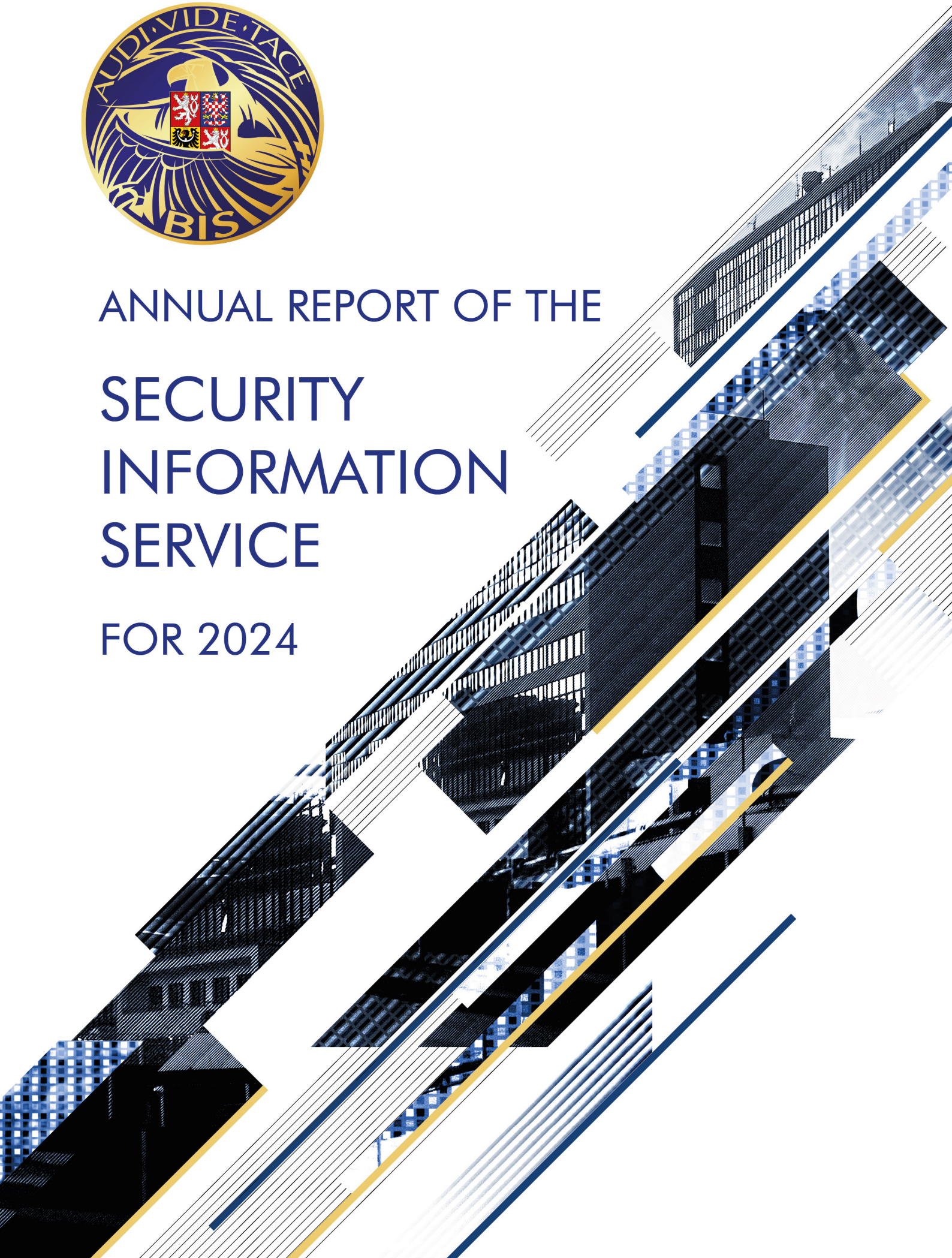
ANNUAL REPORT OF THE

SECURITY INFORMATION SERVICE

FOR 2024



Annual Report of the Security Information Service for 2024

Table of contents

Dear Readers,

Once again, after a year, you are holding in your hands the public annual report of the Security Information Service (BIS). This time we look back at the year 2024 and its events purely domestic in nature, as well as those that originated abroad but whose impact on the Czech Republic was clearly undeniable.

Last year on these pages, I expressed my hope that the unacceptable and brutal aggression of the Russian Federation against Ukraine might soon come to an end. Unfortunately, that did not happen. The ongoing conflict in Ukraine continues to have a direct impact on life in the Czech Republic. Several hundred thousand Ukrainian refugees still live on our territory, and at the same time, we must remain prepared — in case the developments take a turn for the worse — for the possible arrival of another wave of refugees.

We are also registering efforts by certain domestic companies to deliver sanctioned goods to the Russian Federation. The BIS, together with other national authorities, is working successfully to prevent this.

Direct and indirect activities of Russian intelligence services on our territory also continue. BIS has detected and helped stop several attempts at sabotage operations similar to the one that took place at the bus depot in Prague's Klíčov district.

Another area we have focused on is cyberspace and the growing efforts by actors — primarily from Russia and China (i.e. the PRC) — to attack important national institutions and test the resilience of our critical infrastructure. In parallel with this, we monitor and work against the espionage activities of certain states, the most active of which remain Russia and China.

In 2024, society continued to grapple with the spread of disinformation in the public space, originating both directly from Russia and from domestic actors. The most concerned platforms are social networks and so-called alternative media. Social networks are also closely linked to the increasingly evident trend of youth radicalization in the online environment.

The area of major economic interests of the Czech Republic also did not escape the BIS's attention in 2024, as we once again documented numerous cases of clientelism, inefficient use of public funds, and related suspicions of corrupt conduct.

The year 2024 was among the most demanding in the field of security in the modern history of the Czech Republic. Nevertheless, I dare say that as a country — and as citizens — we have excelled. The extraordinarily important support for defending Ukraine continues, the majority of society still resists the spread of disinformation, and citizens clearly express their support for our anchoring in the EU and NATO. All of this gives me hope that even in today's unsettled world, we will stand our ground and maintain our character as a democratic and free country.

Despite the general character of this report, our aim is to offer you an insight into the work of the Czech Republic's domestic intelligence service, sharing an overview of the topics and areas that the BIS has focused on and continues to address. I hope the following pages will reassure you that the BIS makes a significant contribution to ensuring that the Czech Republic remains one of the safest countries in the world.

I wish all of us safe days ahead.

genpor. Ing. Michal Koudelka

NATURE AND SCOPE OF INTELLIGENCE ACTIVITIES

The activities, status, and scope of powers of the BIS are governed by relevant laws, particularly Act No. 153/1994 Coll., on Intelligence Services of the Czech Republic, as amended, and Act No. 154/1994 Coll., on the Security Information Service, as amended. In its activities, the BIS also adheres to the Constitution of the Czech Republic, the Charter of Fundamental Rights and Freedoms, international treaties, and other legal regulations of the Czech Republic.

According to Section 2 (1) of Act No. 153/1994 Coll., intelligence services are public authorities responsible for acquiring, collecting, and evaluating information important for the protection of the constitutional order, major economic interests, security, and defense of the Czech Republic. According to Section 3 of Act No. 153/1994 Coll., the BIS is an intelligence service that, within its powers and responsibilities, as defined in Section 5 (1) of Act No. 153/1994 Coll., secures information on:

- Intentions and activities directed against the democratic foundations, sovereignty, and territorial integrity of the Czech Republic,
- Intelligence services of foreign powers,
- Activities endangering state and service secrets,
- Activities whose consequences may put at risk the security or major economic interests of the Czech Republic,
- Organized crime and terrorism.

According to Section 5 (4) of Act No. 153/1994 Coll., the BIS performs additional tasks as specified by specific legislation (e.g., Act No. 412/2005 Coll., on the Protection of Classified Information and Security Eligibility, as amended) or by international treaties binding on the Czech Republic.

Section 7 of Act No. 153/1994 Coll. further stipulates that the responsibility for the activities of Czech intelligence services and for the coordination of their operations lies with the Government. According to Section 8 (4) of this law, the government assigns tasks to the BIS within its scope of powers and responsibilities. The President of the Czech Republic is also entitled to assign tasks to the BIS within its scope of powers and with the Government's knowledge.

To fulfill its duties, the BIS is authorized to cooperate with other intelligence services of the Czech Republic. According to Section 9 of Act No. 153/1994 Coll., this cooperation is conditional upon agreements concluded between the intelligence services with the consent of the Government.

The BIS may cooperate with intelligence services of foreign powers according to Section 10 of Act No. 153/1994 Coll. only with the consent of the Government.

INTELLIGENCE INSIGHTS

Key Messages

Russia

Russia has long been attempting to undermine the stability and prosperity of European countries. It is in its interest that citizens of the Czech Republic (and the entire EU) do not trust in the institutions upon which democratic society is built.

Despite the considerable resources and efforts that Russian intelligence services invest in recruiting so-called „Telegram agents" (for the purpose of committing sabotage within the EU), this activity has led only to minor security incidents in the Czech Republic. The phenomenon has caused more media impact than actual damage.

Despite Russia's ongoing war campaign against Ukraine — and, by extension, against the EU and NATO — some Czech companies continue to seek ways to supply Russia with sanctioned goods. They most often attempt to deliver these shipments to Russian clients via member states of the Eurasian Economic Union, or via China.

European sanctions cannot prevent all re-export of sanctioned goods to Russia. Nevertheless, they are meaningful — at the very least because they raise the cost of Western goods, which must be transported to Russia covertly and via longer routes. The main supporters of Russian war production are China, Iran, and North Korea.

Radicalization

The way social media algorithms are designed has numerous negative impacts on society (such as addiction, mental health issues, radicalization, and the spread of false and distorted information). The main solution lies in educating users and raising awareness about how social media work and why they operates the way it does.

A trend of youth radicalization — especially among boys — in the online environment has been observed in the Czech Republic. The dominant cause are the increasingly refined social media algorithms that

target users with intensified content toward which they incline naturally (including radical and violent material). These are mostly individuals who are socially excluded and come from difficult family background.

