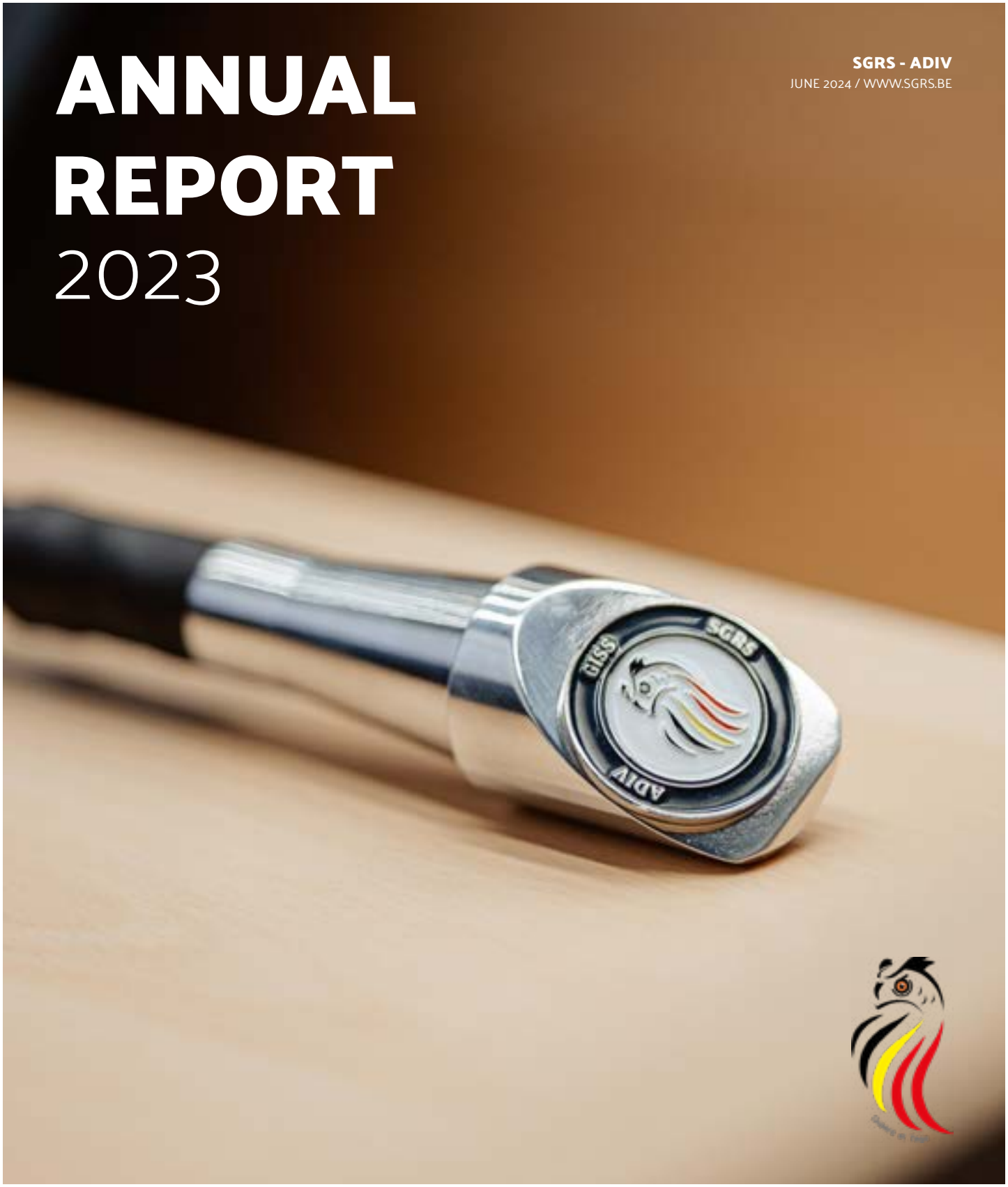
ANNUAL REPORT 2023

SGRS - ADIV
JUNE 2024 / WWW.SGRS.BE



DEFENSIE

.be

The world is changing, but our mission remains the same

TABLE OF CONTENTS

7 Introduction

11 Part I : Identifying Today's and Tomorrow's External Threats to be Better Prepared for Them

- **13** The World in 2023
- **20** Hybrid Warfare in Ukraine
- **26** Israeli-Palestinian Conflict
- **30** Africa

MAJOR GENERAL
STÉPHANE DUTRON
HEAD OF THE SGRS

Quaero et Tego is our motto;

Protecting our country, our companies and our expatriates through our intelligence is our primary mission. Advising the authorities is our duty to our country, our society and our fellow citizens.

RESPONSIBLE EDITOR

M. Van Hecke Bernard

Queen Elisabeth Barracks

Eversestraat 1, 1140 Evere

Photos: DG StratCom and SGRS staff

Lay-out: SGRS-ADIV

38 **Part II: Assessing the State of Threats to Protect Ourselves against Them**

38 Disinformation and Influence Operations

40 Espionage and Cyber Espionage

42 Cyber Threaths

44 Proliferation Threats

"We work for you, for us our country, for peace."

Major General
Stéphane Dutron

46 **Part III : Contributing to National Resilience**

46 Common Platforms in the Fight against Extremism and Terrorism

48 Military Security Assured, National Security Strengthened

52 Keeping Up the Momentum of Technological Change

55 **Part IV: Developing Our Human Capital**

58 Towards a New Reserve Concept

60 First Edition of the Cyber Summer School

READMISSION OF THE RSM BATON

Chief Warrant Officier Frédéric Charlot, former RSM, has made way for the new RSM Dolores Geeraert.

Introduction

2023 was once again a busy year for the intelligence and security services with regard to current affairs.

The successive coups d'état in West Africa, the resurgence of the Israeli-Palestinian conflict, Russia's continuing war of aggression against Ukraine and the conflict in the east of the Democratic Republic of the Congo are just a few examples we can mention.

Over the same period, phenomena such as extremism, terrorism, organised crime, proliferation, and interference continued to pose a structural threat to the European continent. As we already pointed out in our first report in 2022: espionage and foreign interference have reached levels not seen since the Cold War. Unfortunately, this trend was confirmed in 2023. Belgium, and Brussels in particular, as the headquarters of many international organisations, has obviously not been spared.

Working together for a better understanding

To deal with these multiple threats, collaboration with other intelligence and security services is essential, both nationally and internationally. In particular, collaboration with State Security is essential. As part of the implementation of the NSIP , this desire to work together has resulted in the creation of platforms, common to both our institutions, to combat extremism and terrorism.

At the same time, the digitisation of my service is continuing, so that we can deal as effectively as possible with the main commodity with which we work: information. We need to protect this information, analyse it, and connect it with that of our partners. To do this, we need modern, secure IT resources, not only for collection purposes, but also for processing and dissemination.

Information warfare, a reality

The field of information has in fact become a new battlefield and sphere of influence, with foreign powers mass-producing misleading content and/or promoting narratives that run counter to our values. The objective remains the same, in Belgium and around the world: to weaken our democracies by undermining confidence in our leaders and institutions. To achieve this, these powers are trying to polarise public opinion by pitting communities against each other with "fake news". We already monitored the electoral process in 2019 and we are keeping a particularly close eye on the June 2024 elections with all our partners at the federal level.

Continuing to modernise the SGRS

On 1 January 2024, I had the honour of taking the lead of the SGRS. I would like to pay tribute to the immense work of my predecessor, Vice Admiral Wim Robberecht, who was head of the SGRS for almost three years. He brought about profound changes in our organisation and I intend to stay on a path of transforming and modernising our service.

I also feel a great sense of responsibility, because we have to be able to fulfil our ambitions in a world where the traditional geostrategic balances have been upset, where there are many security challenges and one crisis follows another.

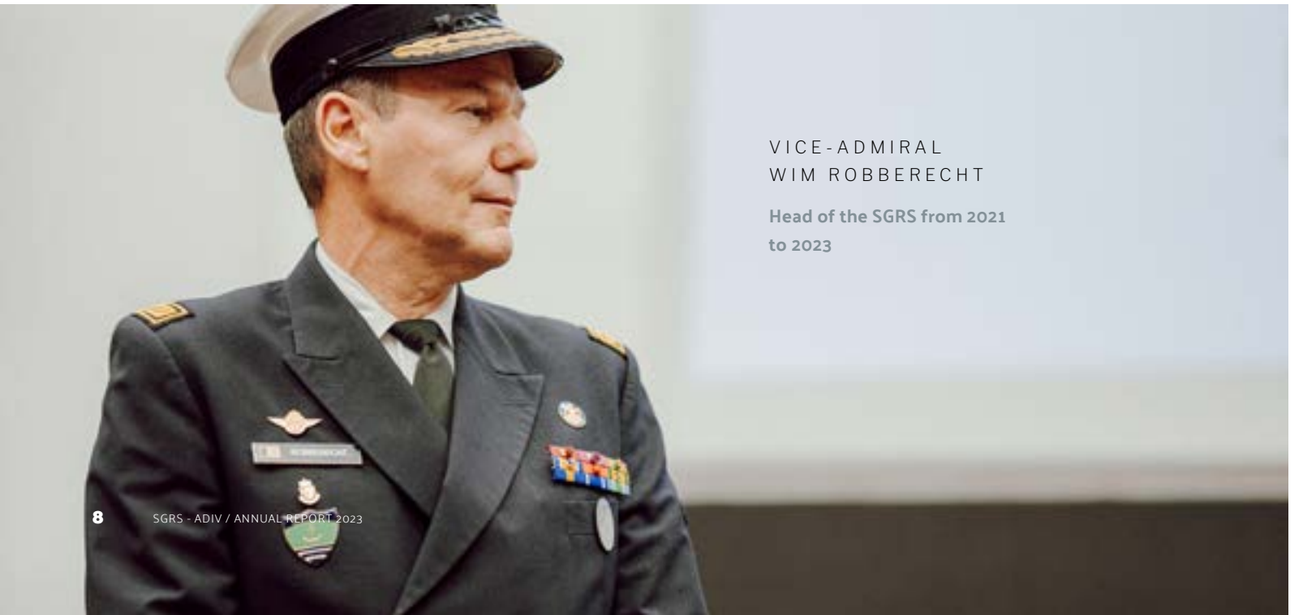
Society is the foundation of our service. The development of our communications, as illustrated in this second annual report, aims to strengthen this link with society and our citizens, within the limits of transparency that our particular profession imposes on us.

This link is also what will enable us to continue to recruit motivated personnel to fight our adversaries, whether at home, abroad or in cyberspace. There are positive signs in this direction; for instance, we attracted more than a thousand applicants when we opened up forty inspector posts in 2023.

I hope you enjoy reading this report.

MAJOR GENERAL

Stephane Dutron



VICE-ADMIRAL
WIM ROBBERECHT

Head of the SGRS from 2021 to 2023

SGRS - ADIV / CYBER COMMAND

Cyber Command

Day by day, the development of Cyber Command within the SGRS continues as well as its introduction as a fifth component within Defence.

Day after day, the development of Cyber Command continues its development within the SGRS as well as its introduction as a fifth component within Defence.

In our increasingly digital society, it is essential not only to strengthen the SGRS's intelligence and security capabilities in cyberspace, but also to develop the cyber defence, electronic warfare and information warfare capabilities in support of all components and Defence in its entirety.

This is a human as well as a technological adventure. Human, because we are recruiting a large number of new employees from all backgrounds: from Defence, academia or research, or from associations. We are hiring military and civilian personnel, and reservists. We recruit both STEM (Science, Technology, Engineering, Mathematics) and non-STEM profiles. There are more than forty jobs at Cyber Command. And we want to offer each of these profiles the same opportunities to develop and grow with us. This requires not only a huge investment but also great flexibility. However, I am convinced that this diversity of profiles and talents is part of our identity and the key to our success.

