POLISH INTERNAL SECURITY AGENCY (ABW)

2024–2025

Selected actvities

TABLE OF CONTENTS

I am pleased to present to you a report summarising selected activities from the last two years of the Internal Security Agency's work. It has been a challenging period: a time of real threats, difficult decisions and intensive service in the interests of national security.

The ABW (Internal Security Agency) is Poland's largest intelligence service with the broadest scope of responsibility. We combat threats to internal security and protect the constitutional order. We identify and combat espionage, terrorism, corruption and the proliferation of weapons of mass destruction. We are responsible for the protection of classified information, the security of public administration ICT systems and critical infrastructure, as well as the field of cryptography. Our mission is the security of the Republic of Poland.

When I took over the leadership of the Agency at the end of 2023, I accepted responsibility for the effective fulfilment of this mission. I knew that the ABW must act decisively, efficiently and close to where threats arise. That is why, in July 2024, we re-established 10 ABW field offices. We are expanding our field structure with field departments and sections, particularly along the eastern border. These measures have yielded tangible results. We have increased our capacity to identify threats and respond swiftly.

The past two years have also seen increased budgetary expenditure on the Agency's development. We are investing in modern solutions, but above all in people. It is the officers and staff who form the foundation of the Internal Security Agency's effectiveness. Their experience, sense of responsibility and readiness to act are what determine our strength. That is why improving qualifications, enhancing working conditions and stemming the loss of experienced staff, as well as recruiting new officers and staff, remain among our priorities.

The most serious challenge remains subversive activity targeting Poland, inspired and organised by the Russian intelligence services. This threat was (and is) real and immediate. It requires full mobilisation. Thanks to the determination, professionalism and commitment of ABW officers, numerous acts of sabotage targeting military facilities, critical infrastructure, public utilities and sites involved in organising support for Ukraine in its fight have been prevented. Where it proved impossible to prevent acts of sabotage, the Agency successfully identified, prosecuted and secured the conviction of the perpetrators and organisers.

Combating subversive threats did not relieve the ABW of its duties relating to counter-intelligence protection against hostile intelligence activities by the Russian and Belarusian intelligence services (and their proxies). We countered terrorist and extremist threats. We protected the state's economic interests. We strengthened cyberspace security by protecting key ICT systems and monitoring the activities of hostile groups responsible for incidents in this area.

We have prepared a report covering the last two years of our work. It is of particular significance as it marks the ABW's return to publicly presenting the results of its activities. The last publication of this kind appeared in 2014. I believe that such a report is much-needed – it serves to build awareness of the Agency's tasks, strengthens trust in state institutions and, to the extent that can be disclosed, allows us to demonstrate the scale of the challenges facing the security of the Republic of Poland. I therefore regard the presentation of such reports as an important commitment and will strive to ensure that they once again become a permanent feature of the ABW's communications.

At this point, I must mention the ABW's cooperation with partner foreign intelligence services and the authorities and structures of our state, whose commitment and responsibility have contributed to the results described here. I would like to extend my special thanks to: the Chancellery of the Prime Minister, the Military Counter-Intelligence Service (SKW), the Foreign Intelligence Agency (AW), the Military Intelligence Service (SWW), the Central Anti-Corruption Bureau (CBA), the Public Prosecutor's Office, the Police, the Border Guard and the National Revenue Administration (KAS). Thank you, and I encourage you to read on.

Colonel Rafał Syrysko
Head of ABW

ABW IN A NUTSHELL

We protect Poland
from security threats

PILLARS

- COUNTERINTELLIGENCE
- COUNTERTERRORISM
- STRATEGIC ECONOMIC INTERESTS PROTECTION
- CYBERSECURITY
- CLASSIFIED INFORMATION PROTECTION

SHIELD

For state secrets

- PERSONAL SECURITY
- INDUSTRIAL SECURITY
- ICT SECURITY
- NATIONAL SECURITY AUTHORITY

HOW WE WORK

OPERATIONS
Obtaining information on persons and events

INVESTIGATIONS
Identifying crimes and prosecuting offenders

ANALYSIS AND FORECAST
Generating reports supporting government decisions

ADVISORY ROLE

- **LICENCES:** vetting of entities applying for a licence to manufacture armaments
- **SPECIAL TRADE:** monitoring the trade in arms, ammunition and military technologies
- **POLISH CARD AND MIGRATION:** assessing applications for the settlement of foreign nationals

SUPERVISION AND CONTROL

- **CIVILIAN OVERSIGHT:** operating under the supervision of the Prime Minister or the Minister-Coordinator of Special Services
- **OVERSIGHT MECHANISMS:** subject to scrutiny by the Sejm, the courts, the Public Prosecutor's Office, the Supreme Audit Office (NIK) and the Ombudsman

ABW IN A NUTSHELL

Tasks

The priority of the Internal Security Agency is to safeguard the stability of the state and ensure the integrity of the territory and the constitutional order. In an era of evolving asymmetric and hybrid threats, the Agency acts as a key bulwark protecting the sovereignty of the Republic of Poland.

The ABW's priority areas of activity include the early **detection** and **effective neutralisation of intelligence and terrorist threats**. The Agency also exercises **systematic oversight over the security** of classified information, ensuring its confidentiality in both domestic and international circulation. In response to contemporary technological and economic challenges, the ABW actively protects Polish cyberspace against attacks targeting public institutions and safeguards the country's strategic economic interests by monitoring sectors critical to the functioning of society. The full scope of its powers and a detailed list of its tasks are set out in **Article 5(1) of the Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency**.

Competences

In carrying out its statutory mission to safeguard the country's internal security, the Agency employs an integrated system of operational, procedural and analytical tools. ABW officers conduct **operational activities**, as well as **investigative** work, which are complemented by in-depth **analytical and informative** work. Another key aspect of the Agency's work is its participation in administrative and advisory procedures, as well as oversight and the performance of **control activities** within the system for the protection of state secrets.

Operational activities

Operational activities are legally authorised **measures designed to gather information about individuals, locations or events**.

The information obtained in this way is used to identify, detect and neutralise threats to national security, as well as to detect crimes and prosecute offenders in criminal proceedings.

In carrying out its tasks, the Internal Security Agency relies primarily on the assistance of citizens. The Act guarantees full protection of their identity and ensures that the details of persons cooperating with the Agency will never be disclosed.

The Agency is authorised, amongst other things, to conduct surveillance of individuals and to record video and audio in public places. In situations where other operational and investigative measures prove ineffective, and in cases of particularly serious crimes, the Agency may employ special measures such as: operational surveillance (e.g. monitoring of correspondence, wiretapping), covert acquisition or seizure of items derived from crime (controlled purchase), covert surveillance of the manufacture, movement, storage and trade of criminal goods (covertly monitored consignment).

Investigative activities

Equipped with extensive **investigative powers**, officers of the Internal Security Agency focus on identifying and combating the most serious crimes that directly threaten the stability of the state and the foundations of its constitutional order. They also prosecute the perpetrators of these crimes. In this regard, ABW officers may carry out procedural activities, which include: **detaining, searching and checking the identity of persons, using direct coercive measures and conducting body searches**, as well as **searching premises**.