Disinformation

The reach of actors and platforms spreading disinformation and conspiracy theories in the Czech environment is limited and largely stagnated in 2024, as these entities failed to find a topic which would attract a broader audience. It is in the state's interest to maintain at least a basic level of communication with the part of society affected by disinformation, in order to continuously offer them a path out of the anti-system sphere.

The spread of disinformation in the Czech Republic is predominantly driven by domestic actors, whose motivations — alongside ideological ones — are mainly financial (as it is a highly profitable business). It is crucial to distinguish between disinformation spread by domestic actors and that sponsored by foreign powers. For a foreign power, the greatest success lies in passing influenced content into the mainstream.

Economy

Representatives of certain energy companies in the Czech Republic exploit above-standard contacts and ties with public officials to gain access to internal information. They then use this information to advance their own interests, in some cases covertly coordinating their actions with other companies in the same industry sector of industry.

In certain parts of the healthcare domain, there has long been a pattern of non-transparent behavior, which creates room for inefficient use of public funds or even outright corruption.

Cybersecurity

Cyber espionage is often a much more effective method of acquiring targeted information than traditional espionage. Electronic devices are most commonly compromised remotely (e.g. through phishing attacks), but compromise via physical access is also possible. This type of attack is particularly likely during travel to high-risk countries, such as China.

China

The Chinese company Emposat, in cooperation with its Czech partner, built a ground satellite station on Czech territory, intended for communication with and data collection from satellites orbiting over Central Europe. Emposat planned to sell this data, among other things, to its foreign clients. A number of security risks were identified during the project's evaluation.

Members of Chinese intelligence services continued cultivating relationships with selected pro-China individuals on the Czech political scene. Their primary goal is to find sympathizers who would promote China's interests, weaken Czech-Taiwanese cooperation, and avoid raising the issue of human rights in China.

Terrorism

The threat level of Islamic terrorism in the Czech Republic remains low. Despite developments in the Middle East, the ideological orientation of Muslims in the Czech Republic generally remains moderate. Anti-Israeli actions have been led primarily by Czech left-wing activists, who have not been notably radical in their actions.

Migration

The migration situation in the Czech Republic remained stable in 2024. Ukrainian citizens continued integrating into Czech society. Another massive migration wave from Ukraine to the Czech Republic would only be likely if Ukrainian defense were to collapse and Russia made a significant breakthrough on the front line.

RUSSIA AS A PERSISTENT THREAT

Intelligence Activities

In 2024, Russia continued its efforts to rebuild broader espionage networks operating under diplomatic cover at the Embassy of the Russian Federation in the Czech Republic. Due to a lack of experienced operatives stationed in the Czech Republic, Russian intelligence services relied not only on their own officers but also on collaborating individuals to carry out intelligence tasks. One person residing in the Czech Republic who was proven to be cooperating with Russian intelligence services was Natallia Sudliankova (a citizen of Belarus). As a result, she was placed on the Czech national sanctions list in April 2025, with a 30-day deadline to leave the country.

Natallia Sudliankova had been granted long-term residency in the Czech Republic as an asylum seeker. She primarily engaged in journalism targeting the local Russian-speaking audience and worked in the field of public relations. Prior to 2021 — when Russian entities were excluded from the tender for the expansion of the Dukovany nuclear power plant — she had for many years been a key figure in promoting Rosatom's interests in the Czech Republic (this was a paid collaboration). She was also among the most active long-term collaborators of Russian intelligence officers operating in the Czech Republic under diplomatic cover and was involved in activities of the Immortal Regiment movement.
In 2021 and 2022, Sudliankova's activities were directed and funded by GRU officer Aleksei Shavrov. Under his instructions, she ensured the publication of several articles, mostly in the form of interviews, which focused on topics such as criticizing a Czech non-governmental organization (in 2021) or opposing aid to Ukraine (in 2022). The financial compensation for these articles — amounting to a few dozens of thousands of euros — was paid to Natallia Sudliankova in cryptocurrency via an intermediary.
In 2024, her activities focused on undermining public trust in the legitimacy of EU sanctions imposed on individuals such as Russian oligarch Alisher Usmanov, due to his support for Russia's war against Ukraine. These efforts involved publishing biased articles in the Czech Republic and several other European countries, coordinated and financed (again in the range of a few dozens of thousands of euros) by an associate of Alisher Usmanov.

A firm approach to the issue of Russian intelligence officers operating under diplomatic cover in the Czech Republic—as well as toward individuals willing to collaborate with Russian intelligence services — remains a key priority in countering hostile Russian activities on Czech territory. In this context, the BIS plays a significant role in developing a joint counterintelligence strategy with foreign partners from Schengen Area countries.

The Russian Orthodox Church of the Moscow Patriarchate remains officially present on Czech territory. It is an entity fully loyal to the Russian state, whose leader, Patriarch Kirill, is a close supporter of Russian President Vladimir Putin and of Russia's military aggression against Ukraine. This led to his inclusion on the Czech sanctions list already in 2023. In the Czech Republic, the church is represented through the Podvorie of the Patriarch of Moscow and All Rus'. Although its representatives in the Czech Republic generally avoid drawing attention with controversial statements, their loyalty to the Moscow leadership and support for Russia's official policy line is unequivocal.

Telegram agents

Over the past year, Russia continued its efforts to disrupt the unity of Western states and sow discord among the citizens of European countries. One of the main targets of Russia's subversive activities has been to weaken the cohesion among Ukraine's supporters, disrupt the supply of essential materials and equipment, and undermine political backing for the attacked country. To achieve these aims, Russia began to increasingly rely on individuals without direct ties to the Russian state, offering them financial rewards for carrying out attacks on pre-selected targets. These individuals are recruited either from organized crime groups with connections to Russia or its allied countries, or online through advertisements promising easy money for unspecified tasks. The most common platform for such online recruitment is Telegram, which led to the popularization of the term "Telegram agents."

These agents are tasked with a wide range of activities, from transporting people or packages, to photographing and filming sensitive sites — such as military bases or transfer points for military aid to Ukraine — all the way to arson attacks and endangering civilian lives. In the Czech Republic last year, this led to the arson of a bus at the Klíčov depot in Prague, carried out by a Colombian national enticed by a financial offer advertised online. Another publicly known case involved the mailing of self-igniting packages via air transport, also traced back to individuals recruited by Russian intelligence services.

It is economically vulnerable migrants from non-EU countries or from states influenced by Russia who are often targeted by recruiters. Tempted by the prospect of high financial rewards, they may be willing to engage in illegal activities. Russian intelligence services use intermediaries for recruitment, so the individual acting as a "Telegram agent" may not even be aware they are working on behalf of Russia.

The tasks assigned to Telegram agents lead not only to a primary effect — such as gathering information, delivering packages, or causing material damage — but also aim to achieve a psychological effect. This includes weakening the cohesion of Western society, instilling fear and uncertainty, undermining public trust in the state's ability to protect its citizens, and reinforcing pressure to reduce support for Ukraine in its defense against Russian aggression.

Other Subversive and Influence Activities

In the first week of September 2024, several hundred bomb threat reports targeting schools in the Czech Republic occurred simultaneously. Similar threats, including threats against schools, have also occurred in other European countries to varying extent in recent years. Investigations so far clearly indicate a connection between these threats and Russian-speaking environments. The bomb threat reports in the Czech Republic were also supported by specific information activities, such as a disinformation campaign carried out by one of the Russian media outlets.

A Russian influence operation named after the online media outlet Voice of Europe was halted in spring 2024 by placing Viktor Medvedchuk (a pro-Kremlin Ukrainian opposition politician), Artem Marchevsky, and the company Voice of Europe s.r.o. on the national sanctions list. Artem Marchevsky is a close associate of Medvedchuk and coordinated the operation from Prague. Immediately after being placed on the national sanctions list, he left the Czech Republic. Both were subsequently added to the EU sanctions list

as well. Although the Voice of Europe operation, which aimed to influence candidates in the 2024 European Parliament elections, was effectively neutralized by this action, numerous similar Russian influence activities continue across Europe.

Cyberattacks

After a temporary decrease during the initial invasion of Ukraine, the activity of Russian state and state-supported cyber actors in the Czech Republic returned to pre-war levels. In 2024, the BIS recorded activities of cyber actors linked to Russian intelligence services GRU, SVR, and FSB. The most active actor was APT28, associated with the GRU, focusing mainly on military affairs, international relations, politics, energy, and the defense, aviation, and space industries. It primarily targets EU and NATO countries as well as international organizations and has been persistently attacking the Czech Republic for many years.

The most significant APT28-related case in 2024 was the continuation of attacks from the previous year, during which the actor exploited vulnerabilities in MS Outlook to obtain login credentials in the form of NTLM hashes (digital encrypted password fingerprints) via compromised routers. This campaign, mainly aimed at EU and NATO states, targeted numerous government institutions in the Czech Republic and also exploited Czech internet infrastructure to attack other countries. In an internationally coordinated operation called Dying Ember, the Czech Military Intelligence intervened actively at the beginning of 2024, resulting in the attackers losing access to compromised devices. In May 2024, the Czech Republic and Germany, supported by NATO and the EU, publicly condemned the activities of APT28, and thus Russia.

As part of international cooperation, the BIS also contributed to the publication of a technical report, the so-called Joint Cyber Security Advisory, titled Russian Military Cyber Actors Target US and Global Critical Infrastructure, which was released in September 2024. The report described the techniques, tactics, and procedures of Ember Bear, another GRU-linked actor, in attacks on critical infrastructure in recent years.

Sanctions Evasion

Despite repeated statements by Russian officials about replacing imports of Western goods with domestic production, Russian companies struggled in many areas — including those involved in manufacturing weapon systems — to eliminate their dependence on foreign imports. Therefore, Russia's efforts to acquire sanctioned goods from the Czech Republic continued in 2024. Russia primarily sought to obtain goods subject to EU restrictive measures through re-exports via third countries. Cases under investigation involved exports from the Czech Republic to member countries of the Eurasian Economic Union or China.

