecy associated with them.

The SGRS-ADIV is responsible for carrying out security investigations and audits and for issuing security clearances, security advice and security certificates.

As part of its mission, SGRS-ADIV provides intelligence to political and military authorities in a national and international context to assist them in their decision-making.

VISION

KNOW AND INFORM

The SGRS-ADIV contributes to the protection of the interests of the Nation, the Belgian Defence and the population through an integrated security approach combining the intelligence, counter-intelligence, security and cyber dimensions, both on Belgian territory and abroad.

It is the Belgian reference service for foreign and defence intelligence.

It participates with its national partners in the maintenance and strengthening of internal security.

VALUES

OUR 10 COMMANDMENTS

1. We seek and find what others cannot
2. We trust ourselves and each other
3. We have the right people in the right place
4. We stand together
5. We work smart and hard
6. We deliver the right information, to the right person, in the right way, at the right time
7. We look to the future
8. Maintaining excellent partnerships
9. We are steeped in the culture of intelligence
10. We work in the shadows

Kathleen Van Acker

OUR STORY

When Belgium became independent in 1830, one of the first acts of the provisional government was to raise an army. As this army did not have a department responsible for intelligence gathering and analysis, the «Police militaire du Département de la Guerre» (Military Police of the War Department) was created in 1831. This new corps worked on an irregular basis with informants supervised by officers and was primarily responsible for detecting and monitoring Orangists and Republicans within the army.

The Royal Decree of 26 June 1910 established the General Staff of the Army. It was made up of four offices, including the «2e Bureau «Renseignement»» (2nd Intelligence Bureau).

At the beginning of 1911, the 2e Bureau «Renseignement» set up a border surveillance and intelligence service with 300 local gendarmes, customs officers and forest rangers.

The «Sûreté militaire belge» (Belgian Military Security) was created on 1 April 1915. Its main task was to thwart the enemy's espionage activities. In order to do this, the Service had extensive powers, including the removal and internment of criminals, suspected collaborators and spies; the power to carry out (body) searches, searches and the confiscation of weapons; the power to prevent subversive meetings; and the power to intercept private correspondence.

After the Armistice, the service was also responsible for the security of Belgian troops involved in the occupation of the Ruhr.

In 1929, the service was disbanded following a scandal involving the falsification of military plans against Germany. When these military plans fell into the hands of the Dutch press, they caused an international scandal called «Le faux d'Utrecht» (The Utrecht Forgery).

In 1937, the service was re-established in great secrecy to deal with growing German espionage.

After the Belgian campaign of 1940, the Belgian government in exile in London wanted to re-establish relations with the occupied homeland as soon as possible. Two Belgian intelligence services coexisted, each operating from London. Due to a lack of clarity about the competences assigned to the two services by the government, a turf war broke out, which affected not only the relationship between the two services, but also the cooperation with the

British intelligence services. The problem persisted until October 1942, when the new ministers of defence and justice signed an agreement defining the responsibilities of the two services.

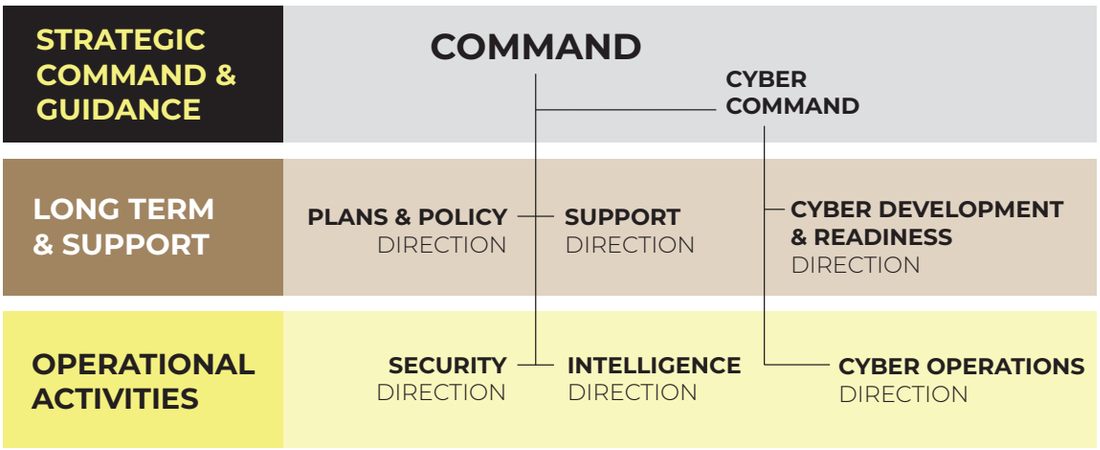
After the Second World War, the «Service de Documentation, de Renseignement et d'Action VIII» (SDRA VIII) was created alongside the Military Intelligence Service. Its main objective was to evacuate the Belgian government to a safe place in the event of a conflict and to maintain contact with the motherland. Within this framework, SDRA VIII gathered intelligence and prepared for escape missions, including the exfiltration of downed pilots or agents discovered by the enemy. It also trained in the sabotage of military targets, organised a structure to resist the enemy and was involved in counter-intelligence.

The then Belgian Minister of Defence, Guy Coëme, had to provide information on these networks at an international meeting in Brussels at the end of October 1990. On the same day, the minister summoned the head of the Service de Renseignement Militaire and the head of SDRA VIII to obtain further information.

Although no one had heard of Gladio before November 1990 and the Belgian «stay-behind» network operated independently, the SDRA VIII found itself at the centre of a media storm and conspiracy theories linking the Belgian secret network to the bloody attacks

committed in Belgium in the 1980s, notably through the files of the «tueurs du Brabant» (Brabant killers) or the «cellules communistes combattantes» (communist fighting cells). On 20 December 1990, the government decided to dissolve the underground network and launch a parliamentary inquiry. The link with possible terrorist attacks was never proven and the identity of the agents was never revealed.

OUR STRUCTURE



THE MAIN LAW THAT GOVERNS US

Article 11 of the law of 30 November 1998 on the intelligence and security services describes the missions of the SGRS-ADIV. In order to carry out these missions, the legislator has provided in the law for various methods of intelligence gathering. The various collection methods are subject to specific conditions and legal control in order to reconcile the requirements of national security with the principles and values of a democratic constitutional state.

When using these methods, the SGRS-ADIV operational managers take great care to comply with legal requirements.

With the emergence of new threats and the development of new technologies, there is always a residual risk of (unintentional) illegal action. Independent monitoring of this residual risk and of the day-to-day activities of the SGRS-ADIV is ensured before, during and after these activities by the Standing Committee of the Intelligence Services (Standing Committee I) and the Administrative Commission, which is responsible for monitoring the specific and exceptional intelligence gathering methods used by the intelligence and security services.