Analysis and information activities

The Internal Security Agency **collects and processes information relevant to the protection of the state's internal security and its constitutional order**. It forwards this information to the President of the Republic of Poland, the Prime Minister, and also – where the information concerns matters falling within the remit of the relevant minister – to members of the Council of Ministers.

The ABW's analytical reports are based on knowledge obtained from operational reconnaissance, findings from investigations and inquiries, as well as data from publicly available sources. Their aim is to assess risks and prevent the negative consequences of phenomena and events, which translates into **supporting the decision-making processes of state authorities**.

Control activities within the classified information protection system

The tasks carried out by the Internal Security Agency under the Act of 5 August 2010 on the protection of classified information are largely preventive. Their aim is to **minimise risks in the area of state secrets protection**. The Agency focuses on establishing robust mechanisms to prevent the disclosure of classified information to unauthorised parties and, in the event of procedural breaches, on the precise identification of those responsible.

The Internal Security Agency's oversight of the classified information protection system is based on four key pillars:

- **personal security** – processes for verifying the reliability of individuals applying for access to legally protected secrets (assessment of their commitment to maintaining secrecy) and specialist training on these matters;
- **industrial security** – verification procedures for economic operators applying for an industrial security certificate;
- **physical security** – defining technical protection standards and supervising the infrastructure used for processing classified information;
- **ICT security** – device certification andaccreditation of systems processing classified data.

The Head of the ABW serves as the NATIONAL SECURITY AUTHORITY in international relations. Within the scope of these responsibilities, he is responsible for implementing harmonised standards and measures for the protection of classified information, thereby ensuring a consistent level of security for data exchanged with foreign partners, NATO and EU bodies. At the national level, the Agency supervises compliance with regulations on the protection of classified information in all civil public authorities, local government bodies and enterprises. This activity also includes the professional development of staff through training for security officers and operational responses to security breaches.

Administrative and advisory procedures

Pursuant to provisions separate from the Act on the Internal Security Agency and the Intelligence Agency, at the request of the relevant state administrative authorities and individual business entities, the **ABW participates in the implementation of over 40 types of procedures aimed at issuing opinions concerning, amongst other things**:

- granting foreigners permission to settle in Poland;
- granting licences for the manufacture of and trade in weapons and ammunition;
- issuing permits for the international trade in military equipment and armaments;
- granting the Polish Card.

Supervision and control

Supervision of the Internal Security Agency's activities is exercised by the Prime Minister or a member of the Council of Ministers appointed by him – **the Minister for the Coordination of Special Services. The College for Special Services**, operating within the Council of Ministers, also acts as an **advisory body** on matters relating to the coordination of special services in Poland. **The Agency's activities** are subject to scrutiny by, amongst others, the Sejm, the Prosecutor General, the courts, the Supreme Audit Office and the Ombudsman.

COUNTERINTELLIGENCE

The ABW's counter-intelligence unit has identified and neutralised numerous hostile operations carried out by foreign intelligence services. Only some of the information regarding our activities could be disclosed to the public. This mainly concerned instances where the results of the counter-intelligence unit's intensive work were highlighted in court proceedings.

Most of our operations – due to the classified nature of the activities carried out – were utilised in other ways. The results of counterintelligence activities included, among other, the thwarting of specific operations conducted by foreign intelligence services, including the use of administrative measures (such as entry bans, expulsion from Polish territory, refusal to grant or withdrawal of accreditation for representatives of foreign states), or the transmission of information and recommendations to the central authorities of the Republic of Poland.

The years 2024–2025 were marked by intensified and growing activity of Russian services, closely cooperating with Belarusian, as well as Chinese services.

Main areas of focus

Russian Federation

In the case of Poland, the **activities of the Russian secret services** focused on:

- **discrediting the Republic of Poland** on the international stage;
- **undermining public trust** in the state and its institutions;
- **promoting a pro-Russian narrative;**
- **fuelling** anti-establishment, anti-European and anti-NATO **sentiments;**
- **polarising and intimidating** society;
- **exploiting** historical ethnic **antagonisms**, mainly in Polish-Ukrainian relations.

The years 2024–2025 have seen a **period of intense operational activity by the Russian Federation targeting Poland** and **other EU and NATO member states**. The Russian Federation's long-term objective remains the disintegration of Euro-Atlantic structures, the isolation of selected states, and their internal socio-political and economic destabilisation.

Since 2022, Russia has been in a state of undeclared war with the Western world, and **Russian intelligence** is increasingly employing methods characteristic for special forces (**reconnaissance and sabotage**). It carries out its operations in a **planned and coordinated manner**. At the same time, Russian intelligence services are attempting to transfer to Poland the experience gained from hybrid operations carried out in Ukraine prior to 2022, using a similar modus operandi.

It should be emphasised that over the past two years, Russian intelligence has conducted large-scale activities in Poland, including preparation for acts of sabotage. The targets of Russian attacks were not only military facilities and critical infrastructure, but also large retail outlets and other public places. By escalating their activities, **Russian services accepted that fatalities would occur**. This was particularly evident in the case of projects that could have led to air or rail disasters.

Russian intelligence services are constantly adapting their methods and developing the tools used in hybrid operations. To carry out reconnaissance and sabotage missions, they recruit people looking for easy money. They recruit them, among other means, via instant messaging apps, posting advertisements offering a chance to get rich quickly in exchange for carrying out specific tasks, often seemingly unrelated to intelligence activities. Communication between clients and contractors takes place mainly online, and payments are made in cryptocurrencies.

In 2025, the ABW has launched the **@ABW_STOPdywersji_bot** on Telegram. This tool allows users to report instances of contact from foreign intelligence services, particularly offers to carry out acts of sabotage, as well as other activities, such as reconnaissance of facilities. The chatbot is available in several languages: Polish, English, Ukrainian and Russian.

Russian subversion operations are organised mainly by specialised units of the GRU and the FSB, with the GRU focusing on military-related targets, whilst the FSB on non-military critical infrastructure and civilian public facilities. Given the **comprehensive nature of Russian hybrid activities** in 2024–2025, this division was not strictly defined: in practice, both services conducted operations against military and civilian targets, depending on their operational capabilities.

Between 2024 and 2025, the ABW's counterintelligence unit observed a 'professionalisation' of Russian subversive activities. Whilst in 2023 Russian services still based their operations mainly on so-called 'one-off agents', recruited on an ad hoc basis via the internet, in subsequent years greater emphasis was placed on creating complex subversive cells, based on the tightly-knit organised crime networks. In this regard, the Russians prefer individuals with experience gained within security forces (e.g. former soldiers, militiamen, mercenaries from the Wagner Group).

Russian services have also stepped up the training within the Russian Federation aimed at professionally preparing operatives for terrorist activities (including the use of weapons and explosives). These operatives consist mainly of foreign nationals.

ABW is involved in safeguarding the presence of allied forces on the territory of Poland. In July 2024, Agency officers secured the recovery and return of components of a specialist NATO communications system that had previously been lost on European territory. The Agency cooperated on this matter with, amongst others, the NATO Security Office.