In this "war for talent", we are mainly investing in young people. In 2023, for instance, we launched the "Summer School", the first cyber summer school for students. This is a week-long immersion in the military environment and behind the scenes of cyber defence, with our experts and those from the Royal Military Academy.

So far, the recruitment results have been very positive. Since the creation of the Cyber Command on 19 October 2022, the number of personnel has increased by more than 15% in net terms. This is a success, given that the Belgian and international job markets are extremely tight in the cyber security sector.

It is also a technological adventure, especially with the emergence of EDT (Emerging and Disruptive Technology) such as artificial intelligence, sovereign cloud applications, and post-quantum cryptography. The latter offer opportunities, but also constitute powerful threats when they are used improperly, particularly in cyberspace.

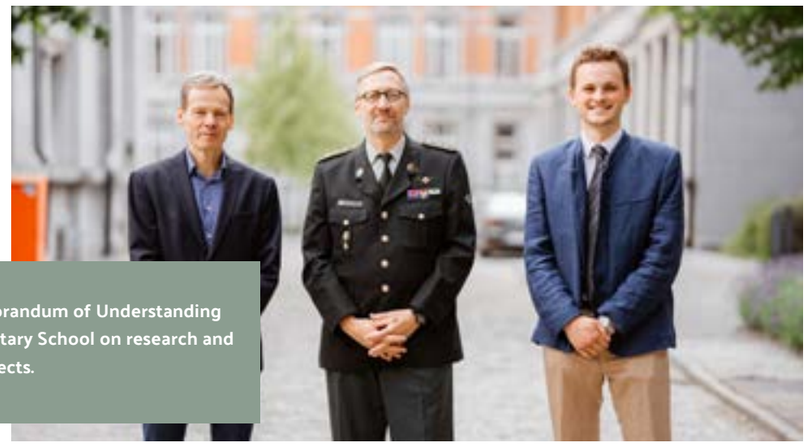
These technologies are set to play a major role in cryptography, enabling us to secure the exchange of extremely sensitive information or to protect the communication and command systems integrated into the new weapon systems of Defence. Examples include the F-35 fighter aircraft, the army's new motorised capability and the navy's future vessels.

We have developed a centralised command and an ambitious structure within SGRS to enable

us to face, detect, respond to and anticipate these threats. Our capabilities will continue to be reinforced within the intelligence and security sphere, because we are intrinsically linked to it, whether in terms of our legal framework or the execution of our missions.

So the adventure continues, and it is only just beginning. Perhaps with you by our side?

MAJOR GENERAL



Signing of a Memorandum of Understanding with the Royal Military School on research and development projects.

First meeting of cyber ambassadors and Cyber Commanders during the Belgian Presidency of the European Union.

Identifying Today's and Tomorrow's External Threats to be Better Prepared for Them

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

As such, it provides expertise in strategic and defence analysis to its clients, the main ones being the Belgian government and the Ministry of Defence. This analysis enables SGRS to identify threats arising from developments occurring outside the country, under the powers granted to it by the Act of 30 November 1998. To this end, it has a diversified information-gathering network at its disposal. SGRS is developing enhanced cooperation with certain foreign and defence intelligence partners, in particular the FPS Foreign Affairs.

The World in 2023

Two conflicts, in Eastern Europe and the Middle East, dominated the news in 2023.

In Ukraine, in the theatre of military operations, the counter-offensive failed to bring about any significant strategic change in the summer of 2023. The Ukrainian conflict has become a war of attrition that is likely to persist.

In the Middle East, the resurgence of the Israeli-Palestinian conflict, through Israel's violent response and the involvement of the Iranian axis through its proxies, has increased regional and international tensions. This has had an impact on maritime security in the Red Sea, with significant economic repercussions.

Major Geopolitical Developments

Both these conflicts reflect major geopolitical developments that are happening in the world. The Rules-Based International Order, a system promoted by the liberal democracies and supported mainly by the UN and Bretton Woods institutions, is now being challenged, ever more ostensibly, by revisionist powers such as Russia and Iran. Multilateralism, the driving force behind international relations in recent decades, is being undermined. The Western powers are vying with their geopolitical rivals to ally themselves with the powers of the so-called Global South, that motley collection of southern nations that are unsure of their strategic position.

The competition between the "great powers" is again a major issue in international relations.

While these two conflicts, and the issue of migration, command the attention of the Western public and politicians, they should not overshadow other issues or areas of the world.

The African continent is struggling with its economic development. It continues to face strong demographic pressures, coups and competition between external powers. The countries of the Sahel and West Africa have been particularly affected by this wave of putsches, leading to changes in alliances. The security situation there remains precarious. Sudan continues to be torn apart by civil war. Africa's Great Lakes region suffers from the conflict in the eastern Democratic Republic of the Congo.

In Asia, India's power continues to rise against a backdrop of nationalism, while its nuclear-armed neighbour Pakistan is struggling with a deep economic crisis. China is trying to contain the structural slowdown in its growth, while pursuing its technological and military development. The development and projection of Chinese power is also causing growing concern in certain neighbouring countries.

A Constantly Changing Battlefield

In conjunction with these crises, structural developments are taking place that are difficult to fully grasp today. Technological developments, such as artificial intelligence, and their impact on battle management, especially with the increased use of drones and cyber assets, require rethinking what tomorrow's world will be like in order to be better prepared for it. Similarly, the issues of access to resources and the energy transition remain essential.

The fragmentation of Western societies by the rise of extremism, the persistence of the terrorist threat and the growing power of criminal groups continue to have an impact on the security situation in Belgium. The threats of espionage, influence and sabotage, resulting from the return of competition between the great powers, will also have a lasting impact on our security landscape.

Return of the “Great Powers” competition

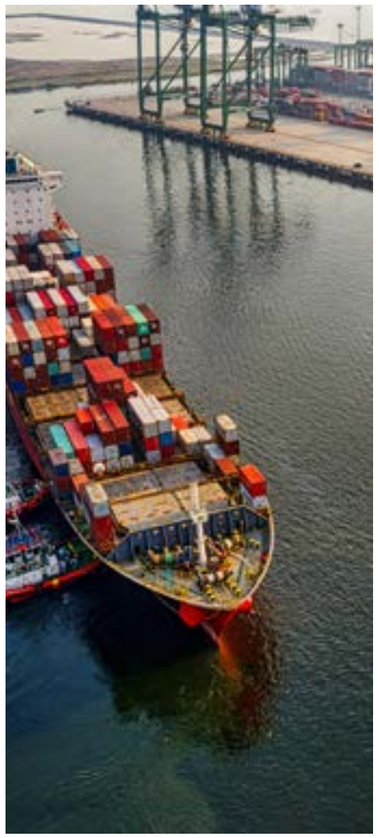
The collapse of the Soviet Union in 1991 ushered in a period of virtual hegemony for US power. The globalisation of the economy and the spread of liberal democracy gave rise to concepts such as Francis Fukuyama’s “The End of History”.

While the first decade of the 21st century was dominated by the fight against terrorism, competition between the great powers has gradually re-emerged as a key feature of international relations. The liberal democracies are faced with authoritarian and revisionist powers that are challenging both Western power and the world order and its institutions.

A Game of Influence and Competition

China’s growing power on all fronts is disrupting established balances. In the game of influence and international competition, China has launched a global project to create the “new silk roads”, designed to improve ground and sea lines of communication between the country and dozens of Asian, African and European countries. And it does so through economic investment in, among other things, infrastructure, diplomatic relations, military support, and the projection of soft power.

Russia’s policy of armed aggression in Ukraine has caused a major rift with Western liberal democracies. To counter its isolation, it has since been trying to increase its influence in the world. It is manipulating to its advantage the movements rejecting Western domination, particularly in Africa, by taking the initiative in military and security cooperation. On the diplomatic front, Russia wishes to develop its vision of a multipolar world order and is seeking allies in international forums to that end.



A Question of Resources

China and Russia have found common ground in their efforts to counter the domination of liberal democracies. For instance, just before Russia’s invasion of Ukraine, the heads of state of Russia and China announced an “unlimited partnership”. Initially, China, which defends the principles of territorial integrity and sovereignty in its international relations, found itself in an uncomfortable position by rejecting the international sanctions against Russia. It has kept the Russian economy afloat by supplying raw materials and providing an alternative to international monetary exchanges restricted by the sanctions. Yet China wishes to maintain the perception of neutrality and present itself as a responsible international player.

For China, the war in Ukraine not only serves as a training ground for a possible future invasion of Taiwan. It is also shifting the balance of power between China and Russia in China’s favour. Russia has become dependent on China to keep its military industry running. Moreover, with Moscow focusing all its attention on the conflict in Ukraine, China can expand its sphere of influence at Russia’s expense, for instance in Central Asia or the Arctic region.

A Game of Communicating Vessels

This interplay of great powers goes far beyond the US, Chinese and Russian powers.

The Middle East is still defined by the rivalry between the Iranian axis and the traditional powers of the Gulf States. Added to this first dividing line are the tensions between the powers close to political Islam (including Qatar) and the Sunni powers who consider the Muslim Brotherhood a threat to their stability (Egypt, Saudi Arabia, United Arab Emirates).

In South Asia, India has been a fully fledged player in globalisation for several years now, enjoying strong growth and housing the world’s largest population. Its arch-rival, Pakistan, is going through a deep economic and political crisis.

Networking

Some examples of disinformation circulating on social networks.

Challenging International Order and Multilateralism

The Rules-Based International Order is the system built by the liberal democracies led by the United States. This system is mainly based on various international and regional institutions, including the UN and Bretton Woods institutions. It relies on international standards that are sometimes legally binding, sometimes more traditional and based on codes of good conduct. It encompasses the economic, political, security and fundamental rights spheres.

This international order is now being shaken. Russia's war of aggression in Ukraine, and the annexation of Crimea that preceded it, are flagrant violations of the United Nations Charter. States such as China and certain countries of the Global South are questioning the use of the legal framework developed to promote fundamental rights.

Empowerment of the Global South and Democracies in Decline

The Western powers are currently competing with their rivals of the BRICS (Brazil, Russia, India, China and South Africa) in the great game of influence over the countries of the so-called Global South.

This concept, although poorly defined, refers to this motley collection of non-Western countries that more or less share the following aspirations: achieve greater economic development, gain more respect from the old powers and have a greater say on the world stage. Some of these nations express unease or even reject the concepts developed in the West regarding fundamental rights and individual freedoms.

More and more of these so-called Global South states are now showing growing autonomy in their positioning in the competition between the great powers, sometimes choosing the Western powers, sometimes the BRICS, depending on what they consider to be in their interests.

It is useful to consider coups, military putsches and other power changes as part of a larger global movement in which the influence of liberal Western democracies on various countries of the Global South is declining, especially in the context of the great power struggle between the United States of America and authoritarian regimes such as Russia and China.

Global Pervasiveness of Information Warfare

State actors such as Russia and China use information warfare to achieve their long-term strategic objectives. They exploit the pre-existing rifts within certain social groups and capitalise on current events to increase polarisation and persuasion. They resort to influencing activities both towards their own population and towards external and international populations, each with their own accents.

These activities are generally aimed at changing perceptions and belief systems, helping to fuel conspiracy theories in our societies, and in the context of current conflicts, discrediting Western governments and sowing distrust among allied partners.