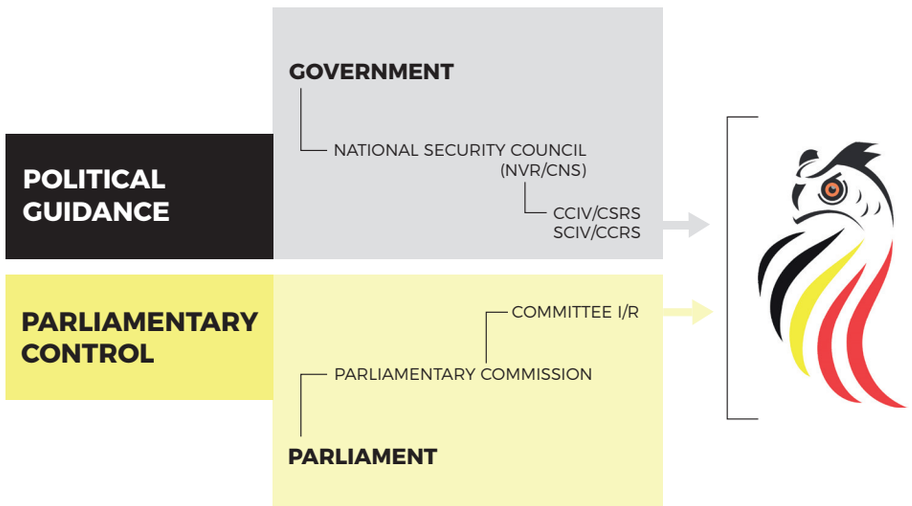
In 2022, the legislator made amendments to the Act of 30 November 1998, partly based on the recommendations of the Parliamentary Investigatory Commission «Terrorist attacks of 22 March 2016». These amendments allow the agents of the intelligence and security services to infiltrate the virtual and real worlds and to commit crimes to a greater extent, subject to appropriate control measures. Human sources will also be allowed to commit crimes, but under very strict conditions. Finally, and more specifically for the SGRS-ADIV, an additional competence has been added in the event of a national cyber security crisis.

The implementation of these new legal powers and the recommendations of the Standing Committee on the Review of the Intelligence Services following the Jürgen Conings case is a priority, although the day-to-day operational work of the SGRS-ADIV continues.

In the course of 2022, first initiatives were taken to also prepare proposals for amendments to the Act of 11 December 1998 on classification and security clearances, security certificates and security advice and the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data.

OUR COMMITMENTS

Political commitment:



The National Security Council defines and coordinates general intelligence and security policy and sets the priorities of the intelligence and security services. It also coordinates the fight against the financing of terrorism and the proliferation of weapons of mass destruction. It also defines policy on the protection of sensitive information. The NSC is chaired by the Prime Minister and includes the ministers responsible for justice, security and home affairs, defence and foreign affairs, as well as the other deputy prime ministers.

Members of the Government who are not members of the Council may be invited by the Prime Minister to participate in the review of files of particular relevance to them. The following persons also attend meetings of the National Security Council as required by the items on the agenda:

- The Head of the General Intelligence and Security Service;
- The Administrator General of State Security;
- The Commissioner General of the Federal Police;
- The Director of the Coordination Unit for Threat Assessment (CUTA);
- The Chairman of the Management Committee of the Federal Public Service Home Affairs;
- A representative of the Board of Public Prosecutors;
- The Federal Public Prosecutor.

The Intelligence and Security Coordination Committee is composed of the heads of the authorities and services involved in intelligence and security policy. It develops strategic proposals, monitors the implementation of the priorities set by the National Security Council and ensures effective cooperation and exchange of information between services and authorities.

The Strategic Committee for Intelligence and Security is responsible for both the preparation and the implementation of policy and is composed of representatives of the members of the National Security Council and the Chairman of the Coordination Committee. The secretariat of the Strategic Committee is provided by the FPS Chancellery of the Prime Minister.

Review Committees:

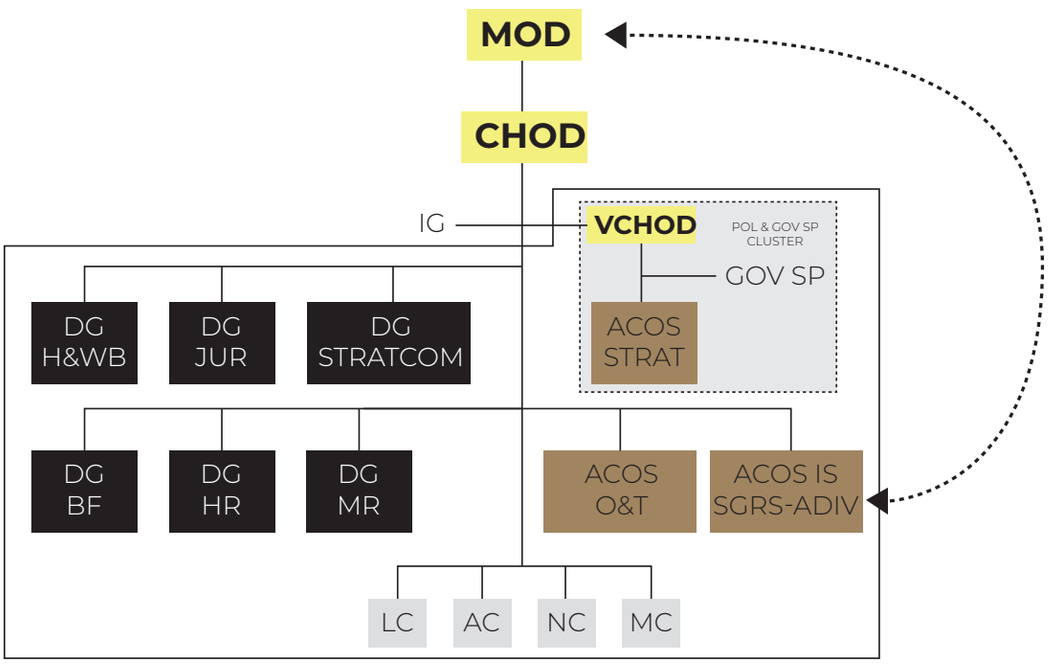
The Standing Committee I is responsible for reviewing the activities and functioning of the State Security and the General Intelligence and Security Service. The review covers legitimacy (verification of compliance with the applicable laws and regulations), efficiency (supervision of the efficiency of the intelligence services) and coordination (mutual harmonisation of the work of the services concerned).

The parliamentary committees and the Parliament, in their respective sessions, may not only ask ministers for explanations and/or specific questions, but also request the summoning of one or more members of an intelligence and security service. However, if the questioning and summoning of a person is also an integral part of democratic control, a closed session may be requested for reasons of confidentiality of the content of the answers.

Military involvement:

The history of the SGRS-ADIV is linked to military operations. Even today, a significant part of its work is intended for the Belgian Defence and in particular for military operations. This link with the Belgian Defence is obvious, as the military directorates manage its personnel, infrastructure and budget. This is also the reason why the SGRS-ADIV, under the name ACOS IS (Intelligence Service Department of Belgian Defence), reports hierarchically to the Chief of Defence.

In recent years, the work of the SGRS-ADIV has been extended to specific civil-military areas such as counter-terrorism and counter-extremism. For this reason, the SGRS-ADIV reports directly to the Minister of Defence.



INTELLIGENCE DIRECTORATE

The Intelligence Directorate provides high quality analysis based on a variety of information types and sources to advise our Government and partners.