Historically, Russian companies were significant buyers of Czech products. After February 2022, when Russia launched a full-scale aggression against Ukraine, many Czech manufacturers accepted the changed geopolitical situation and found buyers in other territories. However, some Czech companies continued to seek ways to deliver their goods to clients in Russia. One specific case investigated by the BIS involved a Czech manufacturer who redirected exports intended for Russia first to a member country of the Eurasian Economic Union and then to China.

In response to Russia's ongoing aggression against Ukraine, the EU further expanded the list of sanctioned goods critical to the Russian arms industry. Although the EU's restrictive measures do not have the potential to stop deliveries to Russia entirely, they increase the costs of acquiring Western goods and complicate the further expansion of Russian manufacturing capacities.

The expansion of EU restrictive measures led to an increase in workload for Czech authorities involved in licensing and approval processes. As a result, the Czech export control system struggled with insufficient personnel capacity and rising financial costs related to export controls due to the growing number of cases handled.

Russia's ability to continue its aggressive war against Ukraine largely depends on China's cooperation, from which Russia obtains a significant share of components crucial for manufacturing its weapon systems, as well as supplies from other supporters, especially Iran and North Korea.

SOCIAL NETWORKS, ALTERNATIVE MEDIA, AND THE SPREAD OF DISINFORMATION

Social Network Algorithms

For part of society, social networks have become a significant source of information about the world. However, the way they operate carries a number of risky aspects — from the large number of fake accounts to the lack of objectivity, as well as settings that strongly promote the development of addiction.

Estimated number of users in the Czech Republic (in millions)

** The estimates are based on an analysis of open sources. Social network operators do not publish exact and up-to-date user numbers by individual countries.*

There is an enormous amount of content on social networks. Individual users, however, see only a small fraction of all the posts published. This fraction is selected for each user by the social networks' algorithms (specially programmed computer calculations).

The main goal of the companies running social networks is to achieve the highest possible profit. The more time users spend on their networks, the greater the profit the network operators earn (from paid ads, sponsored posts, etc.). This is what drives the settings of the algorithms, whose primary goal is to keep each user „online" for as long as possible.

The situation when social networks, through their algorithms, provide users with content that increasingly absorbs them is known as the „rabbit hole." It occurs when a user frequently watches and engages content on a specific topic. The algorithms then gradually pull the user deeper into that topic by selecting increasingly radical content. This process can lead to the user becoming trapped in so-called information bubbles and can influence the user's perception of reality.

Social network algorithms prioritize displaying posts that attract the most attention (i.e., those that receive the most reactions and comments, no matter whether positive or negative). Therefore, they usually favor emotionally charged content — mostly funny, frightening, or violent — over "dry" facts. Therefore, the social media environment strongly facilitates the spread of false or distorted information, and it is not in the commercial interest of platform operators to effectively change these settings.

Posts that provoke strong emotions and are manipulative or target specific user groups (for a fee) can be written and spread by virtually anyone — from extremist groups to political parties, nonprofit organizations, and individuals. The greatest advantage goes to those who can use the algorithms most effectively (and even more so if they also have sufficient funding and other resources, for example allowing mass creation of fake accounts). Social networks are open to everyone, and the conditions for spreading content are the same for all. Therefore, stronger regulation of these platforms is often criticized as a restriction of freedom.

Given that the regulation of social networks is a lengthy and complex issue, it is crucial to focus attention on the users – i.e. their education and awareness of how social networks and their algorithms work. It is in the interest of every democratic society that citizens have this awareness and do not get their information or form opinions solely from content filtered for them by social networks.

The BIS monitors the Czech social media environment as part of its efforts to detect possible influence operations and attempts to sway public opinion in the Czech Republic, especially by Russian intelligence services and other actors connected to the Russian state. The monitoring also plays part in terrorism prevention.

Disinformation and Their Origin

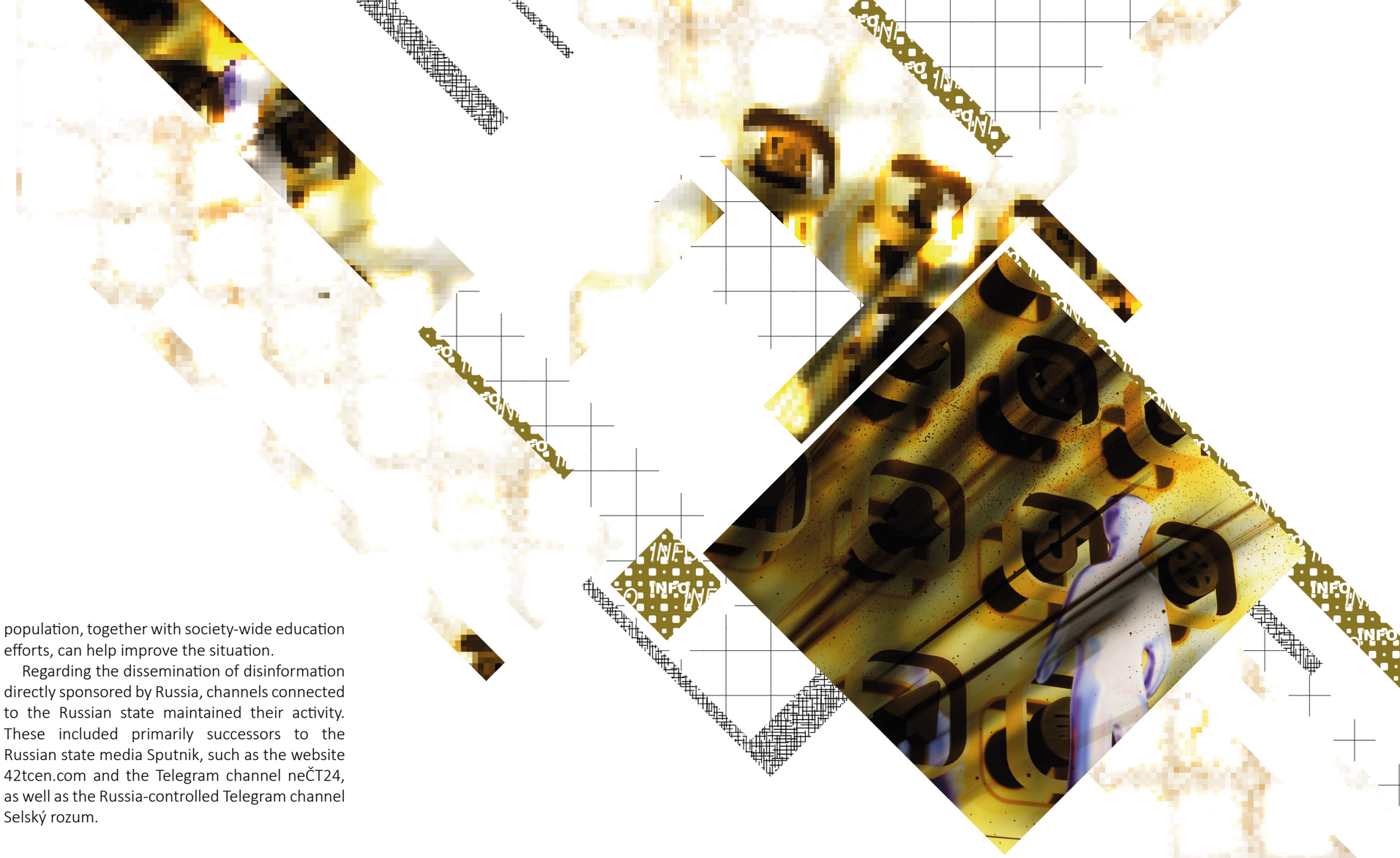
The reach of actors and platforms spreading disinformation and conspiracies in the Czech environment largely stagnated in 2024, as these entities failed to find a topic through which they could attract new groups of consumers or a broader audience. Therefore, their current influence could be interpreted as socially limited. However, a portion of society regularly consumes disinformation, which makes it vulnerable to foreign influence operations.

The spread of disinformation in the Czech environment can be seen primarily as the activity of domestic actors, whose motivations are mainly financial and/or ideological. In specific cases, the motivation is also linked to seeking media attention, which selected individuals then try to convert into political capital. From several recorded cases, there remains a persistent interest from Russia and China in using the domestic disinformation scene to promote their own interests. While China financially supported media and individuals willing to spread an exclusively positive image of China to influence how Czech citizens perceive the country, Russia focused on its long-term strategy of exploiting events in the Czech Republic to incite discontent in Czech society and also for domestic propaganda purposes.

It is crucial to distinguish between the spread of disinformation and conspiracies originating from domestic actors and the spread sponsored by a foreign power, as both require different types of responses: while the spread by an external actor must be uncompromisingly opposed using all available means, domestic sources of disinformation are regarded as a part of the political discourse by their audience, and it is in the state's interest to maintain at least basic communication channels with this part of society, thereby continuously offering it a way out of the anti-system environment. Only trustworthy communication combined with effective action to improve the living conditions of the affected population, together with society-wide education efforts, can help improve the situation.

Regarding the dissemination of disinformation directly sponsored by Russia, channels connected to the Russian state maintained their activity. These included primarily successors to the Russian state media Sputnik, such as the website 42tcen.com and the Telegram channel neČT24, as well as the Russia-controlled Telegram channel Selský rozum.

The Selský rozum channel was created shortly after the war in Ukraine began, and its activities are linked to Russian intelligence services. For example, in February 2024, the channel published an open call for gathering information about the Czech manufacturer of the Vampire rocket launchers and its employees. The Russian side has long criticized the Czech Republic for supplying weapons to Ukraine, including allegations of Czech weapons being used against Russian civilians. Russia has attempted, with limited success, to pass this narrative into the Czech media environment.



In 2024, there was a noticeable increase in the popularity of information and communication channels focused on spreading video content (platforms such as YouTube, Telegram, and TikTok) among the distributors and consumers of disinformation and conspiracies in the Czech Republic. Although Facebook remained the dominant network in this area, as in previous years, the level of risk posed by Telegram significantly increased, as it connected disinformation activities with traditional subversive operations.