By way of example, China presents the conflict in Ukraine as the result of Western interference and sees Russia as an ally in changing the existing world order. China amplifies Russian rhetoric and disinformation in Africa, Latin America and among its allies in the Middle East, many of whom are economically dependent, in order to support Russia diplomatically. In this way, China has seriously weakened Western efforts to isolate Russia and cut it off from the global economy.

These influence strategies are not limited to foreign populations but also extend to the whole of Europe. They have long-term effects and will present a challenge to our authorities in the future.

OUR SERVICE IS WORLDWIDE ACTIVE

Through its intelligence, SGRS advises political and military leaders so that they can make the best choices, independently and sovereignly, to best protect Belgium and its citizens. To this end, our service operates at all times anywhere in the world where our interests require it, in support of military operations but also for the benefit of our citizens, our politicians and our security partners, both nationally and internationally.

IMPORTANCE OF OUR DEFENCE ATTACHES

Good knowledge of the international environment also requires a network of defence attachés. Working closely with Foreign Affairs, local authorities and partner armies, they provide liaison with the SGRS.

1 Military Adviser to the Belgian Delegation to the OSCE and Defence Attaché for Austria, Slovakia and Slovenia.

"As defence attaché, I take part in bilateral activities in these three countries to promote Belgian Defence. The big challenge is to find the right approach for each country. NATO or EU membership, Austria's neutrality and the political climate are all factors that come into play. Keeping abreast of what is going on in these countries and networking are therefore daily tasks. This wide range of tasks can be a real challenge, but it is also what I think makes this job attractive."

2 Defence Attaché in Poland, also accredited to Estonia, Latvia and Lithuania.

"I work in a region that is undeniably of great geostrategic importance. All these countries share a border with Belarus and/or Russia and recent developments have had major security and defence implications, notably with the stronger presence of the Alliance and aid to Ukraine.

Poland plays an essential role in the support of Ukraine, whether by supplying equipment or training Ukrainian servicemen as part of the European mission EUMAM UKR. The three Baltic States also play a key role in NATO's defence, and our country is actively involved in all three dimensions, whether on land, in the air or at sea.

Both for aid to Ukraine and for collective defence, my role is to facilitate and coordinate with the host country to make sure that the mission runs smoothly."

3 Defence Attaché in Jordan, also accredited to Iraq.

"Dialogue is one of the essential keys to bilateral cooperation between Jordan and Belgium. Our team, anchored in the Middle East, has an extensive network that allows it to gather information for both our countries, including in the field of intelligence and security. Developing this expertise in the region is only possible by being present in the area and having direct contacts.

In the embassy, I bring added value as a military adviser to the ambassador by sharing my specific military experience with the diplomats, for instance in the case of planning an evacuation of citizens from a neighbouring country during a crisis. This is an exciting and multifaceted job that combines military diplomacy, bilateral cooperation and operationality."

4 Defence Attaché in Russia, also accredited to Armenia.

"One of the consequences of the sanctions imposed on Russia is that all EU member states have been placed on Russia's "unfriendly countries list". As a result, bilateral relations are currently more limited. Nevertheless, having a personal presence in the world's largest country, whose capital is just 2,500 km from Brussels and which is daily front-page news in the Western media, has great added value. Indeed, in times of crisis, it is essential to be able to observe events as truthfully as possible and in their specific context, and thus help the Belgian authorities to form a clear idea of the situation."

5 Defence Attaché in Morocco, also accredited to Senegal and Cape Verde.

"My mandate in the countries of accreditation is threefold. First, it is necessary to acquire knowledge of the situation in the region to which one is assigned, build and maintain a local network to be able to identify opportunities more easily.

In addition, my job is to determine bilateral activities with the local armed forces each year and monitor their realisation. The Belgian defence industry is approaching me more and more for help in gaining access to local armed forces.

Finally, I also have an advisory role. In my job, you must be able to determine strategic trends, but also be ready to inform the Defence Staff in response to an incident or bottleneck in a particular case."

Hybrid Warfare in Ukraine: Where Does it End?

Russia's war of aggression against Ukraine has turned into a war of attrition between its belligerents.

On the Russian side, the Putin regime has been under political and economic strain since February 2022, but its aim is to stay in power at any cost and it remains relatively stable. The year 2023 was marked by the action taken in June by the leader of the Wagner Group's mercenaries, Yevgeny Prigozhin, but any attempt at a popular uprising is stifled by the use of repression and disinformation.

On the Ukrainian side, President Zelensky's leadership remains undisputed for now, even if the first cracks are beginning to show. His charisma and his role as a symbol of the resistance have earned him undeniable respect within Ukrainian society and institutions, despite his heavy dependence on external (political, economic and military) support. The maximalist objectives set by his armed forces have not been achieved after the failure of the counter-offensive in the summer of 2023. In this difficult context, the Ukrainian leadership runs the risk of having its legitimacy and stability threatened.

On the military front, the strategic situation remains relatively unchanged. In 2023, Russia has strengthened its positions across the entire front line to the extent that it can conduct offensive operations, but without being able to force a real military breakthrough. After the failure of the Ukrainian offensive, Russia regained the initiative on the ground. Its propaganda, through disinformation campaigns, presents the situation as a total failure on the part of Ukraine and, by extension, the West.

After more than two years of war, Ukraine and Russia still face the same military challenges: mass recruitment and mobilisations of part of the population, lack of heavy equipment and ammunition. Both sides remain unable to consolidate or build on their military successes. It is feared that a war of attrition will continue, with attacks in depth and disastrous consequences for the population on both sides. This war of attrition also extends the field of action to the defence industry, which will be crucial to the continuity of operations.

BATTLE GROUP

Since July 2023,

The Belgian Defence is participating in The Battle Group, deployed in Romania under French command, with the aim of reinforcing NATO presence on the eastern flank.

INFORMATION ON THE ROLE OF SGRS

In direct support of the various Defence detachments that are present in the Baltic States and Romania, SGRS provides intelligence, counter-intelligence and security assistance both in Belgium and on site.

Moreover, from a strategic point of view, SGRS plays an active role in keeping the government and its partners in the intelligence and security community informed of developments in the conflict in Ukraine, in particular by producing analysis reports on both the political and military aspects. SGRS' expertise enhances the understanding of Belgian political and military decision-makers of the many facets of the conflict.

Belgian UAV drones used primarily for reconnaissance missions.

Towards a Drone War

The use of drones, or Unmanned Aerial Systems (UAS), has long remained in the hands of conventional armed forces, although some terrorist groups have been using small commercial drones for propaganda purposes or light kinetic strikes for some years. Although the use of military drones was growing rapidly, it was not yet widespread.

Russia's invasion of Ukraine quickly changed that, with both sides stepping up technological developments in the field and their use. Military drones for reconnaissance flights or kinetic missions; targeted attacks with "kamikaze" or "One-way Attack" drones, whether industrially produced or improvised; use of small "First-Person View" commercial drones carrying small and medium-sized explosive charges to hit vehicles or personnel; Unmanned Surface Vessels (USV) to destroy enemy fleets, ... The use of drones in the Ukrainian theatre is varied and extensive.

After more than two years of conflict, these new means of combat have become the driving force for a large number of manufacturers around the world and are beginning to be exported to other theatres.

These developments and the democratisation of some systems have convinced many emerging countries, mainly in Africa and the Middle East, to acquire military combat UAS (UCAV) to fight rebel or terrorist groups in their territory.

Among the main manufacturers of UCAVs, countries such as Turkey, China and Iran are exporting to these countries on a massive scale without little concern for international sanctions or legal or ethical issues.

Similarly, the Yemeni Houthis, with support from Iran, make massive use of drones, both air and sea drones, threatening maritime traffic in the Gulf of Aden and the Red Sea.

As part of the ongoing reinvestment in its armed forces, Belgium will have to take account of this major development in battle management.

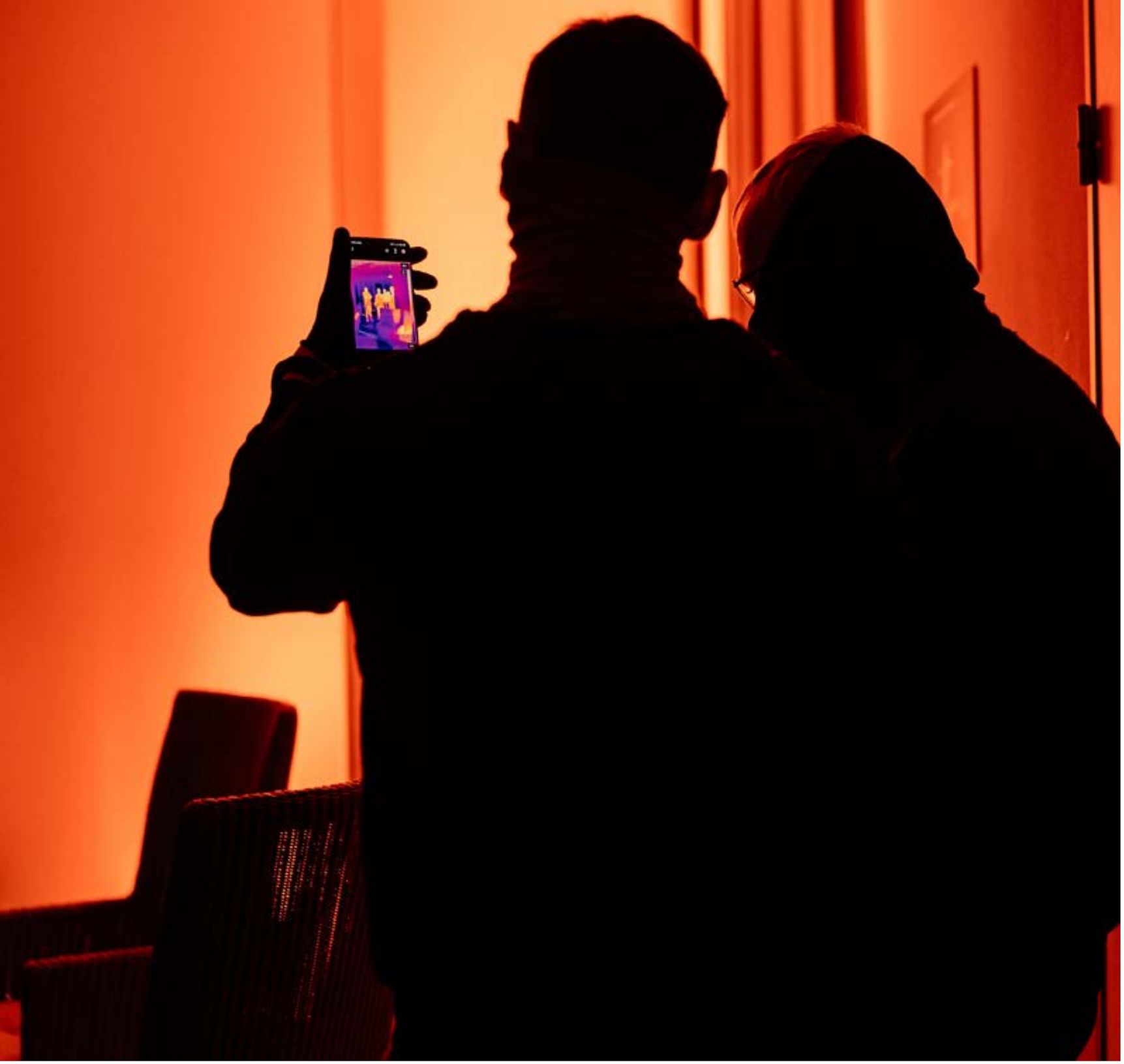
The European "COURAGEOUS" project aims to develop a standardised test method for anti-drone systems.