The Intelligence Directorate is responsible for the collection and exploitation of information and its transformation into intelligence. Information is collected either by agents or by specific technical equipment belonging to the Collection Pillar. It is then passed on to analysts in the Operations Pillar for processing. There are different approaches to information processing, depending on the desired end product. The analyst may place more emphasis on the military, security, political, economic, social aspect... The richness of our intelligence services lies precisely in the possibility of offering different final reports according to the needs of the person.

OUR INTELLIGENCE DIRECTORATE IS THE FIRST AND LAST LINE OF DEFENCE AGAINST CHAOS

The Collection Pillar

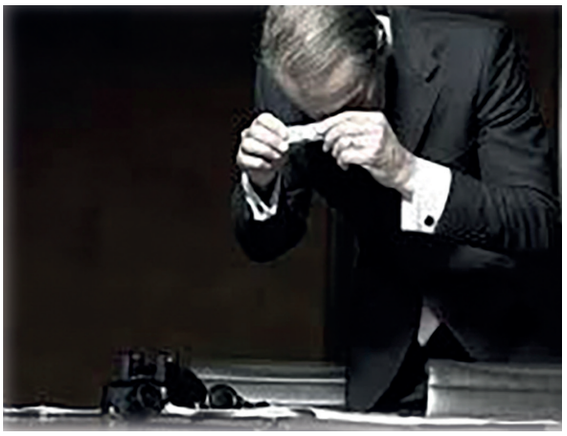
The Collection Pillar of the Intelligence Directorate is made up of several departments that collect information either from field agents or from technicians using special equipment, or both. These services are referred to in the jargon as «collection services».

When we speak of a «human source» or «contact» in intelligence jargon, we mean a person who provides information. They can live either abroad - in a military area of operations or in a target country - or on national territory. The service responsible for national sources and contacts is also involved in investigations relating to a TESSOC threat. These so-called counter-intelligence investigations are related to a threat in the field of terrorism, left-wing and right-wing extremism, espionage, sabotage, subversion and organised crime against the interests of the country and in particular the Belgian Defence.

The term «material» refers to electromagnetic signals, such as electronic eavesdropping, or geographical information, such as satellite images. It also refers to information from so-called «open sources» such as print media, radio or television and all information available on the Internet.

The evolution of intelligence today requires the regrouping of human and material resources in order to improve performance. In the case of a physical surveillance operation, for example, one or more agents in the field and various appropriate technical means are used to counter any eventuality or countermeasures taken by the person being watched.

> The Collection Pillar also has a service that acts as an entry and exit point for all NATO information flows to ensure military cooperation between Allies.



The Exploitation Pillar

The Exploitation Pillar of the Intelligence Directorate is made up of various platforms, organised by geographical area or theme, whose ultimate aim is to provide intelligence products on different topics. Examples include threats to a military operation abroad, extremism in a particular region, the political situation in Ukraine or issues related to predictive analysis such as security in eastern Congo.

The platforms are made up of analysts specialising in espionage and counterintelligence. The main geographical areas covered are Europe, Africa, Asia and the Middle East. The main themes are terrorism, extremism, espionage, sabotage, subversion and organised crime (TESSOC).

> **To ensure the quality of the end products, the Operations Pillar has a Quality Control Service.**

The Coordination Centre

The Intelligence Directorate has a Coordination Centre composed of representatives from the Collection and Exploitation Pillars and the Cyber Operations Directorate.

The Coordination Centre forwards all incoming information or requests to the appropriate persons and all outgoing information or requests to the relevant customers or partner services.

The Centre also has a collection management service, which matches collection efforts with analysis needs and coordinates counter-intelligence efforts between the platforms and the field staff in Belgium.

In order to comply with the law, the Coordination Centre has a department that submits all requests for the use of specific and exceptional methods to the Administrative Commission responsible for supervising these intelligence collection methods. With this authorisation, the SGRS-ADIV can, for example, carry out telephone tapping or the installation of listening devices.

SECURITY DIRECTORATE

The Security Directorate is responsible for maintaining military and industrial security. This competence covers the personnel, installations, weapon systems, equipment and operations of the Belgian Defence, both in Belgium and abroad. It is also responsible for the protection of classified defence information and the maintenance of secrecy, including archiving. It carries out security investigations for defence personnel and related industries.

IT ALL STARTS AND ENDS WITH OUR SECURITY DIRECTORATE

Military and industrial Security

This department is responsible for maintaining the military and industrial security of the Belgian defence and defence-related industries.

Firstly, it has a regulatory role with regard to Belgian defence and civilian companies that provide services or weapons systems.

The security officers advise the defence units or companies on the correct application of the guidelines. Announced inspections or unannounced monitoring visits are also part of the officers' tasks. When things go wrong, they investigate security incidents or assist the police.

Finally, the department has specialists in the detection of spying equipment to protect our own facilities from eavesdropping.

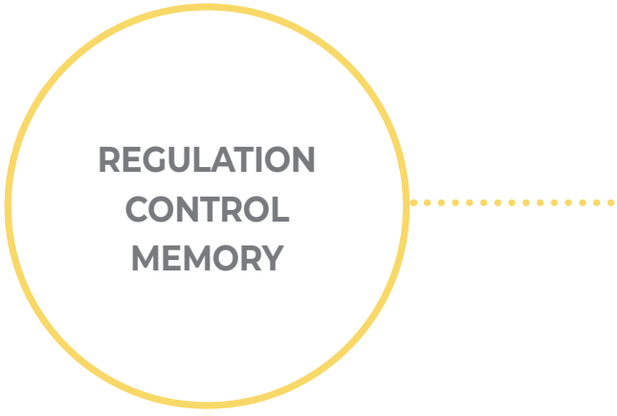
Security Investigation Service

This service conducts investigations in accordance with the Act on Classification and Security Clearance, Security Certificates and Security Advice (Classification Act 11 Dec 98). This law regulates the protection of secrets necessary to safeguard national security, military defence plans and the fundamental interests of our country. Unauthorised or improper use of classified information and weapon systems could potentially cause damage not only to the Belgian Defence, but also to the country as a whole.

Therefore, all prospective members of the Defence, both civilian and military, are subject to a background check during the recruitment process in order to assess their integrity and reliability. In addition, the vast majority of personnel are exposed to classified information, procedures and weapons systems in the course of their duties within our organisation. To do so, they must have a security clearance at the required level: confidential, secret or top secret. The depth of the investigation depends on the level and position. In order to carry out the investigation, the security investigators seek the cooperation of, among others, the police, the judiciary, the National Registry, the tax authorities and even foreign partner services. A security clearance will only be granted if the candidate demonstrates sufficient integrity, loyalty and discretion. A survey of the candidate's inner circle, a digital check or an interview with the candidate are among the possible investigative methods to verify these three criteria. In the event of a refusal to grant a security clearance, the candidate has the possibility of appealing against this decision to the «Commission d'appel des habilitations de sécurité» (Security Clearance Appeals Commission).

Classified archives

This service is in charge of all archived classified information of the Belgian Defence. The service preserves and manages all classified and historical archives of the Belgian Defence as long as they have an administrative use. Preservation takes place in both physical and digital form. All incoming archives are inventoried, preserved and stored in such a way that they can be easily used. The various departments of the SGRS-ADIV frequently consult these classified archives as a database. This service is used for scientific historical research, parliamentary inquiries, questions from the families of prisoners of war or judicial inquiries. On the occasion of important anniversaries of defence units, our archives enable us to recall the existence of a relevant book or brochure. When it is no longer administratively useful to keep the archives at the Ministry of Defence, they are declassified before being transferred to the General State Archives.