In August 2024, the largest prisoner exchange between the US and Russia since the end of the Cold War took place. Poland played a part in this allied operation. The ABW and other Polish security services were responsible, within their respective remits, for ensuring that it is proceeded smoothly. Sixteen journalists and opposition figures were released, whilst eight individuals were handed over to the Russian side, including Pavel Rubtsov, alias Pablo Gonzales Yague, a GRU officer operating in Europe under the cover of a journalist who had been detained by the ABW in 2022.

Between 2024 and 2025, the Russian Federation's services also carried out traditional intelligence operations, which were thwarted by the ABW. These operations involved recruiting sources with access to sensitive information and influencing the decision-making processes of Polish authorities. The **heightened vigilance of officers and increased public awareness of threats in Poland** effectively limited Russian intelligence services' ability to establish operational contacts with Polish citizens, forcing their rezidenturas to focus their attention on Russian-speaking and pro-Russian circles.

Russian oppositionists (the largest community of this type in Europe) remained within the sphere of interest of the Russian Federation's intelligence services, who conducted reconnaissance, influence operations and kinetic actions against this community, in cooperation with other units, prevented, amongst other things, attempts on the lives and health of identified anti-Putin activists.

In response to Russian activities, the **Polish authorities decided to close the Russian Federation's consulates-general** in: **Poznań** (November 2024), **Kraków** (June 2025) and **Gdańsk** (November 2025), which were taken in response to the acts of sabotage inspired and carried out on Polish territory by the Russian intelligence services.

Republic of Belarus

Poland remains a key operational target for the Belarusian intelligence services. In 2024–2025, the primary task of the Belarusian services was to protect the regime; consequently, their activities focused on infiltrating and undermining the numerous Belarusian opposition groups operating in Poland.

Belarusian intelligence, particularly military intelligence, cooperates closely with its Russian counterpart. The **unique symbiosis** between the services of both countries has deepened further in connection with the Russian invasion of Ukraine and the restriction of the ability to conduct operations in Poland from traditional cover positions. The Belarusian military intelligence also undertakes intensive reconnaissance activities targeting facilities of the Polish Armed Forces and allied forces, as well as critical infrastructure.

Belarusian services are conducting mass recruitment within their own country and subsequently attempting to **transfer their agents** to Poland. These operations vary in their degree of professionalism. Over the past two years, we have noted an **increase in oppressive actions taken by Belarusian officers** against Belarusian citizens targeted for recruitment (blackmail, direct coercion).

Further manifestations of hostile activity by the Belarusian services include **attempts to interrogate and recruit Polish citizens** who regularly travel to Belarus, as well as the operational **infiltration of the Polish minority** in that country.

People's Republic of China

In recent years, China has focused on economic expansion in our region, seeking even greater influence over the economy and politics. Poland is subject to pressure and lobbying from China, which is also carried out with increasing involvement from the PRC's intelligence services.

China is characterised by a deep **synergy between politics, economy, media, science and intelligence services**. This effect was also visible in the activities undertaken by Chinese intelligence, which, on the one hand, lobbied on behalf of the PRC's economic interests, including those of specific Chinese entities, whilst, on the other hand, utilising these companies to conduct intelligence operations.

As Chinese activity in Poland increases, the country's intelligence services are seeking to **create a positive image of the PRC**, using domestic media for this purpose and attempting to reach out to the Polish media.

The Chinese diaspora also remains an area of interest for Chinese intelligence. The nature of this interest is twofold: passive (monitoring potential opposition activities against the Chinese authorities) and active (using members of the diaspora for intelligence operations).

Chinese intelligence continues the large-scale, **global recruitment operations** it launched years ago, **utilising the internet** and social media platforms. Over the past two years, intelligence officers have also attempted to recruit experts, scientists, civil servants and individuals associated with security agencies, under the pretext of offering well-paid contracts.

In the context of the ongoing war in Ukraine and threats to Poland's security, particular attention should be paid to the deepening, multifaceted Sino-Russian cooperation, including collaboration in the field of information warfare, as well as the PRC's growing presence and political and economic influence in Belarus.

HIGHLIGHTS

Between 2024 and 2025, the Internal Security Agency carried out intensive operations aimed at countering hostile intelligence activities in Poland. During this period, a total of **over 60 preliminary investigations** were conducted **concerning the offence of espionage**, of which as many as 48 were initiated in 2025, demonstrating an unprecedented increase in threats and the high effectiveness of the service. In cases conducted since the outbreak of full-scale aggression against Ukraine, **91 individuals** have been designated as suspects. The Agency's procedural effectiveness has resulted in **charges** under Article 130 of the Criminal Code (**espionage**) being brought against **82 individuals**, **62 of whom have been detained**.

The ABW provided intelligence support to the highest state authorities, producing and distributing over 430 analyses and reports on current intelligence threats between 2024 and 2025

SHIELD OF POLAND

An unprecedented number of investigations and arrests

91 SUSPECTS
targeted by the measures since the start of the full-scale invasion of Ukraine

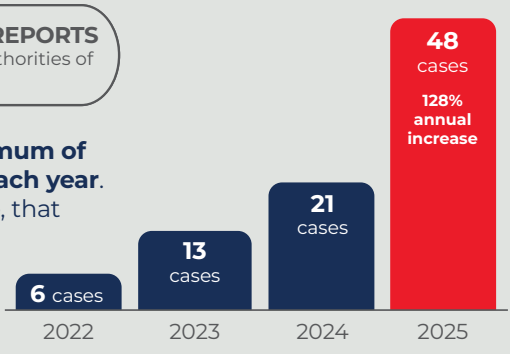
82 FACING CHARGES
of espionage (Article 130 of the Criminal Code)

62 DETENTIONS
the effective removal of agents from public spaces

430+ ANALYSES AND REPORTS
submitted to the highest authorities of the state

From the 1990s onwards, a **maximum of 5 investigations were opened each year**. Since Russia's invasion of Ukraine, that number has risen steadily

In 2024–2025, **69 investigations** were opened – as many as in the entire period from 1991 to 2023.



HIGHLIGHTS

Examples of results achieved by the ABW:

- January 2024 – **indictment** against Polish citizen Janusz N., who was active within circles of Polish and European parliamentarians, suspected of spying for Russian intelligence services
- May 2024 – **indictment** against Ukrainian citizen Oleksandr D., suspected, among other things, of inciting espionage
- May 2024 – **arrest** of Polish citizen Kamil K. and two Belarusian citizens, Stepan K. and Andrei B., who carried out arson attacks on behalf of Russian services
- June 2024 – **indictment** against two Russian citizens, Andrei G. and Alexey T., suspected of involvement in foreign intelligence activities
- November 2024 – **arrest** of Belarusian citizen Yaraslau S., suspected of attempting to set fire to a building in Gdańsk
- March 2025 – **arrest** of Ukrainian national Sergei P., who was conducting reconnaissance of military facilities in Poland
- June 2025 – **indictment** in an ABW investigation against Ukrainian citizen Kristina S., accused of planning acts of sabotage and complicity in causing a direct risk of detonation of explosive materials
- July 2025 – **arrest** of Anuar B., who, under diplomatic cover in a European country, carried out intelligence activities undermining the security of the Republic of Poland and NATO's military structures
- August 2025 – **indictment** in an investigation by the ABW against six suspects belonging to an organised criminal group involved, amongst other things, in organising and carrying out acts of sabotage on Polish territory
- September 2025 – **indictment** against Tomasz L., who is accused, among other things, of spying for Russian civilian intelligence
- October 2025 – **indictment** against Russian citizens Igor R. and Irina R., suspected of causing an immediate risk of detonation of explosive materials and of participating in the activities of foreign intelligence to the detriment of the Republic of Poland

COUNTERTERRORISM

In the area of countering terrorist threats in 2024–2025, the Internal Security Agency analysed risks arising from the war in Ukraine, the situation in the Middle East, and hybrid activities undertaken by Russia and Belarus.