Hybrid Attacks on Critical Infrastructure

In 2023, Russia launched a large-scale campaign targeting critical Ukrainian infrastructure. This campaign particularly targeted the electricity production and distribution network, using intensive and recurrent bombardments (cruise missiles, hypersonic missiles, drones, etc.) as well as cyber-attacks.

For instance, a cyber actor linked to the Russian Military Intelligence Service (GRU) has launched destructive cyber operations at critical infrastructures such as power plants, network and telecommunications operators. In addition, Russian cyber espionage operations have aimed to impede counter-espionage efforts and war crimes investigations.

A clear trend can be observed: Russian cyber actors repeatedly target the same organisations, conduct sustained attacks against Ukrainian media and attempt to circumvent Ukraine's improved detection and recovery capabilities through faster data exfiltration.



TESTIMONIAL

“I worked on three continents in 2023.”

Matthew, 36

In practice, the SGRS is always directly or indirectly involved in all Defence operations. Every year, they are reviewed and translated into operation plans. This happens on land, at sea, in the air and in the cyber domain. But what does a working day in the life of an SGRS officer abroad look like and what do they have to deal with on a daily basis?

“My name is Matthew and I work in the deployable teams of SGRS. With my small team, I go abroad for longer periods of time and I operate in places, where Defence detachments are also present.

What do I do there on a day-to-day basis? I’m in regular contact with the local security services and other partners. In the evening, I write a report on those conversations, which is sent both to the headquarters in Brussels and to the Belgian troops deployed in my region. I then meticulously prepare my interviews for the following day. That way, I keep my finger on the pulse and help detect changes in the situation. In this way, I can keep the Belgian troops informed and help to protect them.

My job is very varied and exciting. Last year I worked on three different continents: Africa, Europe and the Middle East. Eventhough the nature of the work does not change on the different continents, each time I have to adapt to local circumstances and the culture of the local partners.”

Israeli-Palestinian Conflict: Resonance Beyond Borders

The Hamas terrorist attack on 7 October 2023 triggered a series of events, the outcome of which is still unknown. Military operations, armed incidents and protests are on the increase both in the region and internationally.

One Country, Four Conflicts

Since the outbreak of the conflict, tensions on Israel's borders have continued to grow, creating an increasingly complex and multi-faceted situation.

In Gaza, the population finds itself between a rock and a hard place. Israeli operations in response to the attack of 7 October 2023 are aimed at eliminating or weakening the military potential of Hamas, but are causing a profound humanitarian crisis with a high toll in human lives and massive destruction.

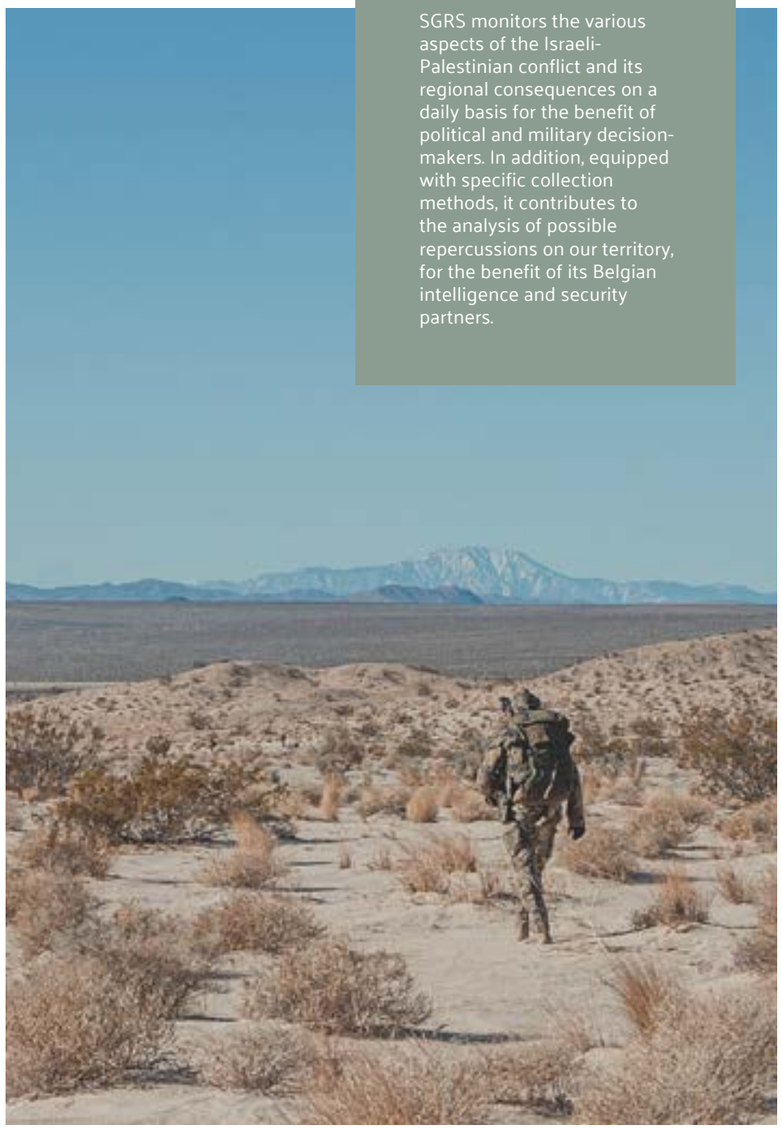
In the West Bank, the temperature continues to rise. Violent clashes between the Palestinian population on the one hand and Israeli troops and settlers on the other are becoming increasingly frequent.

In northern Israel, on the border with Lebanon, the Hebrew state faces the risk of open conflict with Hezbollah. Since 7 October, incidents and mutual bombardments have increased.

Within Israel itself, a fourth dimension of the conflict is the growing polarisation that divides the Israeli population and its politicians.

Constant monitoring

SGRS monitors the various aspects of the Israeli-Palestinian conflict and its regional consequences on a daily basis for the benefit of political and military decision-makers. In addition, equipped with specific collection methods, it contributes to the analysis of possible repercussions on our territory, for the benefit of its Belgian intelligence and security partners.



A Deadly Game of Proxies

The SGRS notes that Iran is not only involved behind the scenes, but also through its impressive network of militias and proxies in the region.

In Lebanon, Hezbollah's military capabilities are a direct threat to Israel. Although Hezbollah conducted small-scale military operations against Israel after 07 October 2023, leading to counterattacks by Israeli forces, a major conflict has been avoided so far but is still looming.

In Syria, the presence of pro-Iranian Shiite militias and elements of the Iranian Revolutionary Guard Corps demonstrates the complexity of the situation there. These forces, which have enabled the Syrian regime to restore its authority over large parts of its territory, have established themselves there for the long term. Israeli forces regularly carry out air strikes against these militias and Iranian elements, particularly in the east of the country and along the demarcation lines with the Golan Heights. Although the Syrian president has officially taken a position in favour of the Palestinians, no concrete action has been taken.

In Iraq, the pro-Iranian Shiite militias assembled in the "Islamic Resistance in Iraq" pose a threat both to the stability in Iraq and to the forces of the international coalition. In October 2023, these militias launched a series of attacks on US bases in Iraq and Syria as well as on a US base in Jordan. The United States responded with strikes against pro-Iranian militias in Iraq and Syria, but without directly confronting Iran. At the political level, pro-Iranian actors exploited the incident to reiterate their demand for the withdrawal of US troops from the territory. A parliamentary vote to this effect failed, but negotiations with the US are continuing.

In Yemen, the Houthi movement, which controls the north of the country and the capital, has undertaken a series of actions in the

region that pose a direct threat to freedom of navigation in the Red Sea. They have carried out direct attacks on Israel. They have also conducted offensive actions in the Red Sea and the Gulf of Aden with the aim of attacking commercial vessels with links to Israel. Since November 2023, more than sixty attacks have been recorded, mainly using missiles and both air and sea drones. When the US and the UK carried out strikes targeting Houthi military capabilities in Yemeni territory, the movement extended its actions to US and British commercial vessels. A US-led coalition led to the deployment of several military vessels in the Red Sea.

Protection of maritime traffic

In February 2024, the European Union officially launched an additional operation, ASPIDES, which is purely defensive in nature and aimed at protecting maritime traffic. The frigate Louise-Marie is the Belgian contribution to both ASPIDES and the European Maritime Awareness in the Strait of Hormuz (EMASoH) operation, which has been ongoing since 2020. Both these multinational missions are aimed at preserving freedom of navigation in the Red Sea and the Strait of Hormuz, respectively. SGRS is providing intelligence and security assistance as part of this deployment.

A Conflict Impacting Western Democracies

The controversies surrounding possible war crimes are generating tensions within the Western democracies themselves. These internal tensions in the Western democracies and the controversies surrounding war crimes mean that Israel runs the risk of becoming increasingly isolated.

Network of Militias, Proxies but also Hacktivists

For Iran, Israel remains a key cyber target. Destructive cyber-attacks, sometimes disguised as ransomware, continue steadily. The Iranian regime regularly carries out cyber-attacks against members of the opposition and Iranian dissidents, both in Iran and in Europe.

The war between Israel and Hamas shows that in a new conflict, hacktivists can be mobilised at short notice and, at the request or with the cooperation of the intelligence services, attempt to carry out disruptive or destructive operations. In the conflict between Israel and Hamas, not only government services and critical infrastructures have been targeted, but also the warning systems in case of a missile attack.

TESTIMONIAL

Rachel, 42, is an “agent handler”

In her daily work, she is in contact with “human sources”. In 2023, she participated in an operation in the Middle East to recruit people who could provide intelligence.

“I met an African source, a very delicate person I met in a third country. She did not know that I was working for SGRS, but during our meeting she shared some sensitive information that might be of interest to us.

The difficulty of my job lies in the fact that I have to be very flexible and, at the same time, I have to be able to act very discreetly. During such interactions, I always look for motivations that could make these people want to help us more concretely, such as a financial motivation, but more often than not it is ideological.

This job gives me immense satisfaction, especially if, through my efforts, I can gather vital information that can be useful to our country.”