Measuring the impact of information operations by foreign powers, or more generally the impact of spreading disinformation and conspiracies, remains a challenge. It is clear, however, that a foreign power considers it a success if the distorted content or narrative it promotes successfully reaches the mainstream — whether through the media, selected politicians, journalists, influencers, and so forth.

The spread of disinformation does not necessarily serve only to influence a specific segment of society, contrary to traditional views. As demonstrated in the Voice of Europe case, the production of propaganda and disinformation can also serve as a smokescreen to cover up a more serious intelligence operation. Such an operation may involve establishing contact channels with selected politicians or other persons of interest through offers of cooperation, interviews, or participation in discussions, which simultaneously provide credible cover for financial reward for their activities. In this way, a foreign power can indirectly support selected individuals or create opportunities for further intelligence activities towards them.

New Technologies

Currently and in the near future, the BIS considers the instrumentalization of artificial intelligence (AI) for spreading disinformation to be a significant risk. AI-controlled accounts (bots) are already able to behave like humans, engage in debates, respond to comments, and thereby increase the credibility of false information. Through AI, it is possible to create fake content in such volume and quality that it becomes a „weapon of mass confusion“. Some actors are already using this technology in information warfare operations, where the goal is not only to spread lies but also to cause confusion and uncertainty, relativize the truth, and weaken the public’s ability to recognize trustworthy sources, thereby undermining trust in national institutions.

Synthetic creation has become a common part of the information environment — including so-called deepfakes, i.e., fake videos and audio recordings. While in the early stages deepfakes were often entirely created using AI, over time this trend has rather declined. Instead, the creation of visual or audiovisual recordings that are then subsequently edited with AI tools has become more frequent. These AI-modified media thus originate from real material but are placed into false or distorted contexts using AI.

Especially during election periods, there is an increased occurrence of content that uses AI for manipulative editing of recordings based on a truthful foundation. Often, less sophisticated AI programs are used for these edits, producing low-quality deepfakes.

The market for automated detection tools continues to lag behind the development of synthetic media. The current most successful detection programs are noticeably better than their predecessors; however, their results are still not reliable enough to fully replace human analysis.

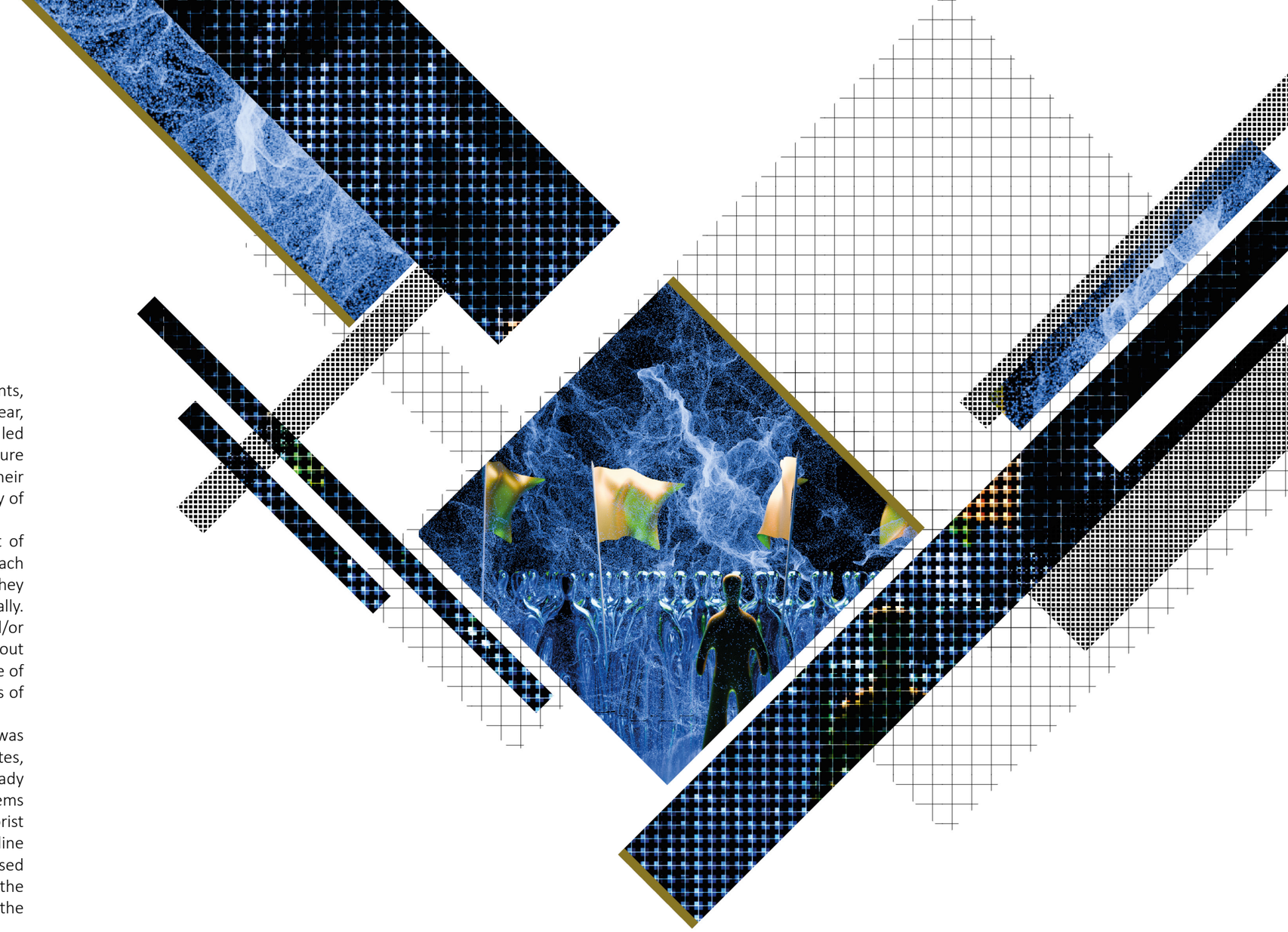
TREND OF ONLINE RADICALIZATION OF YOUTH

In 2024, the trend of radicalization among young people and adolescents, which the BIS has been observing since the autumn of the previous year, continued. This involved roughly two dozen individuals whose radicalization led them to seek and spread materials of Islamist or right-wing extremist nature online. However, the importance of ideology itself was secondary; it was their fascination with violence and the desire to be part of a broader community of like-minded individuals that played the key role.

The age of the young radicals ranged from 13 to 21 years, and most of them were Czech nationals. Except for a few cases, they connected with each other through social networks such as Telegram and TikTok, even though they came from different regions and generally did not know each other personally. They were typically adolescents with dysfunctional family backgrounds and/or ostracized individuals. Radicalization usually occurred autonomously, without direct ties to radical organizations. However, there was also a recorded case of a 21-year-old Czech citizen who was in contact via Telegram with recruiters of the so-called Islamic State (IS).

The trend of radicalization among young people and adolescents was also observed across multiple European countries. In most of these states, the phenomenon shared common characteristics, particularly the already mentioned interest in violence, association into online communities, problems within the family and/or school, and minimal connections to terrorist organizations. Unlike in the past, when most extremist acts related to online radicalization remained verbal, the recent cases indicated an increased willingness among some perpetrators to carry out actual acts of violence in the real world. The sophistication of any potential attacks remains very low for the time being, but this does not diminish the threat they pose to society.

Since May 2024, the BIS, in cooperation with the police and foreign intelligence services, has been monitoring a right-wing extremist group of minors. This group operated through a large number of social media channels and groups, with content that included aggressive right-wing extremist propaganda, strongly emphasizing violence typical of militant accelerationism and the SIEGE culture. The greatest real risk arising from its existence was a call for a terrorist attack against the Rainbow Pride event in Bratislava on July 20, 2024. Due to this threat, the police intervened against the group and launched criminal prosecution against the group's leader.