CYBER COMMAND

The Belgian Cyber Command is building a Cyber Force through partnerships to protect, defend, collect and fight in cyberspace and the electromagnetic environment.

In cyberspace and the electromagnetic environment, the Cyber Command is responsible for carrying out the intelligence and security missions of the SGRS-ADIV, ensuring the freedom of manoeuvre of the Belgian Defence and generating military effects in support of these operations.

The Cyber Command ensures the use of cyberspace for the benefit of the nation, the SGRS-ADIV and the Belgian Defence. As a key player in national resilience, it has a central position in our country's cyber architecture and is a reliable international partner as well as a national reference in cryptography. The Cyber Command develops its innovation process and new military capabilities. It implements these capabilities at the physical, logical and virtual levels of cyber and electromagnetic space. The Cyber Command has a privileged relationship with industry, academia and associations. Its true strength lies in its human capital.

To accomplish its missions, the Cyber Command has four distinct roles:

- First, it supports the other Components and Defence Agencies in developing a coherent and integrated set of cyber capabilities.
- Second, it ensures the development of specialised SGRS-ADIV cyber capabilities.

OUR CYBER FORCE IS THE FIRST AND LAST VIRTUAL FRONTIER OF THE BATTLEFIELD

T
.

- Thirdly, it conducts security and intelligence operations in cyberspace and the electromagnetic environment (Protect, Defend, Collect and Fight).
- Fourth, it has specialised capabilities for national defence and cyber crisis response.

The Cyber Command has the attributions of a 5th Component (Land, Navy, Air, Medical and Cyber) within the Belgian Defence and those of a Directorate within the SGRS-ADIV. Depending on its mission, it is subject to two different legal frameworks: the law governing the intelligence and security services or the legal framework governing the deployment of the Belgian Armed Forces.

THE CYBER COMMAND IS ORGANISED IN TWO DIRECTORATES :

The Cyber Force Directorate consists of four main subordinate units.

- Firstly, the «Unité des cyber opérations défensives - UCD» (Defensive Cyber Operations Unit), which is responsible for the protection and defence of Belgian military networks and weapon systems. This unit authorises our communication, information and weapon systems, carries out vulnerability assessments and hosts the Armed Forces Cryptographic Centre of Excellence. It conducts malware analysis, monitors defence networks from its Cyber Security Operations Centre (CSOC) and stands ready to defend our networks against any foreign or malicious actor.
- Second, the Cyber-SIGINT Collection Unit (CSCU) is responsible for all intrusive and non-intrusive collection operations and the generation of military effects in cyberspace and the electromagnetic environment.
- Thirdly, the Digital Influence Collection Unit (DICU) is responsible for the collection of open source and social media intelligence (OSINT and SOCMINT). It is also responsible for influence analysis and adversarial information warfare operations.
- Finally, the Cyber(space) Threat Intelligence Platform carries out intelligence analysis on harmful cyber activities against Belgian military interests.

The Cyber Development & Readiness Directorate is responsible for developing cyber defence capabilities in support of the SGRS-ADIV and the armed forces.

It focuses on building partnerships with academia, industry and civil society to stimulate innovation in cyber defence. It is also responsible for the education and training of personnel, the establishment of a doctrinal basis for cyber operations and the development of a civilian cyber reserve force. Finally, it is responsible for liaising with structural partners and international organisations.

PLANS & POLICY DIRECTORATE

THE TASKS OF THE PLANS & POLICY DIRECTORATE CAN BE DIVIDED INTO **THREE MAIN CATEGORIES:**

1. Planning in all areas of SGRS-ADIV responsibility, both in terms of intelligence, security, cyber and general operations (personnel, equipment, infrastructure, budget, etc.).

2. Supervising, coordinating and developing synergies with the service's national and international partners.

3. Implementing an organisational control system.

PLANNING, COOPERATION, SYNCHRONISATION AND EVALUATION ARE THE DAILY CHALLENGES OF OUR PLANS & POLICY DIRECTORATE

Planning section

This section is responsible for planning in all areas of SGRS-ADIV. It is in charge of drawing up, in collaboration with all the other directorates, the various plans of the service, such as the restructuring plan to be implemented on 19 October 2022, the master plan defining the priorities of the SGRS-ADIV, the national strategic intelligence plan, a crisis management plan, etc.

This section is also responsible for documenting all agreements signed by the service and, more importantly, for documenting all SGRS-ADIV processes. It also monitors NATO doctrine on intelligence, security and cyber.

Master Plan (PDSGRS)

At the end of 2021, the SGRS-ADIV drew up its Master Plan for 2022 with the aim of identifying the tasks to be carried out as a matter of priority, taking into account the resources available. During 2022, the SGRS-ADIV established its Master Plan for the years 2023 to 2027. This plan aims to improve SGRS-ADIV's ability to understand future developments in terms of threats and risks.

It consists of three complementary components:

- Its **OPERATIONAL** component defines the activities planned in the short and medium term, in compliance with the legal framework, international commitments and higher directives. The development of these activities takes into account the expected arrival of additional resources.
- Its **RESOURCES** component assesses the resources required by the service and their evolution over time.
- Its **FUNCTIONING** component focuses on outlining the key points of the most important projects to improve and maintain the operability of the SGRS-ADIV.

The balance between resources and tasks is the driving force behind this planning.

Relations section

This section is responsible for maintaining an inventory of all existing synergies between the SGRS-ADIV and national and international partners, and for identifying which partnerships need to be further developed. It defines the guidelines for synergies and the rules to be respected in the presence of partners. It is the entry and exit point for all contacts with foreign intelligence services. It also provides liaison officers with our national partners.

Resources and Capabilities Section

This section is responsible for the planning of support tasks for the SGRS-ADIV. This includes planning for human, material and infrastructure management. It is also responsible for the development of a digitisation project aimed at improving the work of analysts and documentation by automating certain processes.

Internal control section

This section aims to implement an effective organisational control system. This is a system of best management practices to ensure that objectives are achieved through the «Plan Do Check Act» cycle. Particular attention is given to process management and risk management. This section is responsible for setting the strategic and operational objectives of the SGRS-ADIV in collaboration with the various Directors. It also follows up on the recommendations of our oversight bodies. Finally, it draws lessons from the outcome of a crisis and prepares an annual report.

In addition to these sections, there is a Culture Project Officer whose objective is to promote organisational culture, security culture and intelligence culture. The aim is to unite agents around common values and behaviours and to develop a sense of belonging to the SGRS-ADIV.

SUPPORT DIRECTORATE

The main role of the SGRS-ADIV Support Directorate is to provide advice and support to the Head of SGRS-ADIV and all SGRS-ADIV Directorates in the areas of personnel, security, equipment, infrastructure, education, training and budget. The Support Directorate is also responsible for the support of Defence Attachés through the Defence Attachés Office (DAO).