AFRICA

Coups d'Etat, Interference and strategic Realignment

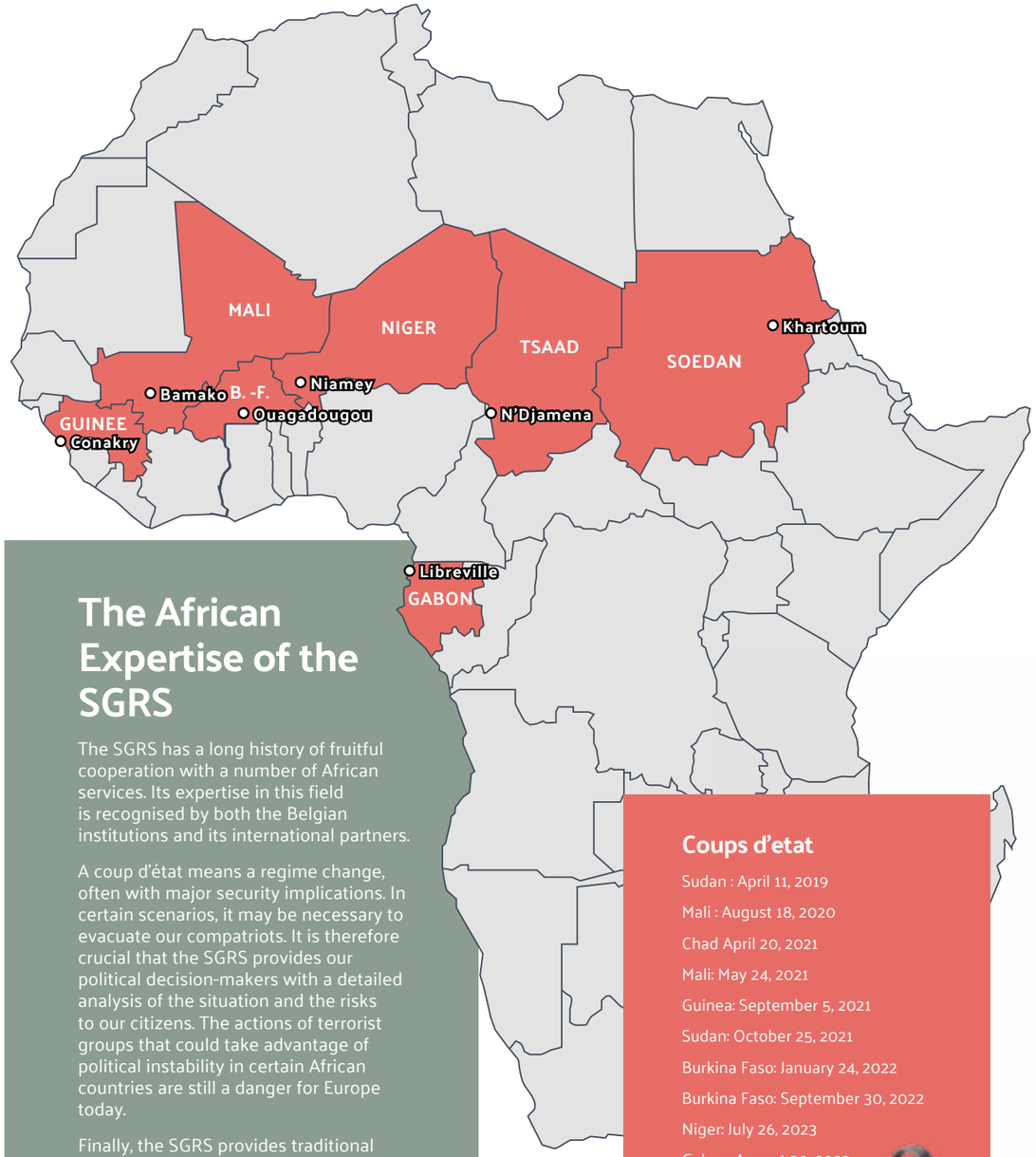
While the Israeli-Palestinian and Russian-Ukrainian conflicts dominate the headlines, developments are taking place in Africa that can have just as significant an impact over the long term. The SGRS must devote all its attention and expertise to informing its clients of these developments.

Upsurge in Coups d'Etat

Military coups d'état have once again become a worrying feature of the African political landscape in recent years. In the past three years, Africa has seen no fewer than eight such coups, including in Chad, Guinea, Mali, Burkina Faso, and in Niger and Gabon in 2023.

The root cause is the inability of certain governments to respond to the socio-economic and security challenges faced by part of the population, and this perceived failure of authority leads to putschist actions. This can give rise to two phenomena: first, one putsch can hide another if the quality of life does not improve in the short term. Secondly, putschists tend to announce a transition fairly quickly, only to have it postponed indefinitely.

Although the African Union (AU) and regional organisations such as the Economic Community of West African States (ECOWAS) have condemned coups, their political decisions and economic sanctions have so far been rather ineffective. Their lack of capabilities and their often inconsistent fight against coups and other unconstitutional changes of government remain worrying.



The African Expertise of the SGRS

The SGRS has a long history of fruitful cooperation with a number of African services. Its expertise in this field is recognised by both the Belgian institutions and its international partners.

A coup d'état means a regime change, often with major security implications. In certain scenarios, it may be necessary to evacuate our compatriots. It is therefore crucial that the SGRS provides our political decision-makers with a detailed analysis of the situation and the risks to our citizens. The actions of terrorist groups that could take advantage of political instability in certain African countries are still a danger for Europe today.

Finally, the SGRS provides traditional intelligence and security support to Belgian military deployments in Africa.

Coups d'etat

Sudan : April 11, 2019
Mali : August 18, 2020
Chad April 20, 2021
Mali: May 24, 2021
Guinea: September 5, 2021
Sudan: October 25, 2021
Burkina Faso: January 24, 2022
Burkina Faso: September 30, 2022
Niger: July 26, 2023
Gabon: August 30, 2023

War in Africa Too

It is not just in Ukraine that an interstate war is raging. On the African continent too, Rwanda and the DRC are engaged in a quasi-interstate war. Admittedly, this is partly done under the cover of auxiliaries present in Eastern Congo and manipulated for the benefit of one of the belligerents, following the example of the M23 rebels.

Other African nations have been hit by armed insurrection or civil conflict. Sudan, in particular, saw the outbreak in April 2023 of a war between two major factions of the military and security apparatus: the military forces and the rapid support forces. These two factions also enjoy their own external support.

Strategic Realignment

In 2023, the African continent underwent significant changes, reflecting an ongoing strategic realignment in several African states. These states are turning away from their traditional partners, particularly Western ones, in favour of other players.

Following the collapse of the G5 Sahel joint force, the international presence in the region is gradually being withdrawn. MINUSMA withdrew from Mali in December 2023, and the French military presence in the Sahel has also decreased significantly.

In Central and East Africa, the international presence has been reduced too: in the Democratic Republic of Congo, the United Nations is preparing for the end of MONUSCO, while in Somalia, the African Union implemented the departure of ATMIS at the end of December.

China and Russia have increased their influence in the “Global South” in a number of areas. However, the two states take different approaches to establishing privileged relations with certain African states. Russia favours military and security cooperation, while China is establishing its cooperation primarily in the economic sector. Other nations, such as Turkey, Iran and the Gulf States, are also getting mixed up in the great African game and are also increasing their involvement in certain African areas.

The result of this strategic realignment is an upheaval in the landscape of foreign interference on the African continent.

MINUSMA: United Nations Multidimensional Integrated Stabilisation Mission in Mali

MONUSCO: United Nations Organisation Stabilisation Mission in the Democratic Republic of Congo

ATMIS: African Union Transition Mission in Somalia

© AFP

Russia Extends its Sphere of Influence to Africa

African countries are in Moscow’s sights. Russia, which is increasingly resorting to anti-Western disinformation, the use of Russian mercenaries and, more generally, the weakening of democratic institutions, is seeking closer ties with a whole series of African states.

It specifically uses the argument that Western countries continue to exploit African populations and imposes the so-called ”anti-colonialist” Russian model. Although Russia’s economic impact in Africa pales in comparison with that of the West or China, it has managed - particularly in the volatile Sahel region - to forge stronger links with a number of countries, partly through the deployment of mercenaries (Africa Corps - formerly Wagner).

Meanwhile, following coups d’état in Guinea, Mali, Burkina Faso, Niger, Sudan and the Central African Republic, several pro-Russian governments are already in power. In practice, this creates a more or less contiguous zone of autocratic regimes and, in addition to strong anti-Western feelings in these countries, also develops insecurity and illegal migratory flows.

Outside the Sahel region, Russia’s influence is not negligible, even if more limited. For example, several African governments, such as South Africa, are also choosing to strengthen their ties with Moscow, despite the Russian invasion of Ukraine. This is partly due to dissatisfaction with their lack of representation and influence in international institutions, but also to pragmatic economic considerations.

OUR ACHIEVEMENTS IN 2023

Quality products for our partners

The quality of several of the SGRS' analysis products has been praised by NATO institutions, as shown by the fact that these products have been included in the reading portfolios recommended to members of the organisation. This highlighting of the SGRS' products underlines the recognition by international bodies of its expertise in the fields it covers.

Closer cooperation with the academic world

A memorandum of understanding has been signed with the Royal Military Academy (RMA), our 'bridgehead' with Belgian and foreign civilian universities. Its fields of application cover different areas of cyberspace, such as 5G and cryptography, and help to support numerous long-term research and development projects, both for the benefit of Defence and civil society.

Increased efforts to raise awareness

Whether it is measures to protect ourselves against the risk of espionage, new security directives or cyber security measures, the SGRS has focused on raising awareness among all Defence personnel in order to increase the security of the organisation. These awareness-raising initiatives are carried out through information and communication campaigns within the SGRS.

The Belgian Cryptography Centre of Excellence is born

In partnership with the RMA, its structure has been defined and resources allocated. Ultimately, this Centre of Excellence, inspired by the French model, will produce technical expertise for the benefit of its federal and international partners.

Cyber security expertise to support our federal partners

The Cyber Command of the SGRS, an expert in cyber audit and control, has been appointed by the National Security Council to approve the new federal classified BSC (Belgian Secure Communication) system, which will be used by all Federal Public Services in the future.

Consolidated cooperation with the National Geographic Institute

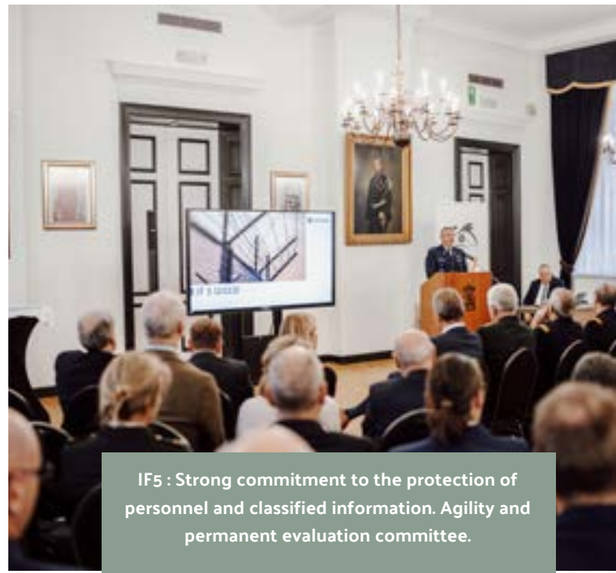
The signing of a cooperation agreement with the NGI in 2023 will maximise synergies, in particular by encouraging the transfer of personnel, and will structurally associate the National Geographic Institute with the Defence geostrategy as a centre of expertise.

Updating military security standards

Military security standards have been updated and optimised to improve the Defence security culture, in line with the recommendations of the Committee I and the action plan issued following the "Jürgen Conings" case.

Joint platform with State Security ECTC

The SGRS and State Security Service worked together throughout 2023, leading to the creation of a joint platform to combat extremism and terrorism, whether confessional or ideological.



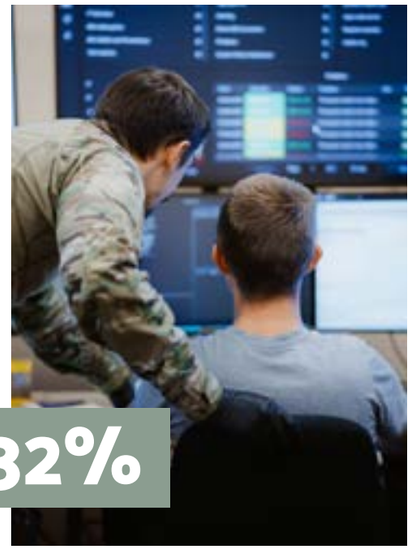
IF5 : Strong commitment to the protection of personnel and classified information. Agility and permanent evaluation committee.

First edition of Cyber Summer School

This summer course, offered by the SGRS' Cyber Command for the first time in 2023, is designed to give young people an insight into the cyber defence challenges of today and tomorrow, as well as helping to attract new talent. The SGRS continues to invest in its human capital.