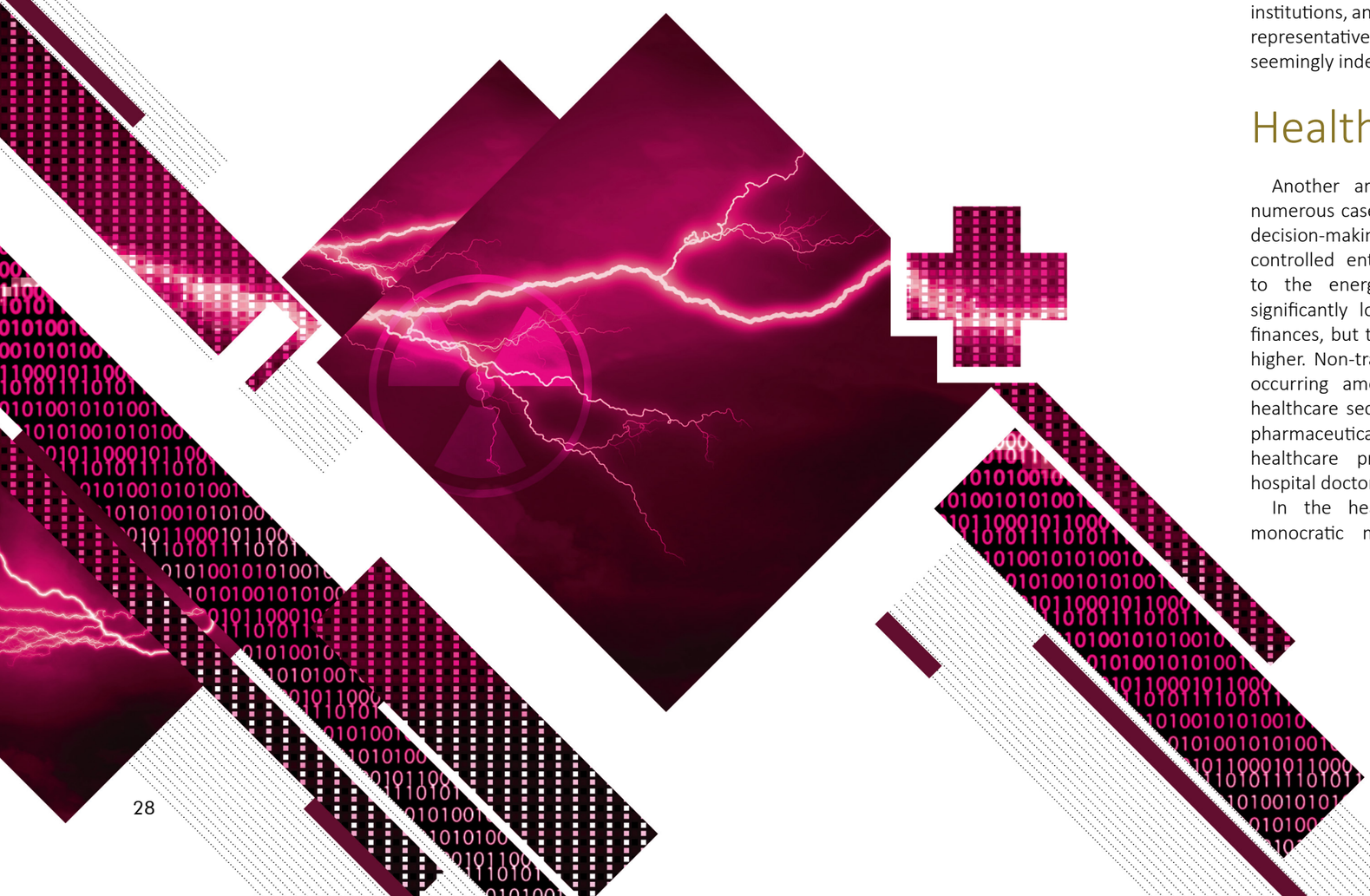
A significant cause of radicalization was social media algorithms, which increasingly directed content — even radical-themed content — to users who were inclined toward it. This factor most convincingly explains the current emergence of youth radicalization across multiple European countries. Secondary role was played by the conflicts in Ukraine and Gaza, which, in some specific cases, marked the beginning of the radicalization process. Most of the monitored individuals had not lived through these conflicts and instead sought out materials that were even a decade old, such as propaganda videos from the peak era of ISIS between 2014 and 2019.

Given that the motivation for interest in radical materials often lies on a personal level — stemming from isolation, lack of social connections, or lack of attention from others — deradicalization of these young individuals is possible. Successful examples of positive behavioral change among even very high-risk youths abroad have typically relied on a multidisciplinary approach, involving not only security agencies but also social services, schools, parents, and imams.

The public can notify the Security Information Service about individuals showing signs of suspicious behavior via the email prevence@bis.cz.

ENERGY SECURITY AND PROTECTION OF PUBLIC FINANCES

With regard to the protection of major economic interests, the main risk lays in the ability of certain private companies to advance their particular interests in relation to the state, state-controlled entities, and institutions. This phenomenon was pervasive across many sectors of the economy, with its connecting elements being clientelism and close ties between representatives of the public administration and the private sector, which in many cases represented a clear conflict of interest.



Energy Sector

As in previous years, the energy sector remained one of the main targets of private companies in 2024, for several reasons. Firstly, significant projects are ongoing or being prepared in the energy sector, not only in terms of financial volume. Secondly, it is a highly regulated area where the setting of certain parameters determines the profit margins of key players. Last but not least, substantial funds from subsidies or support funds are redistributed within this sector.

Therefore, in some cases, energy companies attempted to advance their interests based on secret mutual coordination of their actions. Representatives of energy companies also used privileged contacts and connections with public representatives, through which they obtained internal information from within national institutions, and in some cases covertly employed representatives of interest groups or other seemingly independent individuals.

Healthcare

Another area in which the BIS recorded numerous cases of clientelism or influence over decision-making by representatives of state-controlled entities was healthcare. Compared to the energy sector, these cases had a significantly lower potential impact on public finances, but their frequency of occurrence was higher. Non-transparent conduct has long been occurring among various entities within the healthcare sector (health insurance companies, pharmaceutical companies, drug distributors, healthcare providers, top hospital officials, hospital doctors, professional associations, etc.).

In the healthcare sector, the pitfalls of monocratic management of institutions or workplaces fully manifested, representing a trend that the BIS had already observed in previous years. When strong personalities hold leadership positions, their influence frequently accumulates in some cases and they exploit their influence for personal gain or to benefit another private entity closely connected to them. Examples of such behavior include interference with decision making in various departments within the institution in question, expedited processing of requests from certain entities, accommodating pharmaceutical companies, and so on. This creates significant room for inefficient use of public funds or even outright corruption. However, the motivation of representatives of public administration is not necessarily financial profit; often it involves maintaining and cultivating existing contacts and connections which are beneficial for both sides.

ICT Contracts

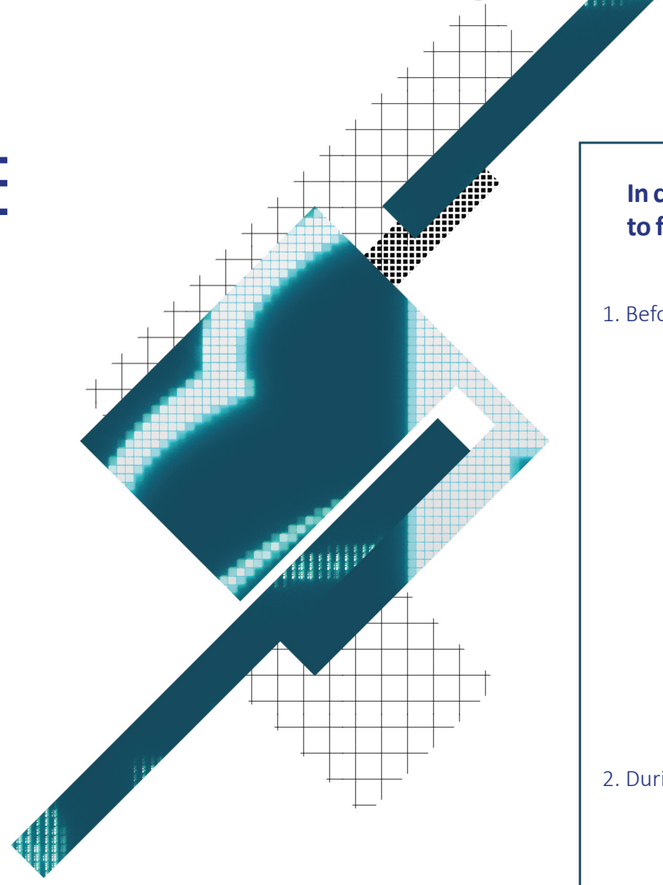
A long-standing problem for some public organizations is the unsatisfactory condition of IT infrastructure, including certain strategically important information systems or projects. The causes of this situation included, for example, several years of inactivity by the management of a specific institution, during which key decisions about the future form of the information system and the method of implementation were repeatedly delayed. In some cases, delays in implementing the necessary IT infrastructure threatened the acquisition of subsidies or created time pressure that increased the risk of choosing an inappropriate approach. In another case, the inability to prepare a contract on time led to a situation where a representative of a public organization demanded hidden participation from potential suppliers in preparing the tender documentation, which, among other things, provided the entity with a competitive advantage. These phenomena are often accompanied by insufficient or misleading information provided to responsible public representatives, who are then unable to fully exercise their supervisory functions.

CYBER ESPIONAGE

When successfully carried out, cyber espionage is a much more effective means of obtaining intelligence and exploitable information than traditional espionage. The advantages of cyber espionage include not only the quantity of potentially acquired information but also its quality and accuracy.

As in previous years, usual attempts or successful compromises of devices or networks, which typically occur remotely — for example, through exploiting vulnerabilities or phishing attacks – were detected in 2024. In addition to these cases, the BIS also dealt with gathering information from compromised devices to which an attacker was temporarily granted physical access. This type of attack usually does not occur on Czech territory but rather in high-risk countries where a Czech citizen travels and becomes the target of heightened intelligence interest. High-risk countries are generally considered to be nondemocratic states that are not members of the EU or NATO and simultaneously possess offensive cyber capabilities.

This typically involves a business visit during which the host party takes advantage of the facilities and resources on its territory and arranges or modifies the itinerary in such a way that the participants temporarily do not have access to their personal or work electronic devices (usually a laptop or phone). During this time, attackers have physical access to the device and are able to compromise it with malicious code without the owner having any suspicion. Since the implanted malware primarily serves espionage functions, the likely purpose of these activities is to gain an informational advantage for further business, diplomatic, or other negotiations.



In connection with trips (especially business trips) to high-risk countries, it is advisable to follow security guidelines that significantly reduce the risk of successful espionage:

1. Before the trip

Use exclusively work communication devices for business matters. Ensure that your device has the latest updates.

Use long passwords in the form of phrases and/or use a password manager.

Change your passwords both before and after your business trip.

Consider using a temporary mobile device that you will use only in this high-risk destination.

Enable location services on your phone only when you need them.

Install only the applications you truly need.

If possible, use multi-factor authentication (MFA).

Use a screen lock to secure your mobile devices.

Be cautious when using devices in public places: others may be watching you unnoticed.

2. During the trip

Regularly restart your phone.

Turn off Bluetooth on all your devices.

Always use your mobile data connection. Also use a VPN connection. Do not use Wi-Fi connections.

Do not download or install any applications while traveling.

Pay attention to unexpected or unusual (security) alerts on your phone, laptop, or tablet. Such notifications may indicate a cyber-attack.

If you want to make calls, use a communication app that employs standard end-to-end encryption.

Never use third-party accessories or cables with telecommunications devices. Also, do not connect your devices to other unknown devices (e.g., printers or chargers).

If you insert a USB flash drive into a third-party device, it may become infected with malware. Do not use this USB device during the trip. Bring it back to destroy or clean it.