In April 2024, at the request of the Head of the Internal Security Agency, a Tajik national – a member of the terrorist organisation Islamic State – was deported from Poland.

The Internal Security Agency's remit also included **monitoring the activities of terrorist organisations**, including verifying information on actions taken by supporters of such groups. In our country, many of them originate from Central Asia.

In Poland, there are four alert levels (ALFA, BRAVO, CHARLIE, DELTA) and their cyber equivalents (CRP), which are activated in the event of terrorist threats. The Head of the ABW plays a key role in this process, submitting relevant recommendations to the Prime Minister.

Since 2022, the second alert level, BRAVO, has been in force in Poland and in relation to Polish energy infrastructure located outside the borders of the Republic of Poland. Due to reported incidents of sabotage against railway infrastructure, on 19 November 2025, the third alert level, CHARLIE, was introduced for railway lines managed by PKP Polskie Linie Kolejowe S.A. and PKP Linia Hutnicza Szerokotorowa Sp. z o.o.

Main areas of focus

Islamist terrorism

In Poland, the risks associated with Islamic terrorism – compared with Western European countries – remain at a relatively low level. However, thanks to the work of the Internal Security Agency, single **cases of radicalisation linked to Islamic fundamentalism** have been **uncovered**, both among Polish citizens and foreign nationals residing in Poland.

Significant threats arose from the **illegal movement of foreigners** across the border with the Republic of Belarus and that country's **hybrid activities** linked to migration. Such activity facilitates the entry into Poland of foreigners who may pose a threat to its security. It should be emphasised that the **detected cases of illegal entry or residence in Poland largely concern citizens of countries with an elevated terrorist risk**.

In November 2025, ABW officers arrested a 19-year-old Polish national on suspicion of planning a terrorist attack in Poland

A worrying trend is the growing interest in terrorist propaganda (e.g. that of Islamic State) **among very young people**. In extreme cases, this may lead to preparations for an attack, physical assaults or attempts to construct explosive devices.

Extremism

The Internal Security Agency monitors the activities of extremist circles, anti-establishment groups and milieus that resort to violence as a mean of achieving political goals, and neutralises the associated threats.

Radical and anti-state movements

The Agency has observed a marked **increase in the activity of far-right groups**, as well as continued **activity among anti-state and anti-establishment groups**. In both cases, social media is being used for propaganda and self-promotion. The recommendation algorithms used on these platforms **encourage polarisation and the entrenchment of extreme views**. The disseminated **negative narrative** targets, amongst others, state bodies and institutions, international alliances strategic to Poland (such as the European Union or NATO), foreigners and ideological opponents, which is intended to **deepen** the **crisis of confidence in the democratic principles of state within society**.

At the same time, there is a **rise in number of incidents involving far-left environmentalist groups**. In their efforts to publicise their demands, their representatives engage in the destruction of property and the disruption of public order and the functioning of critical infrastructure, including facilities responsible for energy supply.

In November 2024, ABW officers arrested a German national who was a member of a terrorist organisation classified as a neo-Nazi right-wing extremist group.

Society polarisation

The dissemination of extremist content deepens divisions within society, making it less resilient to destabilising activities. The narrative of leaders and key activists of anti-state movements often correlates with expressions of support for the policies of the regimes of the Russian Federation and the Republic of Belarus. **Individuals' susceptibility** to such information and psychological operations (**manipulation and disinformation**) facilitates the **radicalisation of their attitudes**.

As a result, some people are beginning to place greater trust in the narrative and models of behaviour promoted by Russia and Belarus, mistakenly viewing them as a source of order, strength and security.

Youth radicalisation

According to the Internal Security Agency, the **radicalisation of minors and young adults** carries a risk of **violent behaviour**. This process is catalysed by exposure to extreme content **distributed online** – particularly via **instant messaging apps and social media platforms**, including gaming forums, which **offer users a high degree of anonymity**.

In May 2025, ABW officers arrested a 17-year-old resident of the Podkarpackie Province who was planning an attack in support of the policies of the radical jihadist organisation Islamic State (ISIS). In April and June 2025, ABW officers arrested three 19-year-olds from Olsztyn who were planning to carry out a terrorist attack, including one on a local school.

Extreme behaviour among young people is rarely driven by a specific ideology. More often, it stems from a **fascination with violence**, including mass murders and the brutal activities of terrorist organisations.

Although most radicalised individuals limit their activities to the virtual sphere, operating online, the ABW has already identified isolated cases of direct preparations being made to carry out terrorist attacks.

Critical infrastructure protection

The Internal Security Agency carries out **intensive counter-terrorism operations aimed at protecting critical infrastructure** and other areas, facilities or installations subject to mandatory protection. In carrying out these tasks, ABW formulates and issues **numerous recommendations** and **preventive guidelines**. These relate, amongst other things, to the protection of facilities forming part of the following systems:

- energy supply, energy resources and fuels,
- communications and ICT networks,
- finance, transport and healthcare.

Arms proliferation

The Internal Security Agency **conducts** ongoing and comprehensive **investigations into reports** concerning **attempts to illegally trade in weapons, their components, military equipment** and **dual-use items classified as goods of strategic importance**. A particular area of our interest remains the identification and countering any involvement of entities registered in Poland in transfers of arms and military technology to recipients in the Eastern region. These activities focus largely on detecting capital and personal links that may be used to circumvent international sanctions and to provide unauthorised support to structures associated with the political regimes in that region.

Counter-Terrorism Centre activity

Since its establishment in 2008, the Counter-Terrorism Centre (CAT ABW) has served as a fusion centre – a structure coordinating the flow of information on terrorist threats. It provides an effective platform for cooperation between Polish secret and police services, enabling not only the monitoring of threats but also a swift and effective response to them.

The Centre bases its activities on cooperation between foreign and domestic services, and above all on integrating the knowledge at their disposal. Officers, soldiers and staff of Polish agencies countering terrorist threats (the Police, Border Guard, SOP, AW, SWW, SKW, KAS, ABW) are on duty 24 hours a day, 7 days a week, verifying the information they receive on an ongoing basis. Their ability to access the databases of their respective services speeds up the process of gathering information, whilst also allowing for its immediate verification and expansion.

HIGHLIGHTS

Between 2024 and 2025, the Internal Security Agency carried out intensive activities aimed at neutralising terrorist threats and strengthening the state's resilience. In this area, it conducted a total of **19 preliminary investigations**, with the number of such activities increasing in 2025, when **7 new** cases were initiated.