ADVICE, SUPPORT AND RESOURCE MANAGEMENT ARE THE ESSENTIAL SERVICES PROVIDED BY OUR SUPPORT DIRECTORATE TO ENSURE THE SUCCESS OF THE SERVICE'S STRATEGY AND AMBITIONS

THE SUPPORT DIRECTORATE IS DIVIDED INTO SIX SECTIONS, EACH OF WHICH IS RESPONSIBLE FOR SPECIFIC AREAS

Human Resources Management

This section advises the Commander on all matters relating to SGRS-ADIV personnel. It maintains staffing levels, plans and implements personnel under various redeployment plans or in support of SGRS-ADIV operations. It also coordinates and implements the various directives of the Belgian Armed Forces in this field.

It is also responsible for the management of the SGRS-ADIV reserve personnel.

Security Section

This section is responsible for dealing with security issues within the SGRS-ADIV. This includes the protection of persons, facilities, equipment and information belonging to the SGRS-ADIV.

This section acts as the Security Officer as defined by law in relation to the security clearance of all SGRS-ADIV personnel. It maintains a list of security incidents, conducts investigations and proposes corrective actions as necessary.

Materials and Infrastructure Management

In the area of Materials Management, this section is responsible for the supply, disposal and management of all SGRS-ADIV equipment, with the exception of transmission equipment, computer equipment and crypto equipment. It is responsible for coordinating and issuing the statement of requirements for this equipment with the material managers of the Directorate General Material Resources. This section also manages all SGRS-ADIV vehicles and transport requests.

Finally, it is responsible for the maintenance of the infrastructure occupied by the SGRS-ADIV services, with the support of the barracks staff.

Communication and Information Systems Management

This section advises the Commander on information systems and information management within the SGRS-ADIV. It advises on the requirements for transmission equipment, computer equipment and cryptographic equipment. It provides logistical and technical support for the SGRS-ADIV internal networks and implements the rights and accesses defined by the functional authorities. It supports information management within the unit.

Education and Training

This section analyses the needs and range of internal and external training opportunities for all SGRS-ADIV staff. It coordinates and provides training periods. Finally, it evaluates the courses and develops the offer according to the evolving needs.

Budget Management

This section advises the Commander on the use of the budgets allocated to the SGRS-ADIV. It draws up a budget plan and sets priorities according to the resources available. It coordinates with the Operations and Training Section all financial aspects of the missions for its personnel. This service also provides financial support and accounting for the Belgian defence attachés abroad. Finally, it is responsible for the management of service visas and passports.

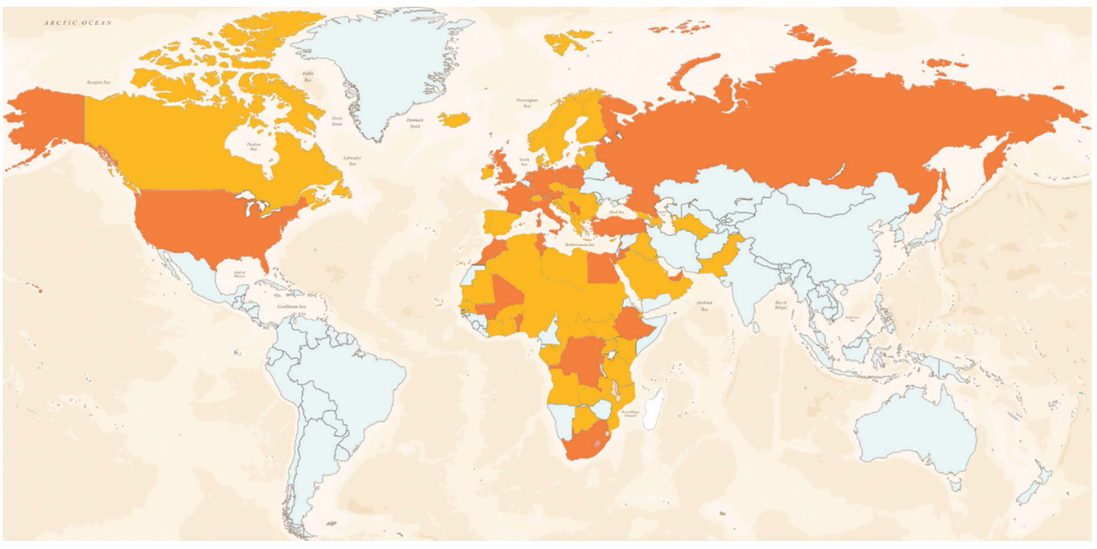
OUR DEFENCE ATTACHÉS OFFICE

The Defence Attachés Office is responsible for liaising with Belgian and foreign defence attachés, military advisers and Belgian security attachés abroad.

It is in charge of organising the selection procedure for Belgian defence attachés, military advisers, security attachés and their Belgian assistants to be appointed to a post abroad. It defines their specific training programme. It acts as an intermediary between the different sections of the SGRS-ADIV Support Directorate in logistical, financial and administrative matters. In coordination with the various SGRS-ADIV departments, it organises the evaluation of all posts according to a specific timetable.

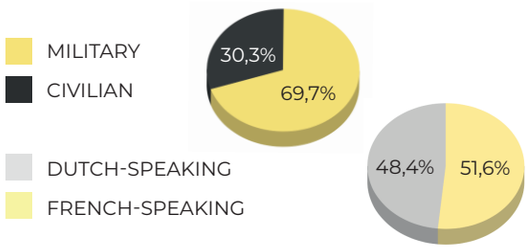
The Defence Attaché Office is also in charge of the foreign defence attachés accredited in Belgium and is involved in the finalisation of the accreditation process on Belgian territory. The Defence Attachés Office acts as a single point of contact for the Ministry of Defence. It centralises all correspondence (requests for information, requests for visits, requests for interviews, invitations, course offers, etc.) from foreign defence attachés accredited in Belgium. Each year, the Foreign Defence Attachés Office draws up a programme of activities for foreign defence attachés, including visits to Belgian defence units and the Belgian defence industry. An annual briefing is also organised, chaired by the Chief of Defence.

The map below shows all the countries where Belgian defence attachés are posted (orange) and the countries to which they are accredited (orange and yellow).



OUR FIGURES

PERSONNEL

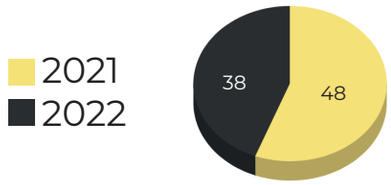


NUMBER OF INDIVIDUALS RECRUITED (PERSONNEL GROWTH)

IMPACT IN THE MEDIA

NUMBER OF MENTIONS IN NATIONAL PRINT MEDIA	**219**
NUMBER OF MENTIONS IN NATIONAL ELECTRONIC MEDIA	**294**
CUMULATIVE HOURS OF AIRTIME ON NATIONAL TELEVISION AND RADIO	**27H**

NUMBER OF PARLIAMENTARY QUESTIONS BY TOPIC



NUMBER OF PAPERS PRODUCED

	2021	2022
Requests for information from our clients and partners	5350	6982
	30,50% evolution compared to 2021	
Volume of the input	65323	69748
	6,77% evolution compared to 2021	
Volume of the ouput		
Requests for information sent to partners (national and international)	60	320
	433,33% evolution compared to 2021	
Number of SGRS-ADIV productions	486	591
	21,60% evolution compared to 2021	

RECRUITMENT

Human capital, our greatest asset:

IT recruitment is closely linked to the digital transformation of society. More specifically, in the field of cybersecurity and cyber defence, the quantitative and qualitative evolution of human capital needs goes hand in hand with the rapid and disruptive evolution of cybersecurity risks and threats. In the context of what we commonly call collective defence, our national cyber resilience is directly linked to our recruitment capacity.