Do not insert any third-party USB devices into your devices. Especially USB flash drives can be infected with malware. If you receive a USB flash drive that is supposed to contain relevant data, verify how you can safely transfer this data into the work network.

Never leave your devices unattended. If absolutely necessary for security reasons, leave them with, for example, a colleague who is not traveling with you. If this is not possible, turn off the device, put it in a sealed bag, and preferably store it in a safe to which you have the key.

Do not allow others to use your devices.

3. After the trip

Change the passwords for all the devices you took with you. Also change the passwords for all email accounts or social media accounts you used abroad.

OTHER IMPORTANT TOPICS OF INTELLIGENCE INTEREST

Terrorism

The level of threat from terrorism in the Czech Republic remained low throughout 2024. However, there were two unsuccessful attempts by Czech citizens to join foreign terrorist organizations in Somalia and Lebanon. These were the first such cases since 2017. A concerning trend was the above-described increase in young people and minors showing interest in radical content on the internet. No immediate threat of terrorism to Czech territory was detected.

In connection with the situation in the Middle East, the ideological orientation of Muslims in the Czech Republic remained unchanged and generally continued to be moderate. As in previous years, a few more radical expressions were noted, but these did not represent the main opinion of the community. The vast majority of these expressions took place on social media platforms.

The main factor driving radicalization during 2024 was the ongoing Palestinian-Israeli conflict, although it was not as strong a topic as in countries with large Muslim communities. With the increasing number of casualties among the families and relatives of Palestinians living in the Czech Republic, more radical reactions to the situation began to appear sporadically, but these were only isolated cases. Anti-Israel actions were primarily led by left-wing activists, while Muslims in the Czech Republic focused on providing real aid to their relatives in Gaza. Over the course of the year, the topic also moved into the academic sphere, where Czech universities were called upon to end their uncritical support of universities in Israel. However, the expressions were not as radical as those at universities abroad.

The turbulent situation in the Middle East brought many risks that needed to be continuously monitored and evaluated. Iran's policy in 2024 was significantly affected by the conflict between Israel and the Hamas and Hezbollah movements, leading to the deaths of their leaders, Israeli attacks on Iran, the deaths of some key figures of the Iranian regime, and the surprising fall of Syrian President Bashar al-Assad's regime. The situation in Europe was negatively influenced by the cooperation of the Iranian regime with local criminal networks to carry out violent attacks against "enemies of the regime" in the region. However, none of these events significantly impacted the situation within the Iranian, Lebanese, or Syrian communities in the Czech Republic nor it altered their moderate character.

Impacts of Russian aggression against Ukraine on the Czech Republic

During 2024, evacuations continued from the war front-line areas in Ukraine. There are over three million internally displaced persons in the country, more than half of whom rely on some form of humanitarian aid.

By the end of 2024, over 390,000 people with temporary protection status were residing in the Czech Republic. Another massive wave of migration from Ukraine to the Czech Republic would only be likely if Russia were to make a significant breakthrough on the front line or take control of the Ukrainian state. Currently, the migration situation in the Czech Republic is stable, and Ukrainian citizens continue to integrate into society, with their economic contribution having already exceeded the volume of financial support and social benefits they have received from the Czech government since the beginning of the war. Their presence has not had a negative impact on the crime rate in the Czech Republic.

Number of people with temporary protection status in the Czech Republic

** The data refers to the end of December of each given year.*

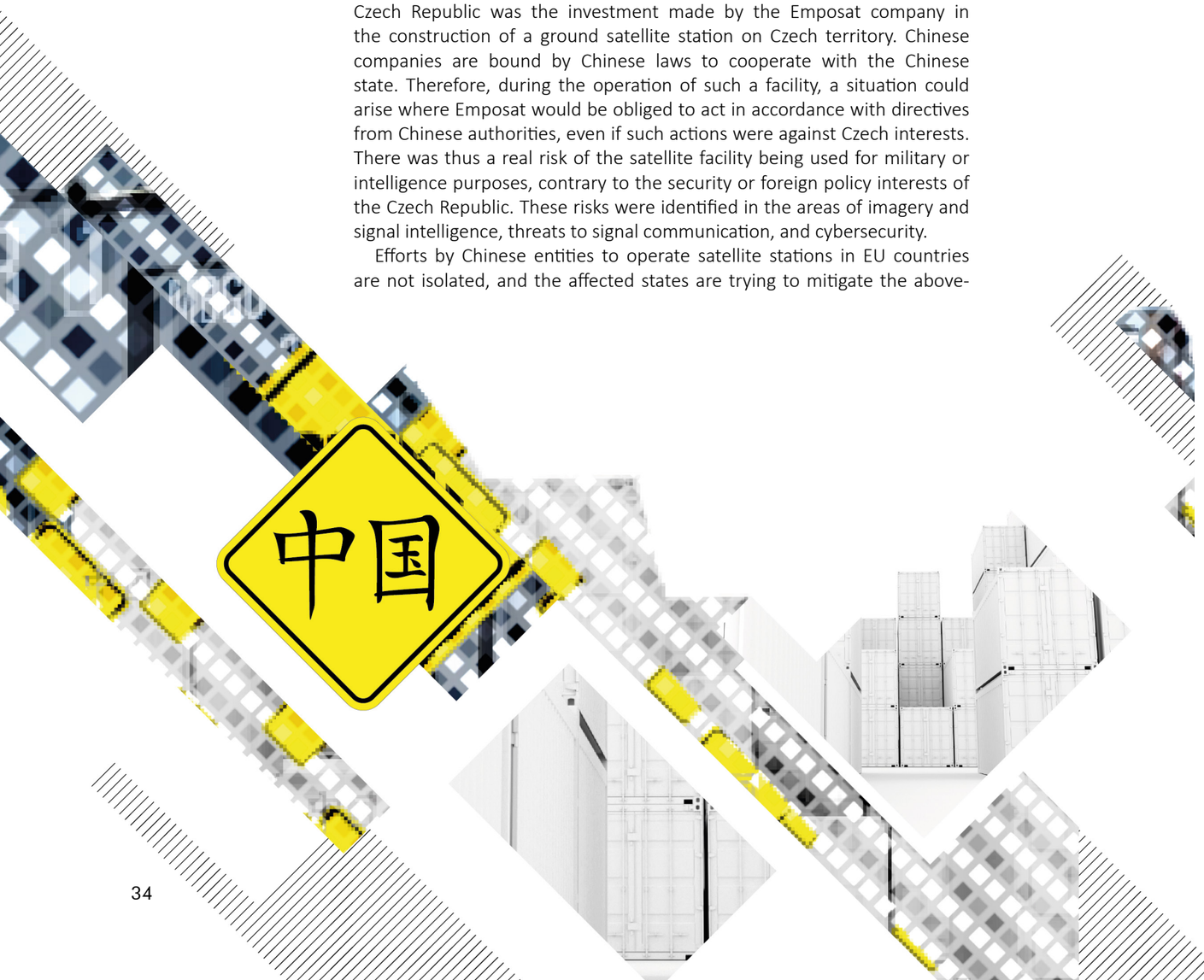
The BIS also monitors the impacts of Russian aggression against Ukraine with regard to the anticipated risk of organized crime structures being used for subversive actions planned by Russian intelligence services. So far, the involvement of members of organized crime groups or other individuals from the criminal environment in sabotage actions has not been recorded in the Czech Republic, but experiences from other EU countries and Ukraine show that this risk is relevant, as is the potential use of members of these structures for Russian influence operations aimed at the EU.

As well as in previous years, the BIS did not have information about the involvement of organized crime representatives in the illegal arms trade from Ukraine in 2024. However, with the end of the conflict, illegal arms and military material trafficking from Ukraine could become a new risk phenomenon.

Threats posed by China

An activity of significant security concern by a Chinese entity in the Czech Republic was the investment made by the Emposat company in the construction of a ground satellite station on Czech territory. Chinese companies are bound by Chinese laws to cooperate with the Chinese state. Therefore, during the operation of such a facility, a situation could arise where Emposat would be obliged to act in accordance with directives from Chinese authorities, even if such actions were against Czech interests. There was thus a real risk of the satellite facility being used for military or intelligence purposes, contrary to the security or foreign policy interests of the Czech Republic. These risks were identified in the areas of imagery and signal intelligence, threats to signal communication, and cybersecurity.

Efforts by Chinese entities to operate satellite stations in EU countries are not isolated, and the affected states are trying to mitigate the above-mentioned risks according to their legal capabilities. The described case is so far the first of its kind in several areas in the Czech Republic. The possibilities to stop such activities of security concern and limit the described threats were addressed by the BIS in cooperation with competent national authorities within their legal powers. By the end of 2024, the Emposat case had not been resolved yet, but in May 2025, the satellite station was removed following a decision by the Ministry of Industry and Trade, based on a government resolution banning the continuation of the investment in question.



The Chinese company Emposat, in cooperation with its Czech partner, commissioned a satellite antenna on a plot of land in the region of South Moravia. The antenna was intended for communication, control, and data collection from satellites over Central Europe for foreign customers. The purpose of operating the Chinese antenna was to establish communication with the Jilin satellite network. The Jilin satellite system is managed by the state-owned Chinese company Chang Guang Satellite Technology, which has been placed on the EU and US sanctions lists for providing high-resolution satellite images to the Wagner private military group operating in Ukraine.

The case met the definition of a foreign investment of security concern on Czech territory under Act No. 34/2021 Coll., on the screening of foreign investments, and the obtained findings enabled the Ministry of Industry and Trade, the law's administrator, to initiate the process of reviewing the entire investment. Based on identified security risks, the Czech Telecommunication Office did not grant permission for the use of radio frequencies for the Emposat antenna system located at the ground station.

In 2024, members of Chinese intelligence services continued to cultivate relationships with pro-China individuals in the Czech political scene. Their primary goal has been to find sympathizers in all political parties who would support the rapprochement of the two countries, promote China's interests, suppress unwanted Czech-Taiwanese cooperation, and avoid raising issues of human rights and democracy in China. The Chinese activities on Czech territory also include gathering intelligence, which is then sent to China and may be used, for example, to more precisely shape China's approach toward the Czech Republic on the international stage.