A key element of the country's counter-terrorism protection was the efficient exchange of operational information – CAT ABW forwarded **nearly 700 operational reports containing indications of potential threats to entities within the counter-terrorism protection system**.

The ABW reviewed and issued opinions on approximately **5,500 applications for licences** for the international trade in goods, technologies and services of strategic importance.

The Agency drew up **over 880 opinions relating to licensing procedures** for entities operating in the field of the manufacture of explosives, weapons, ammunition, products and technologies for military or police use, as well as trade in such items.

At the same time, the Internal Security Agency served as an expert advisory body to decision-makers. Between 2024 and 2025, it prepared and distributed 178 analytical reports on terrorist threats to authorised recipients.

Examples of results achieved by the ABW:

- February 2024 – **arrest** of Russian citizen Alvi A., linked to Islamic State
- April 2024 – **sentencing** of Polish citizen Rafał K., a member of a terrorist organisation who had planned to carry out a terrorist attack, to two years' imprisonment
- July 2025 – Colombian citizen Andrés C. **charged** with committing a terrorist act in Poland
- November 2025 – **arrest** of Polish citizen Mateusz W., suspected of preparing an attack in which he planned to use explosives

HIGHLIGHTS

SHIELD OF POLAND

Active prevention and counter-terrorist protection

WE IDENTIFY

nearly **700** operational reports on potential threats forwarded to the relevant authorities and institutions

WE PROSECUTE

19 ongoing criminal proceedings relating to terrorism (including **7** initiated in 2025)

WE ALERT

178 specialist reports on terrorist threat factors have been submitted to decision-makers

WE PROTECT

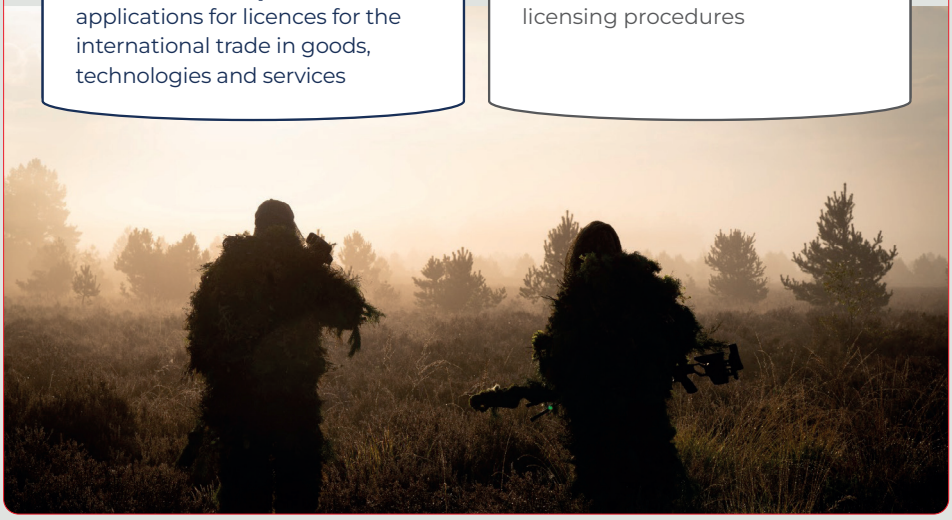
effective risk mitigation and the country's counter-terrorism defences

WE VERIFY

approximately **5,500** applications for licences for the international trade in goods, technologies and services

WE ADVISE

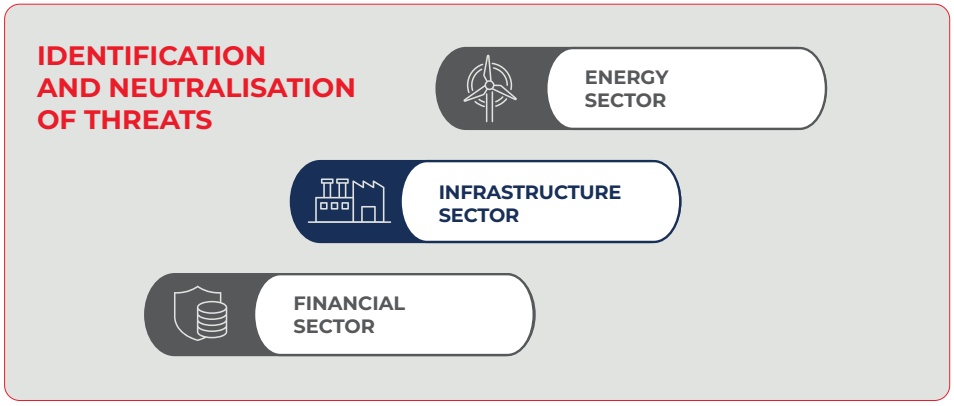
over **880** reviews relating to licensing procedures



STRATEGIC ECONOMIC INTERESTS PROTECTION

As part of its statutory duties relating to the protection of the state's economic interests, the ABW identifies and counteracts a wide range of threats. Its activities in this area focus on analysing risks arising from the geopolitical situation, which has a multifaceted impact on the Polish economy. In this area, the Agency carries out activities aimed at **identifying and neutralising threats to the functioning of key sectors of the economy**, particularly the **energy**, **infrastructure** and **financial** sectors. The assessment covers, in particular, the activities of significant entities controlled by the State Treasury, including potential irregularities in management and operational areas. The Agency also monitors the implementation of development projects of strategic importance to the interests of the Republic of Poland. This activity is conducted in a multi-faceted manner and aims to mitigate potential risks associated, amongst other things, with attempts to destabilise these projects, particularly by external actors, as well as to identify any irregularities in their implementation, including with regard to the reliability of contractors and service providers.

Main areas of focus



Strategic economic sectors

Energy sector

Between 2024 and 2025, the Agency's activities in the energy sector focused on safeguarding key projects whose implementation will significantly strengthen Poland's security. Particular attention is being paid to the **construction of Poland's first nuclear power plant** and associated investments, including the expansion of the electricity transmission network to enable its integration into the national power system. Monitoring has also covered projects related to the **expansion of LNG infrastructure in Świnoujście, the construction of offshore wind farms, the FSRU terminal in Gdańsk and other generation sources** ensuring the balance of Poland's energy system.

Between 2024 and 2025, the Agency carried out a number of procedural steps as part of investigations into irregularities at Orlen S.A. These included both measures targeting individuals and entities identified by the prosecutor, as well as actions aimed at gathering further evidence.

Infrastructure sector

In the area of infrastructure, the Agency monitored, amongst other things, the progress of investment processes, in particular the preparations for the construction of Port Polska, which is set to become a transport hub integrating aviation, rail and road transport. The ABW's activities also focused on development and restructuring projects undertaken by state-owned companies in this sector. In addition, the Agency identified attempts to involve foreign capital in Polish companies in the aviation, rail and IT sectors and mitigated the resulting risks. The ABW also assessed threats to strategic infrastructure facilities in order to ensure the stable functioning of the state, its economy and national security.

Financial sector

Another key area of the Agency's work in 2024–2025 was combating crimes that resulted in a significant reduction in budget revenue, as well as financial losses to the State Treasury. In this regard, the Internal Security Agency carried out investigations into criminal groups involved, amongst other things, in actual or fictitious trade without paying the required taxes. The Agency also focused on detecting and uncovering irregularities in the awarding of grants from targeted programmes and the management of funds received from the EU, including the identification of criminal mechanisms employed during the allocation, expenditure and settlement of funds.