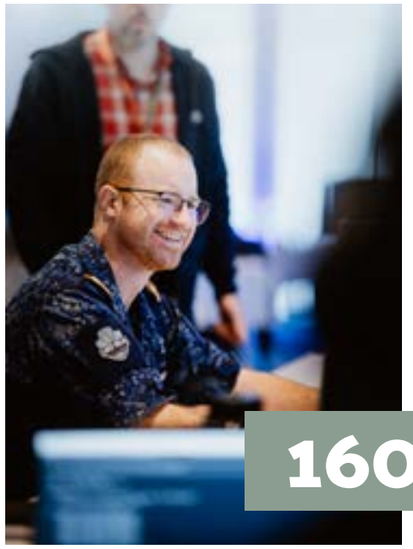
FACTS & FIGURES

6% increase in personnel



32%

CIVILIANS AT THE SGRS



160

MORE THAN 160 RESERVISTS EMPLOYED BY THE SGRS

652

"PAPERS" PRODUCED AND VALIDATED BY THE INTELLIGENCE DIRECTORATE: ANALYSIS DOCUMENTS SHARED WITH OUR CUSTOMERS/PARTNERS

7226

"REQUESTS FOR INFORMATION" REQUESTED BY OUR PARTNERS AND PROCESSED BY THE SGRS

236

NUMBER OF BIMS (EXCEPTIONAL INVESTIGATION METHODS)

5483

SECURITY CHECKS PROCESSED

NUMBER OF SATELLITE IMAGES/ NUMBER OF MAPS CREATED FOR OPERATIONS:

15560
images taken, including 3,154 produced

747
Requests for geographical support

5
Topographical missions carried out

Part II

Assessing the State of Threats to Protect Ourselves against Them

Conflicts beyond borders are shaping the world of tomorrow and defining the threats that our country must be able to deal with.

We are already seeing a high level of espionage threats; an increase in attempts to influence and interfere, and cyberattacks on Belgian and European institutions and companies. Our mission is to prevent forces outside our society from exploiting divisive issues, such as the war in Ukraine or the Near East, to destabilise our democratic model.

The Threats Posed by Disinformation and Influence Operations

Influence operations are on the increase, more diverse channels are used and their impact on behaviour is becoming increasingly perceptible. Examples include the unrest surrounding EVRAS, several farmers' demonstrations and riots following the "Nahel" case in France, all of which have left a tangible and violent mark on our society.

On the eve of the Belgian and European elections, among others, these events are putting our authorities on high alert in the face of efforts to exert influence by hostile state actors such as Russia, China and Iran. Since Twitter became X, the number of "coordinated inauthentic behaviours" has been on the increase. The use of Telegram, the channel of choice for pro-Russian actors, is on the rise in Belgium, with 12% of users of the platform. The anti-vax and COVID conspiracy groups are still active, and others have developed around new themes such as climate, energy and immigration. Recent events have clearly shown that the boundary between the virtual and real worlds is becoming increasingly blurred and can lead to physical violence. In line with our missions, these attempts to influence and spread disinformation must absolutely be monitored.

In 2023, the SGRS took the lead of the Agile Taskforce Information Operations (ATFIO), a working group made up of the main players in security. The aim of this cooperation is to develop a unified and global approach to Foreign Information Manipulation and Interference (FIMI), particularly in relation to the 2024 elections.

2023

Over the past year,

ATFIO[1] has organised numerous multilateral meetings, enabling information to be exchanged between the various stakeholders, and an early warning system has been developed to detect any foreign influence activity at an early stage. This project will be developed and strengthened in the future, as attempts at disinformation are constantly being monitored.

Conspiracies on Telegram

Russia's efforts to influence and its disinformation ecosystem to reach national and European audiences focus primarily on Telegram, the channel par excellence for spreading pro-Kremlin narratives and fuelling conspiracy theories. Russia skilfully exploits any event likely to polarise public opinion and weaken public confidence in their governments and institutions.

[1]ATFIO Agile Taskforce Information Operations

Espionage Threats on the Rise

Espionage is defined in Belgian law as the search for or provision of information not accessible to the public and the maintenance of secret relations likely to prepare or facilitate such acts

For the SGRS, this means any information that could help an ill-intentioned outsider to hinder the execution of defence missions, and therefore not just secret or confidential information in the strict sense of the law.

As the host country of several international organisations such as NATO and the EU, Belgium is a prime target and the SGRS is jointly responsible for their protection. The SGRS believes that the current geopolitical context means that our institutions are facing a very high level of espionage threats and interference. This trend is set to continue in 2024.

Throughout 2023, the SGRS conducted various intelligence investigations in the field of counter-espionage and counter-intelligence. When necessary, the SGRS took measures to neutralise the existing threat, in cooperation with or in support of its Security Directorate, the Directorate General Human Resources of Defence and its Belgian partners (State Security, Public Prosecutor's Office).

The SGRS notes that the techniques used in espionage are diversifying, thanks in part to technological developments, but the traditional use of human contacts as a source of information remains a widespread method. In 2023, several cases of attempted espionage were identified and thwarted.

That is why particular attention was paid this year to raising personnel awareness of the techniques used by foreign intelligence agents and how to protect ourselves against them. In 2023, a large-scale internal awareness campaign was carried out. In the future, prevention tools will be developed and made available to all Defence personnel.

Espionage, Also in the Machinery of Cyberspace

In addition to the theft of commercial secrets and intellectual property, espionage activities by Chinese cyber actors are on the increase, targeting in particular the institutions of the European Union and the government agencies of European countries and NATO. One of their aims is to find out the positions of European countries on Taiwan and the European initiatives aimed at reducing the risks associated with economic dependence on China.

These actors are using increasingly complex network structures, hacking into the insecure infrastructures of individuals and companies or exploiting "zero days" vulnerabilities.

Belgian public bodies, including Defence, have also fallen victim to Chinese cyber espionage. However, these attacks were limited to espionage purposes and did not establish persistent access to the data of the targeted institutions.

In addition to cyber actors linked to Chinese intelligence agencies, Chinese public and private companies also represent a potential cyber threat. China's National Intelligence Law allows Chinese intelligence agencies to demand that Chinese companies and citizens anywhere in the world cooperate at all times. Chinese hardware and software solutions used in the telecommunications and transport sectors are therefore a potential threat of cyber espionage, now and in the future, including in Belgium.

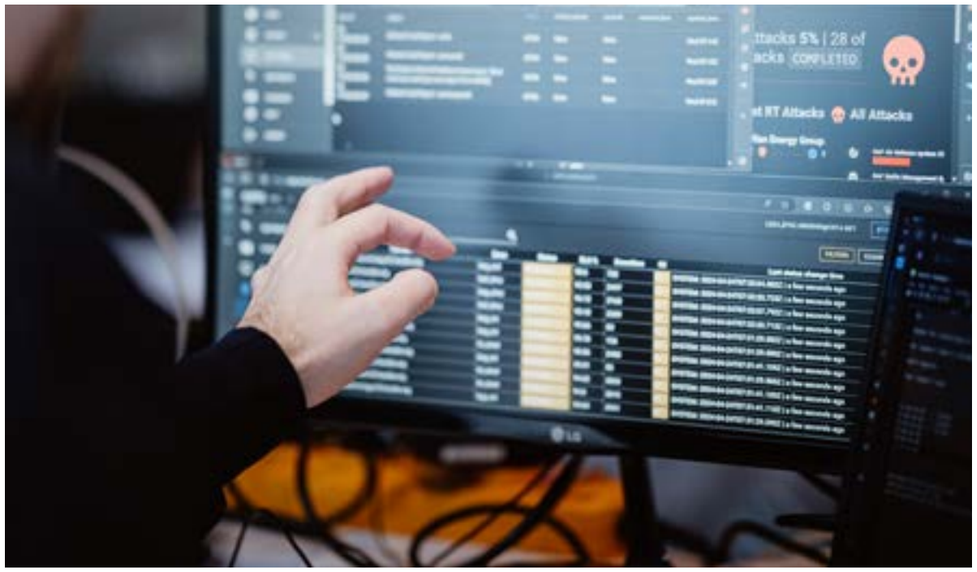
The SGRS has a duty to develop the capabilities needed to protect Belgian interests. Alongside its partners such as the Centre for Cyber Security Belgium (CCB), the National Crisis Centre (NCCN) and the Federal Public Service Justice, the SGRS' Cyber Command is making an active contribution to national cyber resilience. It routinely supports joint efforts by providing technical advice and has sophisticated defensive capabilities.

Cyber Threats: Belgium and Its Allies Fall Victim to Pro-Russian Hacktivists

Within the context of the Russian-Ukrainian conflict, Russian cyber espionage operations, carried out by a cyber actor linked to the Russian Foreign Intelligence Service (SVR), have mainly targeted the diplomatic institutions of the Member States of the European Union and NATO. These operations have led to an increase in the frequency of attacks and the ongoing deployment of new malware designed to thwart the detection tools in place. What is more, because of their increasing use by government authorities and companies, intrusion into Microsoft Cloud solutions has become a major objective for this cyber actor.

At the same time, pro-Russian hacktivists carried out so-called "distributed denial of service" (DDoS) attacks in almost all NATO member states. By overloading websites with multiple malicious requests or data, they prevent them from functioning properly. Belgium has also been the victim of several of these attacks, particularly on government, port and air traffic control sites. In general, however, these cyberattacks have had only a limited impact. Instead, hacktivists exploited the media attention to feed Russian disinformation campaigns.

Various sources of information show that Russia is continuing to develop its cyber-sabotage capabilities and carry out operations in cyberspace with a view, in particular, to corrupting critical infrastructures.



TESTIMONIAL

"Cyber defence is above all a question of prevention and detection", Gilda, 40

Almost every month, Belgium suffers disruptive attacks by pro-Russian "hacktivists" targeting the websites of various government agencies. In addition, the cyber units of the various Russian intelligence services are constantly trying to exploit software weaknesses or gain user access to systems through phishing and other techniques. Intrusion attempts are constantly on the increase in both public and private organisations.

As a transversal capability, the SGRS Cyber Command's mission is to protect the networks and weapons systems used by Defence. Gilda, a CSOC (Cyber Security Operations Centre) analyst, is on the front line of cyber defence.

"As a data analyst, my role is to analyse data for both preventive and reactive purposes. With my team, we monitor the Defence networks and ICT infrastructures, generate alert systems to detect abnormal activities and, in case of detection, determine the actions and measures to be taken to ensure optimum security.

My leitmotiv is to help protect our country and its people. Today, in my role, this seems truer than ever. On a daily basis, I react to security flaws that are very real, and I take concrete action for the benefit of our security and therefore that of our country."

Proliferation Threats

In the area of proliferation, 2023 saw a growing trend in the transfer of sensitive technologies between states and to non-state proxies, including advanced tactical and strategic delivery systems used in Ukraine and the Middle East. The increase in proliferation, despite established international norms, and Russia's increased use of nuclear coercion as part of its confrontation with the West (notably with the withdrawal from several strategic arms reduction treaties such as New START - Strategic Armament Reduction Treaty or CTBT - Comprehensive Test Ban Treaty), are accelerating the erosion of the architecture of non-proliferation of Weapons of Mass Destruction.

The decline of the non-proliferation architecture and the acceleration of competition between the major powers are leading to an arms race, including in strategic areas, and an increased risk of escalation and miscalculation. The development of ballistic and nuclear programmes by a number of sensitive countries (including - but not limited to - China, Iran and North Korea) and the difficulties encountered by international institutions in managing these advances are also a growing source of concern.