China's effort to achieve commercial and technological dominance poses a challenge to the protection of Czech companies, their know-how, and supply chains. Since the introduction of foreign investment screening into Czech legislation, China may increasingly use joint venture projects carried out on Chinese territory, which complicate the control of ownership and the use of Czech know-how. In the case of establishing a manufacturing plant in China, there is a risk of active attempts to transfer technologies supplied by the other party within joint venture projects. Even purely civilian technologies subsequently face the risk of misuse in the Chinese military industry, as China actively pursues a policy of merging the civilian and military sectors.

Regarding Chinese cyber espionage, China's intelligence services include their own (internal) cyber units. However, these represent only a part of a whole complex, systematically managed, and interconnected ecosystem that also includes other entities. A key element is that at least some private IT companies that cooperate directly with the intelligence services or other state bodies. As proven by leaked data from the Chinese company i-SOON, it is common for one company to provide services for various purposes (including military or internal security) to multiple state entities. The main strength of the entire Chinese cyber ecosystem lies in the fact that its sole purpose is to act in the interest of the Chinese government, specifically the Communist Party of China.

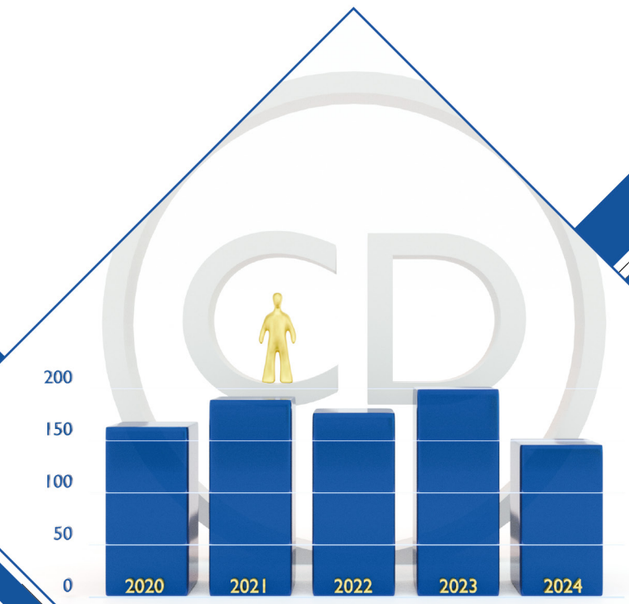
Cyber actors from private IT companies fit into the application of China's so-called whole-of-society approach, which is closely linked with the National Intelligence Law. This means that beyond intelligence services, China's diplomatic representation, the Chinese communities abroad, party organizations, and private entities (such as cyber actors) are all involved in the collection of targeted information. Cooperation among all these entities with China's intelligence agencies is enforceable under the aforementioned law.

COOPERATION AT THE NATIONAL LEVEL

Cooperation with Czech Intelligence Services

In 2024, the BIS sent more than 70 pieces of information to the, and more than 40 pieces of information to the Military Intelligence. Cooperation with both services also takes place in other operational, analytical, or support activities.

The BIS's cooperation with the Office for Foreign Relations and Information in vetting applicants for diplomatic accreditation in the Czech Republic is one of the tools to reduce the security risks arising from hostile activities by individuals working in the diplomatic services of foreign states on our territory. This cooperation continued smoothly in 2024, during which 145 diplomatic representatives, diplomatic staff members, and their family members were vetted.



Number of individuals vetted in connection with applications for diplomatic accreditation

The BIS, Military Intelligence and Office for Foreign Relations and Information also cooperated during the preparation and execution of NATO crisis management exercises and in updating the National Crisis Response System.

Cooperation with the Czech Police

In 2024, the BIS continued its cooperation with the Directorate of the Alien and Border Police in vetting applicants for short-term and long-term visas. In 2024, BIS reviewed 1,800,000 applications, which represented an increase of 100,000 compared to 2023.

An increase was recorded in the number of applications from Russian nationals. While approximately 470,000 applications from Russian nationals were reviewed in 2023, this number rose to nearly 600,000 in 2024. In most cases, these were visa applications submitted at the embassies of Schengen member states. Only around 700 applications from Russian nationals were submitted at Czech embassies, as the Czech Republic continues to enforce strict visa issuance rules toward Russia, limiting the categories of individuals who can apply for a visa. The ability to review visa applications from Russian Federation citizens submitted at embassies of other member states, combined with the restricted categories of Russian nationals who can apply for visas at Czech embassies, is a significant factor in reducing the security threat posed by the movement of Russian intelligence officers within the Schengen area.

In 2024, the BIS continued its cooperation with the Directorate of the Alien and Border Police in vetting individuals applying for a reliability certificate. The purpose of this certificate is to exclude security risks posed by individuals seeking permission to enter restricted security areas of airports. In 2024, over 20,000 individuals were vetted, which is double the number compared to 2023. The increase was likely caused by the reduction of the certificate's validity period from five to one year, resulting in more frequent vetting of applicants.

The Directorate of the Alien and Border Police is an important partner for the BIS in registering foreigners on the list of undesirable persons, which is a key tool for preventing entry of individuals who could threaten national security.

Standard cooperation and regular exchange of information also took place with other units of the Czech Police, especially the National Centre for Combating Organized Crime and the National Centre against Terrorism, Extremism, and Cybercrime.

Cooperation with Other National Authorities and Institutions

The BIS provides information and assessments to selected national authorities regarding security vetting of individuals and legal entities, either based on law or on agreements for interdepartmental cooperation. The most important recipients of this information include the National Security Authority, the Ministry of the Interior, the Ministry of Foreign Affairs, the Digital and Information Agency, and the Ministry of Industry and Trade.

Cooperation between the BIS and the National Security Authority takes place on several levels on a daily basis. In the area of security vetting, the BIS responds to the National Security Authority's requests or actively participates in security procedures related to personnel and industrial security and security eligibility by providing relevant information. The BIS also provides relevant information concerning circumstances indicating that holders of security eligibility certificates have ceased to meet the conditions for their issuance.

Intensive cooperation continues on measures related to the digitization of public administration within the interdepartmental working group

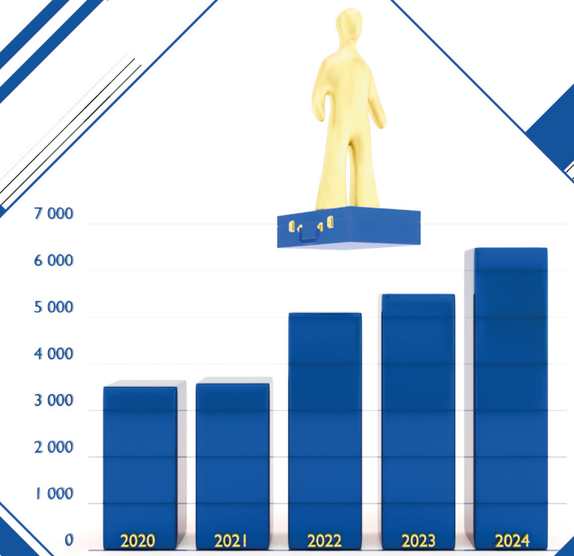
"Impacts of Public Administration Digitization on the Activities of the Security Forces of the Czech Republic," especially with the Security Department of the Ministry of Interior and other involved security agencies.

In 2024, the BIS also collaborated with the Department of Security Policy of the Ministry of Interior on vetting individuals and legal entities applying for permits to mediate employment under the Employment Act. In connection with the ongoing war conflict in Ukraine, vetting of persons applying under the Military Service Act for permission to join the Ukrainian armed forces continued in 2024 as well.

Cooperation with the Asylum and Migration Policy Department of the Ministry of Interior primarily concerns the vetting of individuals applying within the Czech Republic for the granting or extension of international protection and for residence permits. As in 2022 and 2023, the war conflict in Ukraine also influenced the structure of applicants in 2024. BIS provided opinions on 624 applicants for international protection, with the largest representation being applicants from Ukraine, followed by a significant gap by applicants from Syria, Belarus, and Russia. BIS also provided opinions on approximately 150,000 applicants for residence permits and nearly 327,000 applicants for the granting or extension of temporary protection. Compared to 2023, there was only a slight increase in temporary protection applications, indicating a continuing interest in this residence status.

As part of the MEDEVAC health and humanitarian project and the Humanitarian, Stabilization, Reconstruction, and Economic Assistance Program for Ukraine, the BIS vetted 39 individuals. In most cases, these were medical personnel participating in professional internships in the Czech Republic. In two cases, it involved escorts of a child who was to undergo treatment on Czech territory.

In 2024, BIS continued cooperating with the Ministry of Interior in vetting individuals over 15 years old applying for Czech citizenship. In 2024, the BIS provided opinions on 6,500 applicants, nearly 1,000 more than the previous year. Besides the benefits associated with obtaining citizenship of an EU member state, the current global security situation may also be a reason for the increasing number of applicants.



Number of applications for Czech citizenship
** Data include only individuals over 15 years old.*

As part of cooperation with the Digital and Information Agency, the BIS conducted security screenings of a total of 96 legal entities and 180 individuals in connection with applications for entry in the cloud computing catalog (storage of data, applications, and programs on provider servers, where user access is ensured remotely) and the repeated screening of already registered companies. In connection with the application for accreditation to manage the certified electronic identification system granted under the Electronic Identification Act, one legal entity and 14 individuals were screened.

Cooperation with the Ministry of Foreign Affairs, as in previous years, focused on eliminating security risks related to persons seeking cooperation with this ministry. The number of screened individuals did not differ significantly from the previous year, with a total of 660 individuals and 12 legal entities screened.