The ABW carried out the tasks assigned to it by the Public Prosecutor's Office in an investigation into irregularities in the expenditure of funds from the Justice Fund. The individuals detained by officers were charged with abuse of power, dereliction of duty, misappropriation of property of significant value, and money laundering.

ABW also combats the activities of international organised criminal networks (in particular Eurasian and Russian-speaking groups) in light of the threats they pose to the state's fiscal and financial security and to other sectors of the economy. These criminal organisations constitute one of the key tools used by the Russian services to

destabilise the internal situation in Poland and the EU, including providing significant support for the Russian Federation's hybrid operations. At the same time, these groups may be used to develop and operate new ways of circumventing international sanctions and to provide channels for transferring funds to the Russian Federation.

New technologies – crypto-assets

New technologies, including those related to crypto-assets, have also posed numerous challenges for the Internal Security Agency in safeguarding the country's economic security in recent times. The dynamic growth of the virtual currency market means that these currencies no longer serve solely as modern payment and investment instruments. They now constitute an advanced tool in criminal activity that directly undermines the country's economic interests and public security. The use of crypto-assets for illegal purposes covers a wide spectrum of criminal acts, among which the transfer and laundering of proceeds from crime, fraud and large-scale extortion (fake investment platforms, pyramid schemes), corruption and the financing of terrorism are of key importance.

The Internal Security Agency has identified a scheme involving the use of blockchain technology by Russian intelligence services. This allows foreign intelligence agencies to circumvent international sanctions and provides anonymous financing for hostile sabotage operations on the territory of NATO member states. The Agency's intelligence also indicates that transactions involving these assets are being used in a scheme of controlled, illegal migration on the Belarus–Poland border.

Anti-corruption measure

Another priority for the ABW is countering threats within the framework of the so-called anti-corruption shield. Its aim is to **identify and neutralise irregularities in the implementation of projects of key importance to the security and economic interests of the state**. In accordance with the Prime Minister's Guidelines on the functioning of anti-corruption safeguards, the

Agency monitors projects in the energy sector, the fuel sector, the financial sector, and road, rail and aviation infrastructure. As part of the anti-corruption shield, the ABW analyses corruption risks, checks the credibility of individuals and entities, and monitors procedures regarding potential price-fixing or conflicts of interest.

By the **end of 2024**, **23 projects** were covered by the ABW's anti-corruption protection, whilst by the **end of 2025**, the Agency was already protecting **36 projects**.

Economic sanctions

The Internal Security Agency also plays a significant role in implementing national and international sanctions policies relating to the armed conflict in Ukraine. One of the Agency's priority tasks in this area is to identify entities that possess financial means, funds and economic resources supporting the Russian Federation's aggression, or that violate human rights or repress civil society in Russia and Belarus. Activities in this regard are carried out on the basis of the Act of 13 April 2022 on special measures to counteract support for aggression against Ukraine and to protect national security (the so-called Sanctions Act). Over the past two years, the ABW has also focused on identifying structures involved in circumventing international and national sanctions (both at sectoral and individual levels).

Between 2024 and 2025, the Agency submitted **requests** to the Minister of the Interior and Administration **to impose restrictive measures** on **further 15 business entities**.

HIGHLIGHTS

In the area of combating threats to the key economic interests of the Republic of Poland, the Internal Security Agency conducted a total of **180 investigations**, 50 of which were initiated in 2025.

Between 2024 and 2025, the **ABW vetted candidates nominated for the highest positions in the public administration and state-owned companies**. As part of these vetting procedures, **820 individuals were screened**.

Between 2024 and 2025, the Internal Security Agency (ABW) prepared and provided authorised recipients with **446 analytical reports, briefings and opinions** concerning the protection of Poland's strategic economic interests.

SHIELD OF POLAND

State personnel protections

WE PROSECUTE

a sharp increase in investigative activity in 2025 in response to contemporary economic threats

WE VERIFY

820 vetted candidates for top government posts and positions in state-owned companies

WE PROTECT

the effective elimination of personnel and operational risks in strategic sectors of the economy

WE REACT

180 preliminary investigations into cases of key economic importance (including **50** initiated in 2025)

HIGHLIGHTS

Examples of results achieved by the ABW:

- March–July 2024 – **procedural actions were carried out** at the Orlen S.A. headquarters in Płock, which enabled the gathering of evidence concerning fuel pricing and the company's emergency release of diesel and petrol stocks. The hostile actions resulted in financial losses to the company amounting to approximately **PLN 4 billion**
- October 2024 – **arrest** of five individuals in connection with irregularities in the expenditure of funds from the Justice Fund. They were charged with abuse of office, embezzlement and money laundering. The total scale of losses to the State Treasury is estimated at at least **several hundred million PLN**
- November 2024 – **arrest** of German citizen Mark A., who was charged with exporting dual-use goods to the Russian Federation
- April 2025 – joint operations by officers from the ABW, the National Revenue Administration (KAS), the Central Investigation Bureau of the Police (CBŚP) and the Central Bureau for Combating Cybercrime (CBZC) led to the **arrest** of four individuals – members of an organised criminal group involved in VAT fraud, resulting in losses to the State Treasury estimated at over **PLN 38 million**
- June 2025 – **arrest** of Michał R., a former member of the management board of Orlen S.A. responsible for supervising Orlen Trading Switzerland GmbH, based in Switzerland, in connection with acting to the detriment of the company in order to gain financial advantage through improper supervision of funds transferred to OTS and the conclusion of contracts for the supply of crude oil. Investigators estimate the loss at approximately **PLN 1.5 billion**
- June 2025 – **arrest** of two Polish citizens, Marek D.T. and Magdalena D.T., wanted under a European Arrest Warrant in connection with causing damage to the property of PGE GiEK S.A. amounting to nearly **PLN 21 million**
- September 2025 – joint operations by the ABW and the CBŚP led to the **arrest** of the leaders of an international organised crime group, Marek M., alias 'Oczko', Daniel S. and Marcin K. The group was involved, amongst other things, in smuggling of drugs from Western Europe to Poland and illegal manufacture and distribution of tobacco products in Poland. The losses to the State Treasury were estimated at no less than **PLN 9 million**
- December 2025 – an **indictment** was brought against, amongst others, Joanna S., the creator of a pyramid scheme representing Galleri New Form. The charges relate to inducing victims to dispose of their assets to their detriment, amounting to a total of no less than **PLN 300 million**

POLISH CYBERSPACE PROTECTION

The Internal Security Agency is carrying out **intensive operational and technical activities aimed at neutralising cyber threats to the Republic of Poland**. These initiatives form the basis for safeguarding the public administration's ICT systems, ensuring the integrity of electoral processes, and protecting other entities that are critical to the continuity of the state's functioning.

The **Computer Security Incident Response Team (CSIRT GOV)**, which operates within the Internal Security Agency, remains a key component of the national cybersecurity system. At national level, it is responsible for coordinating security measures for public administration bodies and operators of critical infrastructure.