EU2024BE

Meeting of the Cyber Commanders

International Relations in Cyberspace

Interacting with national, international and multinational organisations remains one of our priorities. These interactions enable us not only to establish ourselves as a reliable international partner, but also to monitor developments in cybersecurity governance, support new initiatives and seek out potential opportunities for cooperation or synergies.

Regular meetings are held with our counterparts at the Centre for Cyber Security Belgium, Belgium's Permanent Representation to NATO and the European Union, as well as the Federal Public Service Foreign Affairs to work together more effectively to meet the challenges of today and tomorrow.

In 2023, a special effort has been made to align national strategies and processes with the new cyber security policy and governance defined by NATO and the EU. This is vital to ensure harmonious cooperation and maintain the technical interoperability of our countries. In March 2023, the Cyber Command became a full member of the Cyber Rapid Response Teams (CRRT), a project designed to enable Member States to help each other achieve a higher level of cyber resilience and respond collectively to cyber incidents.

Part III

Facing up to Threats and Contributing to National Resilience

The SGRS anticipates technological developments, maintains its expertise and contributes to homeland security together with its partners.

To ensure our security and contribute to national resilience, we must not only maintain our expertise in a whole range of areas, but also anticipate technological and societal developments in the years ahead. Through partnerships, our organisation is adapting in all its lines of development and is constantly strengthening its ability to fulfil the missions entrusted to it. In the event of a national or international crisis, the SGRS may be called upon to provide expertise or technical support. Staying at the cutting edge of technology and the latest trends is therefore not just a strategic objective, it is a necessity. This is achieved through partnerships with the intelligence community, industry, academia and associations. Optimisation and innovation are the key words here.

Common Platforms in the Fight against Extremism and Terrorism

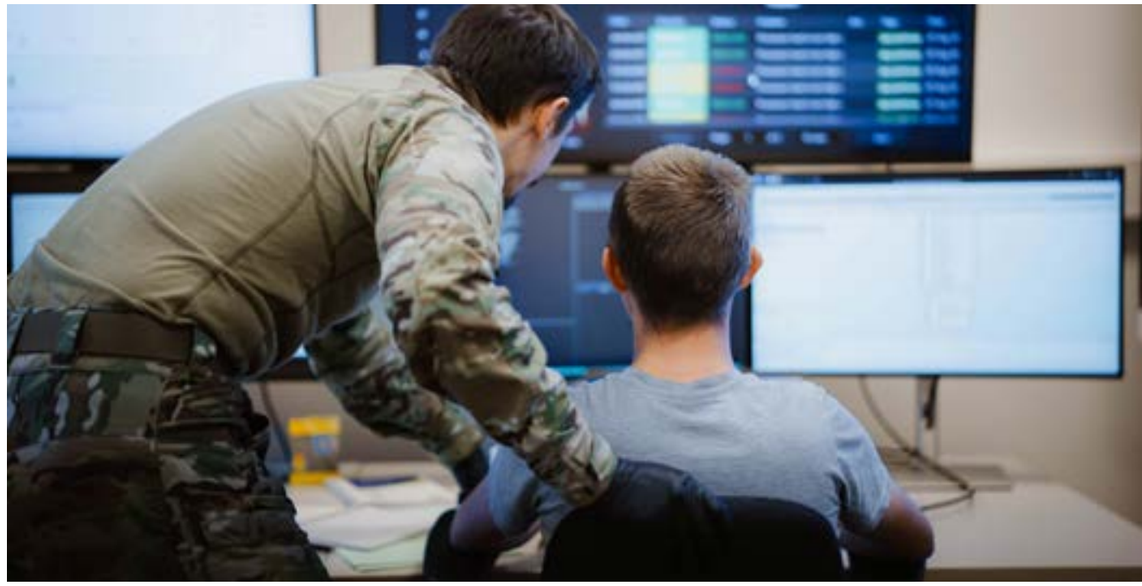
In 2018, the SGRS and State Security agreed on the "national intelligence strategic plan", an ambitious plan for enhanced structural cooperation to better combat the common threats that fall within their remits. Since 2022, it has been in its second iteration, marked by a strengthening of areas of cooperation and synergies. The aim is for each service to benefit intelligently from the comparative advantages of the other, particularly in terms of expertise and specific collection resources, and also to pool efforts in the fight against certain specific threats.

At the beginning of 2024, the joint platform to combat extremism and terrorism, both confessional and ideological (right-wing and left-wing extremism) came into force. The SGRS and State Security personnel now work within a single entity, optimising the exchange of information and the use of available personnel. This is a major extension of an existing joint platform that has been operational since 2018. The latter, which was limited to the fight against confessional terrorism, has led to many advances.

The recent terrorist attacks in Europe and Belgium have demonstrated the need for closer cooperation between our various intelligence services. This synergy should enable maximum exchange of information, pooling of resources and joint assessment for our partners. Among other measures, mixed teams of SGRS and State Security personnel will be set up.

In the long term, this cooperation will also cover other types of threat, in particular espionage and interference, according to procedures specific to each threat. Better information sharing and coordination should make it easier and more effective to unmask spies operating on our territory or working against our national interests.

Alongside these advances, the national intelligence strategic plan also covers Information and Communication Technologies (ICT) and training. Its gradual implementation reflects the desire of the two services to work together ever more closely, in mutual respect and trust, in accordance with the national motto "Strength through Unity".



Military Security Assured, National Security Strengthened

Following the “Jürgen Conings” case in 2021, a series of measures have been defined in an action plan aimed at improving Defence’s security culture.

The year 2023 saw the implementation and completion of a number of them, namely the updating of Defence military security standards by a SGRS working group.

Espionage, subversion and sabotage, as well as terrorism and organised crime, are realities that the entire organisation must be able to tackle with agility. The implementation of these new standards, based on potential risks and taking into account technological developments and new legislation, is a key step in guaranteeing Defence’s security. But also that of its industrial and institutional partners, both national and international. In the event of incidents, the actions to be taken are defined to restore operational readiness as quickly as possible.

Considerable efforts have been made in a number of areas, such as raising awareness at all levels of command, training, monitoring security clearances and stepping up controls on weapons and ammunition.

The aim of all these measures is to guarantee the rigour but also the flexibility necessary for Defence to adapt to its constantly changing security environment, as well as increased collaboration between the various competent authorities.

In Concrete Terms

1. Introduction of the “Security by Design” concept, including cyber security, into the design of Defence infrastructures.
2. Strengthening exchanges between the units, the General Intelligence and Security Service (SGRS) and the Directorate General Human Resources (DGHR).
3. Increased awareness, training and controls at all levels of command.
4. Checking the reliability of Defence employees from the moment they are recruited and throughout their careers.
5. Establishment of a permanent assessment body capable of making adjustments in the light of technological or contextual developments, for example.

A student officer of the RMS before the 21 July parade.

TESTIMONIAL

“I wanted to refocus on a job with strong values.” Jean, 30

At Defence, all current and future communications and weapons systems are based on the use of cryptographic keys. Their operability and freedom of movement depend directly on this. Jean, aged 30, an IT engineer specialising in cyber security, is currently Systems Audit and Accreditation Manager. After working for various multinationals, he joined the Cyber Command.

“I wanted to refocus on a job with strong values. So, I naturally gravitated towards Defence. Here, I feel part of a team and we work together to achieve a common goal. On a day-to-day basis, my role consists of approving weapons systems or ensuring their level of security. It touches on just about everything, from network infrastructure to systems linked to the F-35, the new motorised capability (CaMo), and the Belgian-Dutch minehunter programme.

My job is quite varied. Tomorrow, I will be at the Royal Military Academy (RMA) for training, then I will be doing a check at the Peutie barracks and the following week I will be going to Strasbourg to support Eurocorps … There is a diversity of actions and tasks that keep the job interesting, even if my function remains the same.

In fact, the SGRS’ Cyber Command has really put the means of its ambitions on the table. There is a political will that is directly translated into action, and I like that.”

Jean and his team will also be involved in the design of the future headquarters in Evere, where they will be responsible for controlling home automation, electromagnetic emission security standards and many other systems.

Keeping Up the Momentum of Technological Change

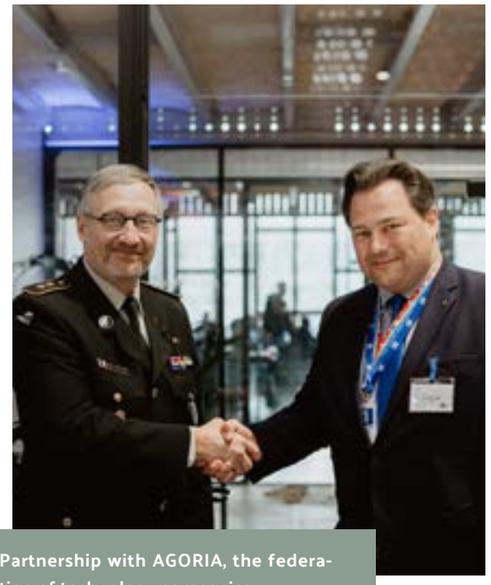
Cyberspace has become one of the most powerful vectors for spreading threats. Attempts to break into defence systems are on the increase, as is the explosion in cyberattacks on both public and private structures, particularly within the context of Russia's war of aggression against Ukraine. Being able to respond to these threats in the various areas of cyberspace is one of the founding roles of the Cyber Command.

The SGRS' Cyber Command has been allocated €140 million to develop its capabilities as part of the STAR plan, which also includes the implementation of the Defence, Industry and Research Strategy (DIRS) to focus on the development of a strong and technologically advanced Defence industry.

When it comes to cyber defence, cooperation with industry, national research centres and academia is a sine qua non for the development of new technologies. The Cyber Command, a future component of Defence and still within the intelligence sphere, must be able to guarantee in the short and long term the knowledge and resources needed to respond to current and future high-tech threats.

Within this context, a structural cooperation agreement was signed with the Royal Military Academy on 26 June 2023, designating the latter as a privileged partner in cyber research and development projects. It supports numerous long-term research and development projects for the benefit of Defence and civil society. In addition to this cooperation, exchanges are underway with other university bodies such as UC Louvain, the University of Ghent and HOWEST.

Intensive cooperation is also being developed with industry through Cyber Made in Belgium for Defence (CMIB4Def), a joint initiative of AGORIA, the federation of technology companies, and the Cyber Command. It is based on the observation that improving our cyber defence and our collective resilience will necessarily require closer links between Defence and industry. The discussions and work carried out within CMIB4Def cover subjects such as support for Defence operational capabilities, strengthening the cyber defence supply chain and developing cyber skills.



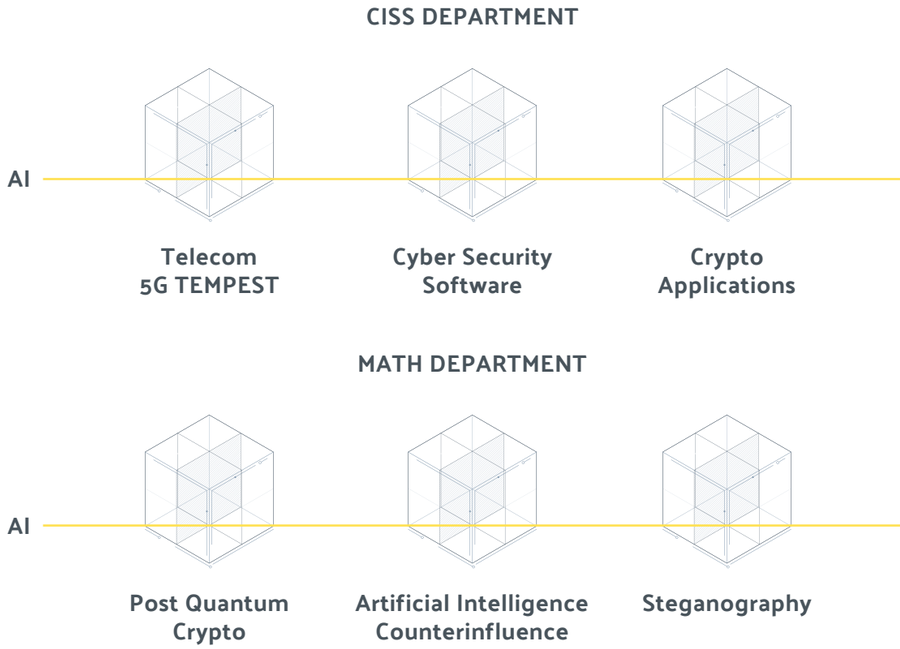
Partnership with AGORIA, the federation of technology companies.