Protect-Defend-Collect-Fight, ... & Recruit with agility:

The Cyber Command already includes no fewer than 40 STEM (science, technology, engineering and mathematics) and non-STEM occupations related to its four mission areas. The goal of asserting our sovereignty in cyberspace therefore clearly entails sustainable recruitment goals for the next decade and beyond. We need to start thinking today about the jobs of the future.

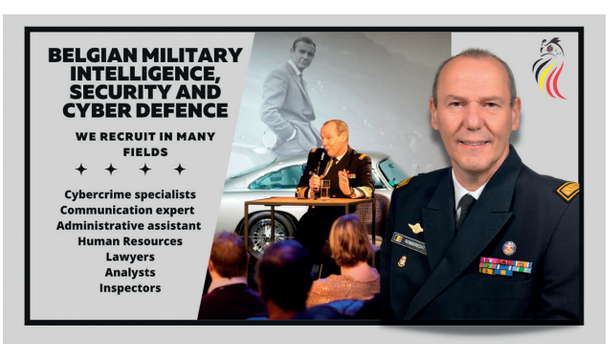
Defence is never just a job, it is always a MISSION... with high societal added value:

When it comes to attracting potential recruits among a plethora of cyber IT job offers from other sectors, the Cyber Command can count on a unique positioning linked to the specificity of the Armed Forces and the missions dedicated exclusively to our Defence. As an employer, our Defence department invests heavily in the training and continuous skills upgrading of its personnel, both civilian and military.

HUMAN CAPITAL INNOVATION: BOTH, A BIG CHALLENGE AND A BIG OPPORTUNITY

Exploratory, innovative and anti-fragile projects:

The unavailability of appropriate skills profiles in the labour market is notorious. Some essential skills to meet the needs of tomorrow are still not being raised to the level of transversal skills in our schools. Moreover, it is clear that neither our direct competitors in the labour market, nor our self-proclaimed adversaries in cyberspace, worry too much about bureaucracy in their own efforts to attract and recruit. The Cyber Command has no intention of starting a war for talent. Rather, it seeks to rally many stakeholders around a common societal project: to enable every cyber-skilled citizen to volunteer their time and talent in the service of a new kind of reserve. To this end, «junior» profiles, not necessarily graduates, but full of talent and certified by external bodies, are an interesting option. With this in mind, the Cyber Command has developed a number of partnerships in the associative world with non-profit organisations such as «MolenGeek» or «BeCode».



OUR COOPERATION WITH THE STATE SECURITY: THE NATIONAL INTELLIGENCE STRATEGIC PLAN

In 2018, the State Security (Sûreté de l'Etat – Veiligheid van de Staat) and the SGRS-ADIV worked closely together and shared certain tasks or capabilities. For example, staff from both services have been brought together to form a joint counter-terrorism platform. Surveillance teams have also been merged. Other synergies have been further developed, in particular in the processing of human sources. This has been formalised in a National Intelligence Strategic Plan (PSNR 2018).

In 2022, the two services have decided to take their cooperation to the next level.

FOUR PRIORITY AREAS HAVE BEEN IDENTIFIED

1. Counter-extremism and counter-terrorism

2. Counter-espionage and counter-interference

3. Cyber intelligence

4. Interconnection of information and communication technology (ICT) environments

Each of the two intelligence and security services has its own mission and specific capabilities, but they complement each other. Sharing data, exchanging knowledge, harmonising processes, pooling tasks or centralising resources are all ways to increase the efficiency of both services and thus contribute to national security.

Countering extremism and terrorism

In line with the creation of the joint counter-terrorism platform, the State Security and the SGRS-ADIV will also pool their tasks and resources to combat extremism. The existing Counter-Terrorism Platform will be transformed into two new joint platforms: one for sectarian counter-extremism and counter-terrorism, and the other for ideological counter-extremism and counter-terrorism.

Counter-espionage and the fight against interference

The synergy in the fight against espionage and interference will be organised in so-called «houses», which will focus their efforts on threats emanating from countries or entities. Tasks will be allocated in the best way possible and mixed teams may be formed to deal with specific issues.

Cyber Intelligence

Cyber intelligence is the collection of information about threats in cyberspace and the analysis of this raw information to produce actionable intelligence. This collection of information in cyberspace can be done by a variety of means, both intrusive and otherwise. The SGRS-ADIV is developing a significant cyber capability through its Cyber Command. Cooperation in this area aims to enable State Security to benefit from SGRS-ADIV capabilities by linking them to the specific niches developed within State Security.

Interconnection of ICT environments

In order to support the growing cooperation between the two intelligence and security services, a thorough interconnection of the ICT environments of both services is essential. This will require the synchronisation of their respective ICT developments. This will allow, among other things, the rapid and efficient exchange of classified information, the harmonisation, where necessary, of IT processes and the use of common tools.

Other synergies will also be developed, particularly in the field of education and training.

The State Security and the SGRS-ADIV are making every effort to implement the various synergies foreseen in the National Intelligence Strategic Plan 2022.

OUR PARTNERS

DEFENSE
STATE SECURITY
POLICE
CUSTOMS
FPS ECONOMY
FPS FOREIGN AFFAIRS
NATIONAL CRISIS CENTER
CTIF
MP
OCAM
EUROPE
NATO
CCB
R COMMITTEE
FPS JUSTICE

The SGRS-ADIV is part of several communities:

- The intelligence community, both at the national level with State Security and CUTA, and at the international level with foreign intelligence services.
- The security community, which is why it has close relations with the Integrated Police, the Public Prosecutor's Office, Customs, the CCB, the National Crisis Centre, etc. The SGRS-ADIV is a member of the National Security Agency.
- International organisations, the most important of which are the European Union and NATO.
- As a mainly external service, it maintains close relations with the FPS Foreign Affairs.

Due to its wide range of competences, the SGRS-ADIV also maintains relations with many other Belgian institutions, too numerous to list exhaustively: Immigration, CGRS, CTIF-CFI, CIAOSN-IACSSO and FANC...

It is essential for an intelligence service to maintain a relationship of trust with its partners and to exchange information. Synergies with the Federal Police must also be strengthened, particularly in the fields of training and cyber. A new liaison officer has been appointed by the SGRS-ADIV to facilitate these contacts and further cooperation with the Ministry of Foreign Affairs.

The Centre for Cybersecurity Belgium (CCB) coordinates the implementation of the national cybersecurity strategy, of which the SGRS-ADIV, and in particular its Cyber Command, is an active partner. We provide technical support to the CCB in responding to incidents, we provide expertise in malware analysis and, from our unique intelligence position, we provide in-depth analysis of cyber threats from state actors.