The team's statutory remit includes **identifying threats, responding to cyber-attacks**, providing expert **support to organisations** in managing incidents, and **implementing** multi-layered **preventive and protective measures**.

Security of Polish cyberspace

The Internal Security Agency has noted an **increased threat level in Polish cyberspace**, which is directly reflected in the maintenance of heightened **CRP alert levels** across the entire country. Poland – due to its strategic location and its status as a member of NATO and the European Union – is one of the key targets for cyber-offensive groups linked to foreign government centres (so-called state-sponsored groups), as well as cybercriminal groups and hacktivist organisations. Nowadays, **cyberattacks** have lost their incidental nature, becoming an integral **part** of multidimensional **hybrid operations**. Their aim is not merely **data theft**. Increasingly, they are directed towards carrying out aggressive **disinformation campaigns** and **destabilising state** structures and decision-making processes.

A classic example of hybrid operations was the takeover of an employee's account at the Polish Press Agency in May 2024. This incident was used by external actors to publish a fake news report claiming that a mobilisation had been announced in Poland. The authors of the fake report specified that specific occupational groups would be subject to conscription, including miners and drivers with C and D licences.

Disinformation

Disinformation campaigns carried out by state and non-state actors **represent one of the greatest challenges to internal security**, particularly in the context of Russian hybrid operations. Nowadays, **virtually every socially sensitive topic** or event immediately becomes the **target** of so-called internet trolls and bots, which spread

false narratives. These activities are primarily aimed at **increasing polarisation within society** and **undermining Polish citizens' trust in state institutions and international bodies**.

Hostile disinformation campaigns are increasingly supported by the **activities of cyber-offensive groups**.

Social engineering campaigns

Social engineering campaigns remain one of the most common and effective tools in a cybercriminal's arsenal. It is worth noting that they are taking on increasingly sophisticated forms. Attackers are constantly developing and modifying classic phishing methods. Alongside traditional emails containing **dangerous links, malicious QR codes** are being used with increasing frequency. To effectively bypass recipients' vigilance, attackers impersonate trusted commercial entities and government institutions. A particularly dangerous phenomenon is the use of **compromised email accounts** belonging to central and local government bodies, as well as the **branding of companies, organisations and public institutions** for this purpose. Such activities are designed to create a false sense of security among recipients.

From a technical analysis perspective, a significant challenge for security systems is the change in the method of malware distribution. Perpetrators are migrating their resources (fake forms, infected documents) en masse to legitimate public cloud services. This approach allows them to conceal traffic within trusted domains, which drastically reduces the effectiveness of standard blocking rules and early warning systems.

QR phishing

The threat known as **quishing** (QR phishing) capitalises on the popularity and growing prevalence of QR codes, as well as the trust that users place in this technology. From a cybersecurity perspective, a key feature of QR phishing is its ability to **conceal a malicious hyperlink** from automated security systems that scan message content. This allows attackers to successfully deliver malicious payloads by bypassing security mechanisms. The distribution of malicious QR codes takes place in two ways:

- **in the digital domain** – messages most often reach victims through mass or targeted distribution via instant messaging apps and social media platforms;
- **in urban areas** – by physically affixing fake QR codes in public places, on legitimate urban infrastructure (e.g. parking meters, ticket machines).

This hybrid approach drastically increases the likelihood of lulling the victim into a false sense of security.

Attacks on infrastructure

The Internal Security Agency has noted a steady **increase in the number of cyberattacks targeting supply chains, critical infrastructure facilities and industrial control systems for municipal infrastructure** (including sewage treatment plants, water treatment plants and waste incinerators). By targeting contractors, cybercriminals seek to obtain data on contracts, project documentation and authentication credentials enabling access to end-customer systems. The resources obtained in this way are used, directly or indirectly, to build a knowledge base on the architecture and functioning of key facilities within the country.

Activity targeting municipal infrastructure was particularly intense among hacktivist groups. In attempting to interfere with the operation of such facilities, they exploited glaring vulnerabilities in the form of poor password policies and unsecured device management panels, accessible directly via the public internet.

In 2025, security breaches were reported at **water treatment plants** in the following towns: Jabłonna Lacka, Szczytno, Małdyty, Tolkmicko and Sierakowo. By gaining access, in some cases, to industrial control systems, the attackers were able to **alter the technical parameters of the equipment**, which posed a direct risk to the continuity of their operation and, consequently, to the supply of water to the population.

APT Groups

Alongside the observed increase in the overall number of cyberattacks, the Internal Security Agency has noted a systematic rise in the sophistication of operations carried out by **APT** (Advanced Persistent Threat) groups. These are highly specialised actors, sponsored by hostile governments, who carry out sophisticated, long-term espionage and sabotage operations. Among the most active groups in the field of cyber attacks, we can indicate, Russian APT28 (Fancy Bear), APT29 (Midnight Blizzard) and the group UNC1151, linked to the Belarusian state apparatus. These are teams of specialists acting on behalf of state entities (primarily Eastern intelligence services), whose primary objective remains the **acquisition of strategic intelligence, cyber espionage, the conduct of influence operations, and the execution of multi-domain disinformation campaigns**.

In August 2024, the Polish Anti-Doping Agency (POLADA) fell victim to a serious cyberattack, as a result of which sensitive data—including medical records and the results of anti-doping tests carried out on Polish athletes—was stolen and published online.

Hackers are constantly refining and modifying their attack methods, aiming to exfiltrate data by bypassing the detection and defence mechanisms deployed on the victim's devices (such as antivirus systems). In doing so, they most often exploit vulnerabilities and weaknesses in the software and hardware used.

ARAKIS GOV early warning system

An analysis of data from ARAKIS GOV (Poland's operational early warning system for online threats), carried out by the ABW, shows that the **years 2024–2025** were marked by an unprecedented **intensification of defensive activities in Poland's cyberspace**.

Attackers not only employ technologically advanced tools, but above all **target directly the weakest link in security systems– the human factor (users)**. In the face of such a dynamic evolution of threats, the implementation and application of a multi-layered cybersecurity strategy has become a key issue for the protection of Polish cyberspace. This encompasses both permanent monitoring of infrastructure, regular audit procedures, as well as systematic user education.

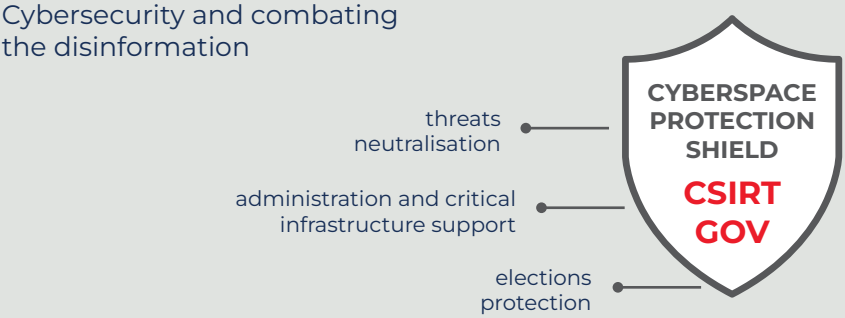
During the period in question, the Agency identified **increased activity in cyberspace** by foreign intelligence services, with particular emphasis on Russian **services**.