ESA

Since May 2023, the Cyber Command has also been working with the European Space Agency on the development of their training centre, the European Space Security & Education Centre (ESEC) in Redu. This structural cooperation aims to promote exchanges between the two parties, including research and development in the field of quantum technologies.

OUR SIX AREAS OF RESEARCH

An example: guaranteeing the availability of a 5G network in the event of a crisis



Involved in numerous projects in collaboration with the academic and industrial worlds, the Cyber Command is constantly preparing for the future. One of the key areas for developing our national cyber resilience is the protection of critical networks and infrastructures.

The aim of a project stemming from the memorandum of understanding with the Royal Military Academy is to study, in collaboration with Orange Belgium, the use of a 5G installation to support 'critical' networks at Belgian Defence bases. These networks must be able to provide permanent support for operations or logistical and technical support for emergency plans. It is therefore important for Defence to analyse what type of 5G infrastructure is suitable for this requirement in terms of information security (confidentiality, integrity and availability) and communications (integration with our existing networks, specific services, etc.).

In addition, to carry out its study, the consortium with Orange Belgium received subsidies for both experimental development and research infrastructure, including by responding to a call for subsidies launched by the FPS Economy. All in all, it will be possible to test and integrate critical solutions, as well as carrying out a complete assessment of cyber security and the 5G plan.

VISIT

Cyber Command

In January 2024, the Cyber Command of the SGRS received a visit from the Chief of Defence, Admiral Hofman.

Part IV

Developing Our Human Capital

Our personnel are the SGRS' greatest asset. The diversity of professions within our service and technological developments make it essential to continue investing in our human capital and to be more open to civil society.

hiring policy paradigms. It is looking at new ways of supporting talent, in collaboration with the academic world, associations and industry. When it comes to security and collective defence, the equation to be solved and the challenges ahead, both for companies and the public sector, are indeed considerable.

The professional world of cyber defence remains particularly demanding and competitive. And certain cross-disciplinary skills are sometimes insufficiently consolidated among those entering the job market. Within this context, any form of rigidity in recruitment and selection procedures could be detrimental.

In 2023, a number of initiatives have been launched to improve accessibility, streamline recruitment procedures and, of course, offer a training pathway more in line with the expectations of all stakeholders.

Well aware of their added social value in (re)getting young NEETs (Not in Education, Employment or Training) into work, players who provide training and employment opportunities are now striving to promote themselves as genuine recruitment partners. Their approach is to train learners not only to meet practical requirements, but also to meet the expectations and needs of future employers as effectively as possible. The SGRS intends to fully support these initiatives. By teaming up with talent providers such as Molengeek and BeCode, with whom it is already partnered, the SGRS is offering candidates the opportunity to enter the cyber defence sector in a more flexible way and to learn more throughout their professional lives. This effort should continue in 2024 with, among other things, the opening of its civil offices in Charleroi in the A6K[1] offices.

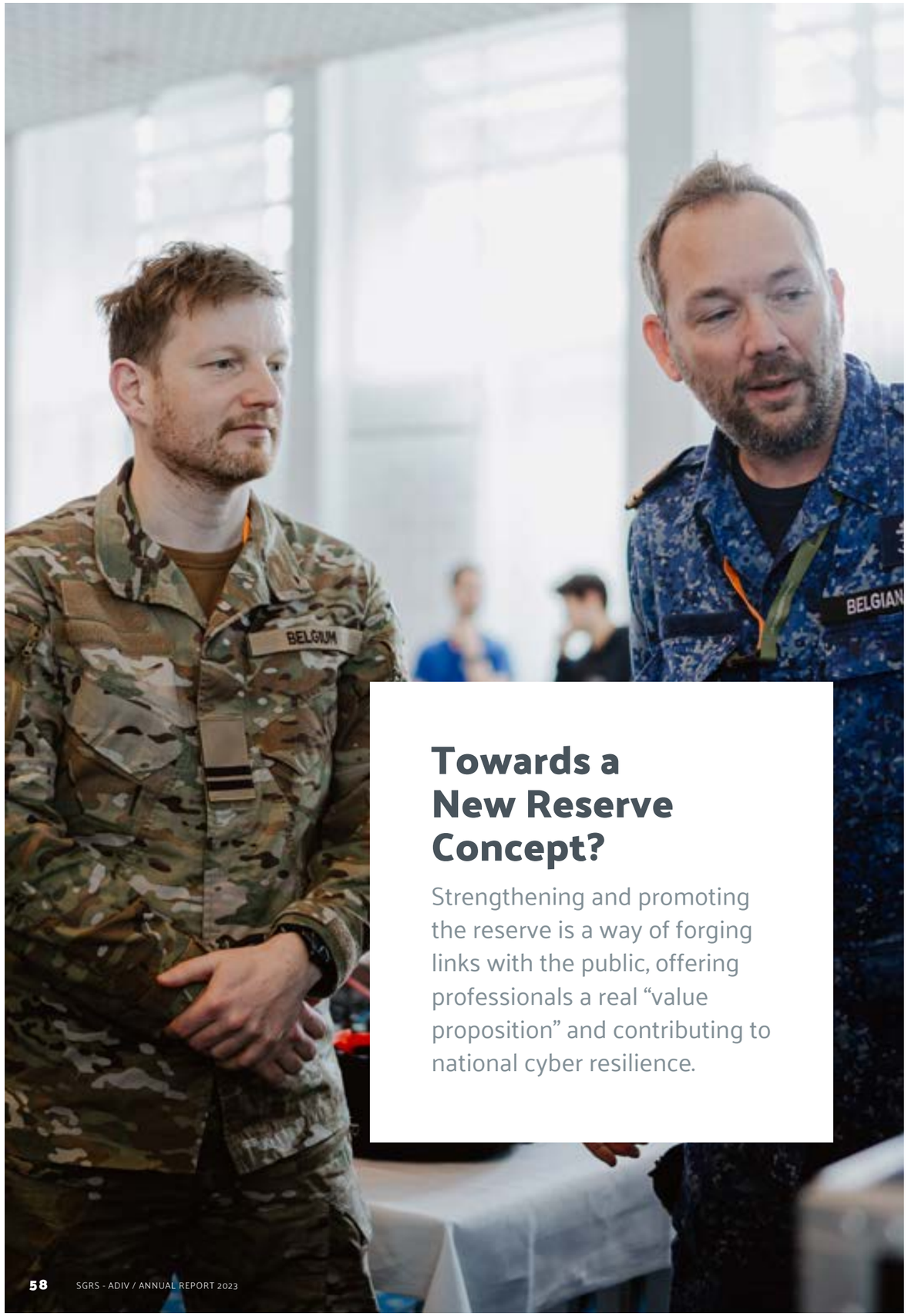
Among the initiatives designed to promote recruitment and train future cyber defence experts, both now and in the future, the SGRS is participating in the Cyber Made in Belgium for Talents research and innovation group initiated by Agoria, and is deploying its communication and accessibility efforts by organising targeted events. It is also aiming to develop its reserve more in line with the business world.

[1]A6K

A6K is a unique and stimulating ecosystem in the heart of Europe where industry leaders, emerging start-ups, universities, institutional players and research centres come together in one location to foster innovation in engineering.

Cyber Command maintains close contacts with non-profit organisations such as BeCode to recruit cyber experts under Rosetta contracts.

A “win - win - win” formula, in the short and long term, for everyone, from learners, young and not so young talents, to professionals and industries in the cyber security sector. In the future, the SGRS aims to offer a real ‘value proposition’ that is a win-win for all parties, always with a view to contributing to national resilience.



Towards a New Reserve Concept?

Strengthening and promoting the reserve is a way of forging links with the public, offering professionals a real “value proposition” and contributing to national cyber resilience.

Becoming a reservist

gives you the opportunity to join the military and serve your country, but also to share your knowledge, exchange ideas with other professionals and develop your expertise by contributing to innovative projects.

At the SGRS, for example, reservists have the opportunity to take courses, to take part in training such as ‘Locked Shields’, the largest full-scale cyber defence exercise organised by NATO’s Cooperative Cyber Defence Centre of Excellence (CCDCOE). By proposing concrete projects and ”continuing education” opportunities for cyber security professionals, the SGRS aims to better meet the needs of companies, professionals and Defence.

The reserve, seen from this angle, is a three-way ‘win-win’ for companies, professionals and Defence alike. It will enhance the knowledge and expertise of each party, promote the mobility of cyber security experts and foster collaboration between industry and the cyber defence community.

It is also a means of strengthening national cyber resilience. In the event of a national crisis, the Cyber Command remains an essential link, but by developing this collaboration with companies and their professionals, they will also be able to take action at their own level. The first line of cyber defence remains the users, i.e. the citizens, and raising their awareness undoubtedly contributes to the security of our nation as a whole. Developing the reserve means increasing our protection by developing a wider network, both with the professional and his or her company.

First Edition of the “Cyber Summer School” en de “Cyber Discovery Day”

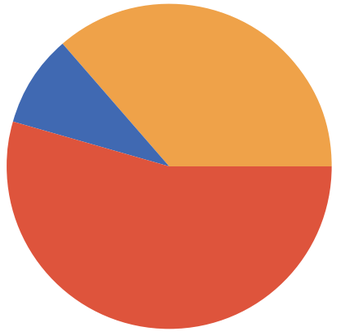
Enabling talented young people to discover the DNA of their future employer and gain a better understanding of the challenges represented by cyber defence is certainly one of the avenues to be explored to meet the challenges of the job market.

As part of this commitment to openness, the Cyber Command organised its first Cyber Summer School in the summer of 2023, followed by a “scaled-down” version, the Cyber Discovery Day. These two new initiatives invited students and young professionals to go behind the scenes of the Cyber Command and its missions in a more in-depth, human and original way.

Following an extensive selection process, around twenty candidates were chosen to take part in the Cyber Summer School programme, a summer course in a military environment. Hosted for five days at the Royal Military Academy, they had the opportunity to discover the Cyber Command’s culture and capabilities from the inside, through practical workshops and fun activities. Participants had the opportunity to carry out a forensic analysis of smartphones, dissect the hacking of a computer network and learn techniques aimed at searching for information on the dark web.

SGRS - ADIV / PART IV

Thank you so much for a wonderful week that we will not soon forget.” Judging by the reactions of the participants, this year’s event was a great success. This targeted initiative which reflects the Cyber Command’s image, has clearly attracted many new recruits, as nearly a quarter of them have already joined our ranks, either as reservists or full-time employees.



AFTER THE CYBER SUMMER SCHOOL, WOULD YOU BE INCLINED TO JOIN THE CYBER COMMAND?

MILITARY (BLUE)

CIVILIAN (RED)

RESERVE (ORANGE)

NO (GREEN)

WWW.SGRS.BE