At the international level, the SGRS-ADIV is working with the State Security to update the National Security Council-approved policy on relations with foreign intelligence services.

OUR 2022 MEDIA REVIEW

January – February – March

- The SGRS-ADIV Master Plan for the year 2022 is approved by the Minister of Defence.
- Legislation introducing additional security measures for the provision of 5G mobile services is passed by the House on 10 February. This legislation prescribes that mobile operators will have to obtain prior authorisation in order to use 5G components. This authorisation will be granted by a panel consisting of the Prime Minister and the Ministers of Telecoms, Defence, Justice, Interior and Foreign Affairs. The ministers will rely on the advice of the intelligence and security services and the BIPT (the telecoms regulator) to determine the provider's risk profile.
- The SGRS-ADIV is heard by the "inner cabinet" about the war in Ukraine.
- Russia's invasion of Ukraine is accompanied by a wave of Russian cyber operations, both in Ukraine and abroad. Under the leadership of the Centre for Cybersecurity, several initiatives have been taken at national level and consultations have been held with representatives of the Cyber Directorate. Our teams were responsible for monitoring suspicious cyber activities in close cooperation with NATO and other international partners.
- The SGRS-ADIV issues a warning to Defence personnel to increase vigilance for incidents that may be related to the Russian invasion of Ukraine.
- Belgium expels 21 Russian diplomats.
- The Minister of Defence presents a plan to improve the functioning of the SGRS-ADIV (Master Plan 2022) to the Defence Committee in a closed session.
- On 30 March, an interview with the Minister of Defence and Vice-Admiral Wim Robberecht concerning the Master Plan is published in De Standaard and La Libre.

April – May – June

- On 7 April, accusations appear in the Dutch-language press about the purchase and use of Huawei Wi-Fi routers by the SGRS-ADIV. This attempt at disinformation is refuted by Vice-Admiral Wim Robberecht in several interviews.
- The office of the Minister of Justice wants the provisions on public procurement to include the possibility of refusing a tender if there is a risk of espionage.
- On 29 May, an interview with Vice-Admiral Wim Robberecht is published in De Tijd and L'Echo concerning the structural evolution of the SGRS-ADIV.
- Minister of Justice Vincent Van Quickenborne and Minister of Defence Ludivine Dedonder are tabling a bill in Parliament to give the Belgian intelligence services more flexibility.
- Articles appear on the first anniversary of the 'Jürgen Conings' crisis.
- The different governments of our country conclude a cooperation agreement within the Advisory Committee. This agreement concerns a screening mechanism for foreign investments in sectors that are important for public order and security or of strategic importance.
- Operation Cerberus is a success. Belgium repatriates 16 children of jihadists and six mothers of Belgian nationality from a Kurdish-controlled camp in north-eastern Syria in a plane belonging to Belgian Defence.
- The House Economy Committee approves in second reading the new version of the Data Retention Act, which requires telecom operators to retain their customers' metadata.
- The SGRS-ADIV adopts its new Mission Statement: mission, vision and values.
- The government is urgently tabling a bill in Parliament on five mutual legal assistance treaties.

July – August – September

- The act amending the Act of 30 November 1998 governing the intelligence and security services is adopted.
- The SGRS-ADIV and the VSSE sign a new cooperation agreement: the National Intelligence Strategic Plan 2.0 (PSNR2022).
- During a Foreign Affairs press conference, the cyber-attack on Belgian Defence is attributed to Chinese actors. During the first half of 2022, work was undertaken to restore all attacked systems to operational status and remove all malware. An incident handling report and an intelligence report with technical findings were provided.
- Defence personnel (civilian and military) will be screened every 5 years.
- According to a CUTA report, about 500 jihadist fighters are being monitored as a priority in Belgium.
- In September, the act introducing a general regulation on declassification of classified documents was published in the Belgian Official Gazette. This act ensures that classified documents can no longer remain classified indefinitely. The act provides that after a period of 20 years (for confidential documents), 30 years (for secret documents) or 50 years (for top secret documents), the originating government is required to decide whether a classified document can be declassified. If the originating authority considers that it cannot be declassified at that time, this must be thoroughly justified. A document can never remain classified for more than 100 years. After 100 years, the classification expires automatically.
- News articles report that, following an investigation by the SGRS-ADIV, a Belgian soldier has been suspended from his duties for his strong sympathies for right-wing extremism.

October – November – December

- The new SGRS-ADIV structure is implemented.
- The inauguration of the Cyber Command takes place in Evere in the presence of the Minister of Defence: it will ensure the exploitation of cyberspace for the benefit of the whole nation, Defence and the SGRS-ADIV. Its ambition is to become a national reference in cryptography and to occupy a central position in the federal cyber security ecosystem. Thanks to its network of partners in the economic, academic and associative worlds, it will ensure the growth of the future fifth Component.
- Yanjun Xu of China is convicted of industrial espionage in the United States and sentenced to 20 years in prison.
- China's investments in the ports of Antwerp and Zeebrugge carry a risk of interference or influence in our decision-making processes, according to the Minister of Justice in the House Justice Committee.
- The Master Plan for the years 2023 to 2027 (PDSGRS 23-27) is finalised.
- The Christmas interview with Vice-Admiral Wim Robberecht by Belga shows that, overall, politicians listen more to the SGRS-ADIV.
- The SGRS-ADIV jigsaw puzzle is revealed. This game aims to raise public interest in the world of intelligence

TODAY'S PERSPECTIVES ON TOMORROW'S THREATS

By the Intelligence Directorate and by theme:

Terrorism

The number of incidents, which by the nature of their motivation can be classified as religious terrorist attacks, is expected to be stable in 2023 compared to 2022.

In 2022, several senior members of the two main international jihadist movements, Al Qaeda and the Islamic State, were eliminated. Contrary to what has been observed in the past, these two organisations have not communicated on the establishment of successors.

Furthermore, there is currently no confirmed information on the reactivation of a structure dedicated to the organisation of external operations centred on Western countries and/or Belgium within these two movements.

However, while capacity is probably lacking at present, the terrorist intent of these groups persists. In addition, attacks and/or claims of opportunity cannot be excluded as well as the act of a self-radicalised person. An attack by a lone individual is the most likely scenario.

Extremism

The threat posed by non-religious extremism is not expected to decrease in 2023.

The economic crisis, aggravated by the energy crisis and the war in Ukraine, will result in the persistence of high inflation, which will continue to weigh on purchasing power, particularly for the most vulnerable groups. This crisis will therefore encourage the emergence of protest movements, which extremist groups, both left and right, will seek to exploit.

Continued migratory pressure on Europe will continue to feed right-wing extremist propaganda. The structural fragmentation of the political scene in many Western democracies and the polarisation fostered by the use of social networks will continue to attract extremist groups and individuals. The emergence of new forms of extremism that only imperfectly meet the criteria for left and right-wing extremism but are characterised by adherence to conspiracy theories is likely to continue. The occurrence of a new health crisis would be a catalyst in this regard.

Proliferation

Overall, the architecture of non-proliferation of Weapons of Mass Destruction continues to weaken.

This trend undermines international relations, encourages the arms race and increases the risk of escalation and miscalculation.