The BIS continued to focus on the screening of foreign investments in 2024. A total of 18 cases were initiated, with half of the screenings conducted through administrative proceedings, while the remaining cases involved an accelerated consultation process. The Ministry of Industry and Trade used the option provided by the law on the screening of foreign investments several times to initiate proceedings ex officio, that is, without the investor requesting the screening. As in previous years, the BIS evaluated and submitted to the Ministry of Industry and Trade assessments based on its own intelligence activities and monitoring of both non-public and open sources in the area of foreign investment screening.

COOPERATION AT THE INTERNATIONAL LEVEL

Cooperation with foreign intelligence services is a key factor in many areas of the BIS's activities, enabling the securing of information important for the security of the Czech Republic. With the consent of the Czech government, the BIS is authorized to cooperate with more than a hundred intelligence services from over 80 countries worldwide. The BIS develops information exchange and active contacts primarily with services from EU and NATO countries. At the multilateral level, the BIS participated in 2024 in all groups of which it is a member (e.g., the Counter-Terrorism Group and the NATO Civilian Intelligence Committee).

The main areas of cooperation between the BIS and foreign intelligence services include counterterrorism, counterintelligence and subversive activities, proliferation, cybersecurity and the protection of classified information, and security clearance matters. Within international cooperation, BIS received over 14,000 reports and forwarded more than 2,500 documents in 2024. At the strategic and expert levels, the BIS representatives attended more than 1,000 international meetings.

European intelligence services in 2024 also intensively focused on protecting the European Parliament elections to prevent interference by foreign actors, often state-sponsored. Cooperation with EU institutions continued within the framework of European initiatives and reforms.

COMPLIANCE WITH SERVICE REGULATIONS

Within the BIS, there is an Inspection Department that handles requests from law enforcement authorities or other national administration bodies and investigates reports and complaints concerning BIS employees and officers. The Inspection Department investigates cases of suspected misconduct that may constitute an administrative offense and disciplinary offenses, including the investigation of extraordinary events. Furthermore, in cases of suspected criminal offenses committed by the BIS personnel, the Inspection Department acts as a police authority pursuant to Section 12 (2f) of the Code of Criminal Procedure. In cases of suspected criminal offenses by BIS personnel, the Inspection Department is supervised both materially and territorially by the competent public prosecutor's office.

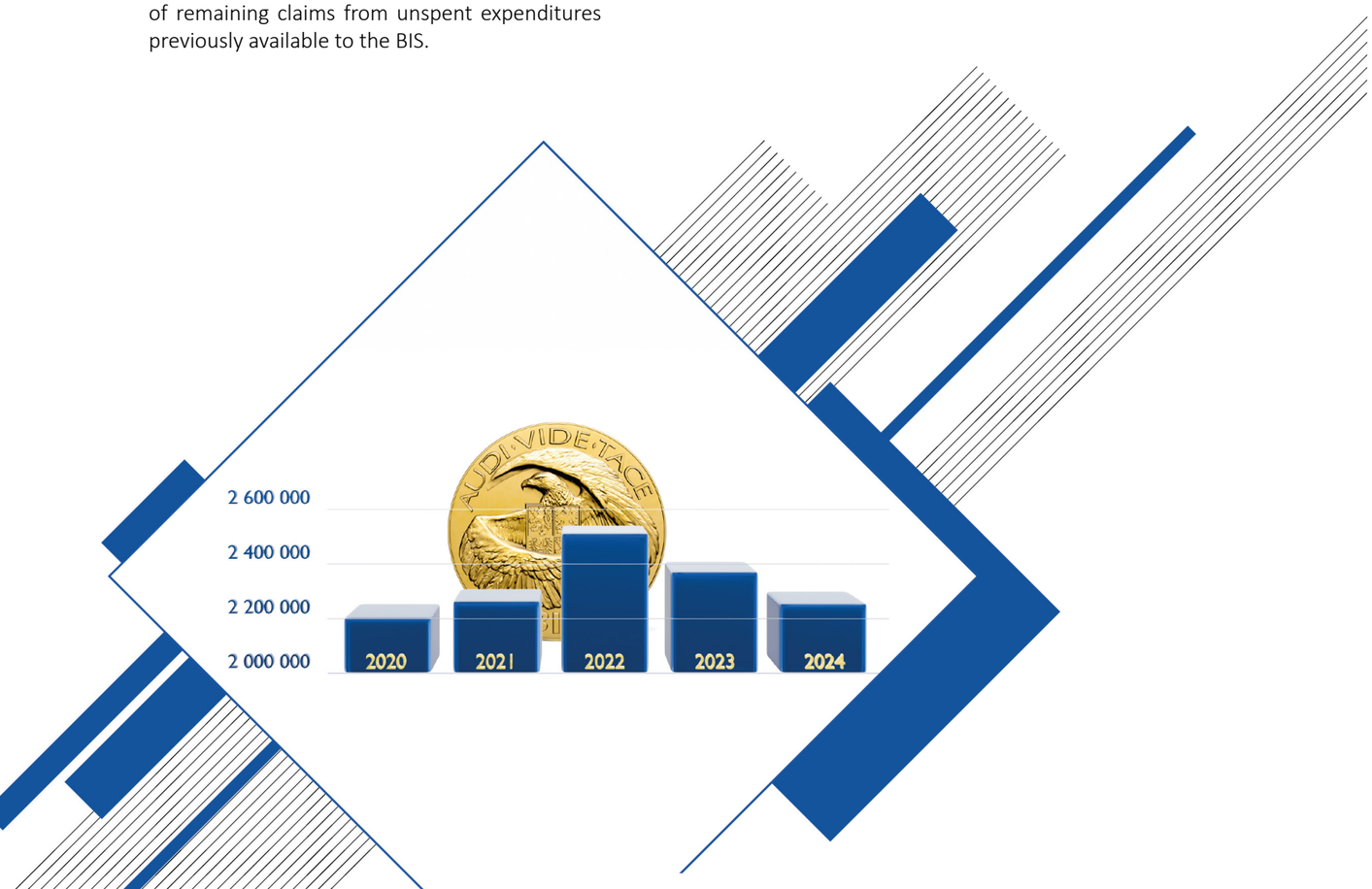
The vast majority of investigations into suspected disciplinary offenses or conduct that may constitute an administrative offense in 2024 concerned traffic matters, such as traffic accidents involving official or private vehicles, damage to service vehicles, and suspicions of other violations of the Road Traffic Act. Cases where suspicion of a disciplinary offense or administrative offense by a BIS member was found were referred for disciplinary proceedings.

Out of a total of 126 submissions, the investigations of which were completed in 2024, two were assessed as complaints regarding the conduct of BIS personnel, with one case being referred to the relevant service official for disciplinary proceedings. The content of all other submissions was examined and evaluated. Some submissions were forwarded to BIS intelligence units for further measures, while others were passed on to, for example, the competent national authorities or the Czech Police. The content of the reports from citizens reflects the overall societal situation in the Czech Republic as well as developments abroad, particularly the situation related to the war conflict in Ukraine and the Middle East.

There were no changes in the legal regulation of intelligence service oversight in 2024. However, a significant practical change is that in July 2024, the Independent Oversight Body for the Intelligence Services of the Czech Republic began its activities. This body was established in Act No. 153/1994 Coll. with effect from January 1, 2018, but had not been staffed until 2024.

BUDGET

The BIS budget for 2024 was established by Act No. 433/2023 Coll., on the State Budget of the Czech Republic for 2024. The budgeted revenues for the chapter were set at 260,000 thousand CZK and were fulfilled at 298,094 thousand CZK. The budgeted expenditures were set at 2,149,787 thousand CZK and were carried out at 2,257,172 thousand CZK, including the use of remaining claims from unspent expenditures previously available to the BIS.



BIS expenditures over the last five years (in thousands of CZK)

In the volume of current expenditure, the most significant item was personnel expenses. Besides expenses for salaries and related allowances, this also includes retirement benefits paid to former members after the termination of their service. Salary and related expenses in 2024 were negatively affected by public expenditure consolidation measures, which resulted in a 2% reduction in their budgeted amount and subsequently required strengthening from claims on unspent expenditures. Another significant category of current expenditures includes expenses for special equipment specific to intelligence service activities and special financial resources designated for direct intelligence operations.

Current expenditures also include operational expenses, primarily costs for services and commodities needed to ensure operational requirements, including contractor services for repairs and maintenance of assets managed by BIS. The amount of current expenditures was also influenced by a significant increase in spending on acquiring licenses for the use of computer programs and databases, generally related to changes in software vendors' licensing policies. Additionally, in 2024 the BIS had to cover increased expenses for energy commodities, which resulted from new contractual terms following the expiration of fixed prices in 2023 and the overall situation in the energy commodity market. Expenses for electricity rose year-on-year by 88.7%, for gas by 23%, while fuel costs were kept nearly at the 2023 level.

The main investment project in terms of strategic importance for the BIS was work on a new intelligence information system, for which steps were taken to issue a tender for a new supplier. Based on preliminary market consultations, a suitable direction for the continuation of the project was identified. In addition, a significant portion of investments was directed toward the acquisition and modernization of intelligence technology as well as information and communication technologies. Funds were also allocated for the necessary renewal of vehicles. Construction investments were reduced to an essential minimum in 2024 following the completion of the construction of the technical-administrative building.

The level of expenditures directed toward investments and the acquisition of technical equipment in 2024 can be considered a minimal maintenance level, which, however, is not sustainable in the long term given the need—or rather the necessity—to respond to changes in the environment, primarily driven by the rapid development of information and communication technologies. These changes require strengthening the capacities of the BIS, including appropriate personnel and budgetary support.

In accordance with Act No. 320/2001 Coll., on Financial Control in Public Administration and on Amendments to Certain Laws, as amended, an internal audit service is established within the BIS. In 2024, four audit assignments were completed. During the year, no serious deficiencies were identified that would adversely affect the activities of the BIS or indicate a reduced quality of the internal control system.

Annual Report of the Security Information Service for 2024

P.O.BOX 31
155 00 Prague 515
Czech Republic
Phone: 235 521 400
Fax: 235 521 715
E-mail: info@bis.cz
Data box: cx2aize