From this perspective, Russia is the main and most direct threat to Euro-Atlantic peace, especially in the current context of its invasion of Ukraine.

In the Middle East, Iran's behaviour (ballistic and nuclear developments, interference) constitutes a major potential for destabilisation in a region of major interest to the world economy. The Syrian regime, with Russian support, remains a challenge for chemical disarmament.

In Asia, the conflicting relations between the nuclear powers of Pakistan and India, the rise of China, and the nuclear developments of North Korea remain a concern.

In the West, the CBRN terrorist threat remains.

By the Intelligence Directorate and by country:

Russia

Several expulsions led to a temporary reduction of Russian intelligence capabilities on Belgian soil. On 29 March, 21 Russian diplomats attached to the Russian embassy in Belgium and the consulate in Antwerp were expelled. On 5 April, 19 more Russian diplomats working at the Russian mission to the EU were sent packing. The deteriorated image of Russia in Belgian society due to the war reinforces this trend.

However, the Russian intelligence services will adapt to the changing situation to meet their intelligence needs.

China

With XI Jinping's third term in office, the Chinese Communist Party's (CCP) intelligence needs are increasingly focused abroad. For the first time, a head of intelligence is part of the Politburo, which will result in increased resources for the intelligence agencies. These agencies are to provide intelligence that will enable China to become technologically self-sufficient, to position itself in conflicts with the West and to secure China's economic interests globally.

With intelligence gathering and influence towards the EU and NATO, Belgium will only become more important for Chinese intelligence work.

African countries

The upcoming legislative elections in the DRC and Rwanda should reinforce the will of the various African authorities to persevere in activities that support their national interests.

It is likely that Russia's invasion of Ukraine will also have consequences for the African continent in 2023. Revisionist states such as China or Russia may seek to use African proxies as instruments to achieve or consolidate an advantageous, even dominant, position against political, military or economic rivals. Such tensions may have consequences in Belgium or for Belgian interests and nationals in Africa.

The SGRS-ADIV will therefore continue to monitor international developments and possible consequences for the activities of African intelligence services.

By the Cyber Force Directorate:

General Points

Cyber threat actors are showing increasing interest in attacks on the IT supply chain and attacks on cloud and IT service providers.

These attacks allow these actors to gain a foothold in the entities they target. The disruption of satellite communications is likely to be an increasingly important trend in the short to medium term. The disruption of fibre optic cables made headlines in 2022 and it is likely that such cyber-physical attacks will increase in the short to medium term.

Russia

In the short term, the Russian military intelligence service GRU will be mostly focused on Ukraine, while the Russian foreign intelligence service SVR continues to target governments, NGOs and think tanks with new malware. Economic sanctions that limit Russia's access to technology could lead to an increase in economic cyber espionage.

After conducting disruptive attacks against Ukraine with as many as nine data erasers in the first half of 2022, GRU-linked actors continued to target Ukraine with new data erasure malware in the second half of 2022.

In 2022, new types of Russian malware targeting industrial control systems and operational technologies were discovered. A Russian attack on the power grid in Ukraine could disrupt power distribution. Russian state actors have also been observed conducting cyber reconnaissance against critical infrastructure in Western countries. Analysts are concerned about a possible attack on Western critical infrastructure if the war in Ukraine spreads beyond the Ukrainian theatre. Pro-Russian hacktivists have carried out an increasing number of disruptive cyber-attacks against almost all NATO countries (and beyond), often in response to actions taken by these countries that Russia perceives as threatening. The Baltic States were reportedly the hardest hit by the hacktivists, allowing Russia to conduct cyber operations and disinformation. These disruptive cyber-attacks will continue into 2023 and are often a Russian reaction to a strong political statement or the delivery of military equipment to Ukraine. Cybercrime in the form of ransomware attacks has been increasingly used as a geopolitical weapon since the second half of 2022, not only against Ukrainian entities but also against NATO members' government services (e.g. Montenegro). In addition to providing Russia with plausible deniability, ransomware attacks allow Russia to carry out destructive attacks against NATO members while remaining under the Article 5 threshold. We therefore believe that this trend of using ransomware as a geopolitical weapon will continue.

China

Cyber targeting is likely to continue to serve economic and military interests, with a particular focus on countries that play an important role in China's Belt and Road Initiative and in China's strategic objectives in the South China Sea.

The disruptive attacks by Chinese hacktivists on Taiwan during U.S. House Speaker Nancy Pelosi's visit to Taipei in August 2022 are likely to be repeated if China perceives the actions of other countries towards Taiwan as running counter to China's «One China» principle.

Rest of the world

Disruptive cyber operations against the government services of a NATO partner (Albania) have been attributed to Iran, suggesting less restraint in attacking EU/NATO targets in the future. An Iranian proxy group based in Iraq has targeted Ukrainian targets on two occasions, which may indicate increasing collaboration between Iran and Russia in terms of cyber operations. While some offensive private sector cyber actors, such as the Israeli NSO Group (Pegasus), are under scrutiny by various governments, press reports nevertheless indicate that the cyber mercenary business is booming. Their 'surveillance as a service' offer allows their clients to penetrate the networks, computers and smartphones of their targets (often dissidents, journalists, human rights activists). A trend to watch is the collaboration of private sector offensive cyber actors with private military companies (e.g. the Wagner Group).

WE DO THE WORK

We are the eyes and ears of the nation. We look for what our enemies want to keep hidden. We operate where our enemies hide, always in the shadows and with the utmost discretion. We study our enemies to anticipate new threats and ensure the security of our military secrets and technological knowledge.

We advise our political and military leaders so that they can make the best decisions, independently and sovereignly, to best protect our country and its citizens. We operate around the world, wherever our interests demand. Today, the threats to our society have become more complex, unpredictable and diverse.

We are present in support of military operations, in the fight against espionage and interference, in cyber security, in the fight against terrorism, in the fight against extremism, in the fight against the proliferation of weapons of mass destruction. We are also present in the fight against sectarian or criminal organisations and in scientific and economic fields such as the protection of companies and vital infrastructures.

OUR SHORT LEXICON

SGRS-ADIV : General Intelligence and Security Service

VSSE : State Security

CUTA : Coordination Unit for Threat Analysis

GRU : Russian military intelligence service

SVR : Russia's external intelligence service

NATO : North Atlantic Treaty Organisation

EU : European Union

NGO : non-governmental organisation

CBRN : chemical, biological, radiological and nuclear agents or materials

PSNR : National Intelligence Strategic Plan

PDSGRS : SGRS-ADIV Master Plan

CGRS : Office of the Commissioner General for Refugees and Stateless Persons

FANC : Federal Agency for Nuclear Control

CTIF-CFI : Financial Intelligence Processing Unit

CIAOSN-IACSSO : center for information and advice on harmful sectarian organizations

CCB : Centre for Cybersecurity Belgium

DAO : Defence Attachés Office

UCD : Defensive Cyber Operations Unit (Unité des cyber opérations défensives)

CSOC : Cyber Security Operations Centre

CSCU : Cyber-SIGINT Collection Unit

DICU : Digital Influence Collection Unit

OSINT : Open-source intelligence

TESSOC : Terrorism - Espionage - Subversion - Sabotage - Organised Crime