The scale of these activities is reflected in the statistics of the CSIRT GOV team led by the Head of the Internal Security Agency, which recorded **over 40,000 reports** of potential ICT incidents. Furthermore, in 2025, the ARAKIS GOV system recorded an **18 per cent year-on-year increase in the number of incidents**, resulting in a record number of **over 5.5 million security alerts**.

ARAKIS GOV is an early warning system for online threats, developed to support the protection of ICT resources belonging to government bodies and critical infrastructure operators. The system aggregates and processes data indicative of a potential attack or malicious network traffic, correlating it with existing data to identify indicators such as unique IP addresses, ports, timestamps, and threat types and methodologies.

SHIELD OF POLAND

Cybersecurity and combating the disinformation



THREATS
ARCHITECTURE

DISINFORMATION CAMPAIGNS

The spread of false narratives
Objective: to polarise opinion and undermine trust in institutions

SOCIAL ENGINEERING CAMPAIGNS

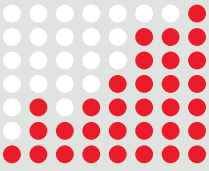
The use of phishing and quishing
Objective: to obtain confidential information

ATTACKS ON WATER TREATMENT PLANTS

Objective: to disrupt the day-to-day functioning of the state and create a sense of instability

APT GROUPS

Targeted attacks by state-sponsored groups (APT28, APT29, UNC1151)
Objective: espionage and data exfiltration



ALERT!!!

The CRP alert level remains elevated:

- **over 40,000** reports of potential incidents
- **an 18% increase** in the number of incidents (year-on-year)
- a record number of **over 5.5 million alerts**

CLASSIFIED INFORMATION PROTECTION

The Internal Security Agency **oversees the operation of the classified information protection system**. The effectiveness and integrity of this mechanism depend on close synergy between organisational, technical and legal measures. Efficient coordination of activities between the specialist institutions responsible for national security also remains a key pillar of its stability. The Internal Security Agency's activities in this area include not only monitoring compliance with procedures for accessing legally protected secrets, but also the certification of ICT systems and audits of businesses applying for industrial security certificates.

The Internal Security Agency has initiated works on amending the Act on the Protection of Classified Information to include provisions relating to states of emergency, in particular during armed conflict. The aim of the amendment is to introduce provisions ensuring effective operation in the event of a threat of war.

In any information system, **the human factor remains the weakest link**. Breaches of regulations may result

both from **deliberate actions**, such as **espionage** or **sabotage**, and from **unintentional errors**, which are often the result of routine, lack of awareness of the risks, or external pressure. Furthermore, the **rapid pace of digitalisation**, which enables the processing of classified information in systems that are frequently targeted by cyberattacks, can lead to the unauthorised acquisition, modification or disclosure of information of critical importance to national security.

The case of former judge Tomasz Szmydt, suspected of espionage, who fled to Belarus in May 2024 and was granted political asylum there, prompted the ABW to begin work on amending the regulations governing access to classified information for judges and prosecutors performing duties involving access to such information. The proposed amendments received the support of the College for Special Services, which operates under the Prime Minister.

Between 2024 and 2025, the Internal Security Agency issued nearly **23,000 security clearances** as part of its statutory vetting procedures. These documents grant access to classified information at the national level and to the secrets of international organisations. Strict criteria for assessing the ability to maintain confidentiality meant that, during the same period, nearly **200 people** were refused clearance, and over **100 people** had their previously granted clearance revoked.

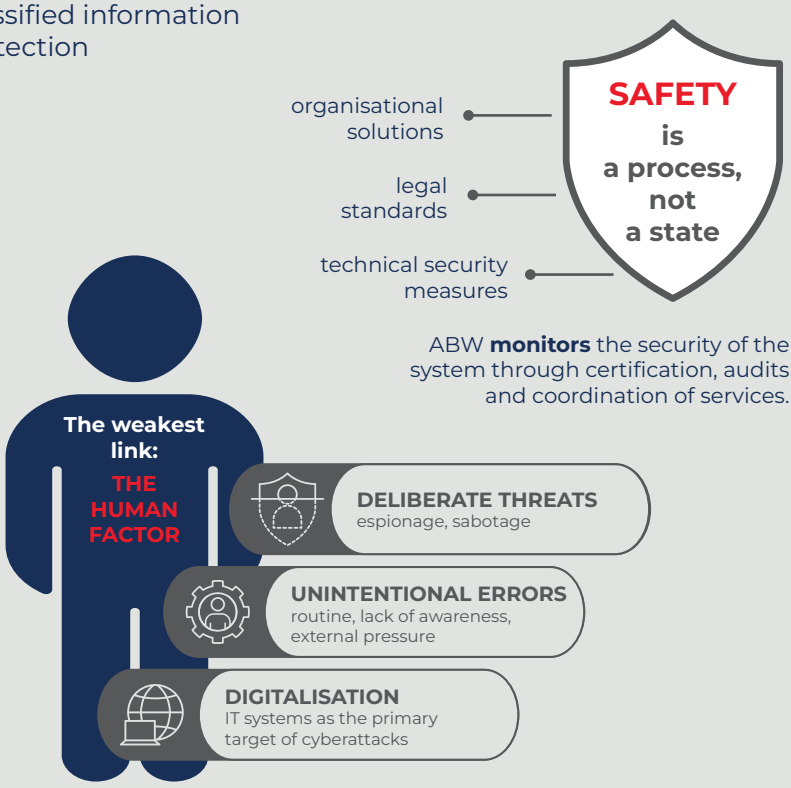
In carrying out its duties relating to the protection of classified information in the economic sphere, the Internal Security Agency has issued over **550 industrial security certificates**. These documents confirm the ability of businesses to ensure the required standards of protection for classified information. As a result of rigorous verification procedures during the same period, **8 entities were refused** such a certificate, and **6 businesses** received a decision revoking previously granted authorisations in this regard. In the years indicated above, businesses holding approximately 2,200 industrial security certificates remained within the scope of the Internal Security Agency's remit and oversight regarding the protection of classified information.

The Internal Security Agency also carries out statutory tasks in the field of information and communications technology security. Consequently, **over 1,000 accreditation certificates** were issued during the period in question for systems designed to process classified information. These procedures were designed to confirm that the environments under review meet stringent criteria for cryptographic, electromagnetic and physical protection, thereby guaranteeing the integrity and confidentiality of state data.

As part of its statutory supervision of the classified information protection system, the ABW initiated a total of **nearly 80 inspections** in public institutions and commercial entities. The vast majority of these, over 70, were **planned system audits**. At the same time, in response to identified risks and reports of potential breaches, the Agency initiated **four ad hoc inspection procedures**.

SHIELD OF POLAND

Classified information protection



ABW **monitors** the security of the system through certification, audits and coordination of services.

STATISTICS

PERSONAL SECURITY

- **23,000** security clearances issued
- nearly **200** refusals to issue clearances
- over **100** revocations of clearances

INDUSTRIAL SECURITY

- over **550** certificates for businesses
- **8** refusals to issue certificates
- **6** revoked certificates

ICT SYSTEMS

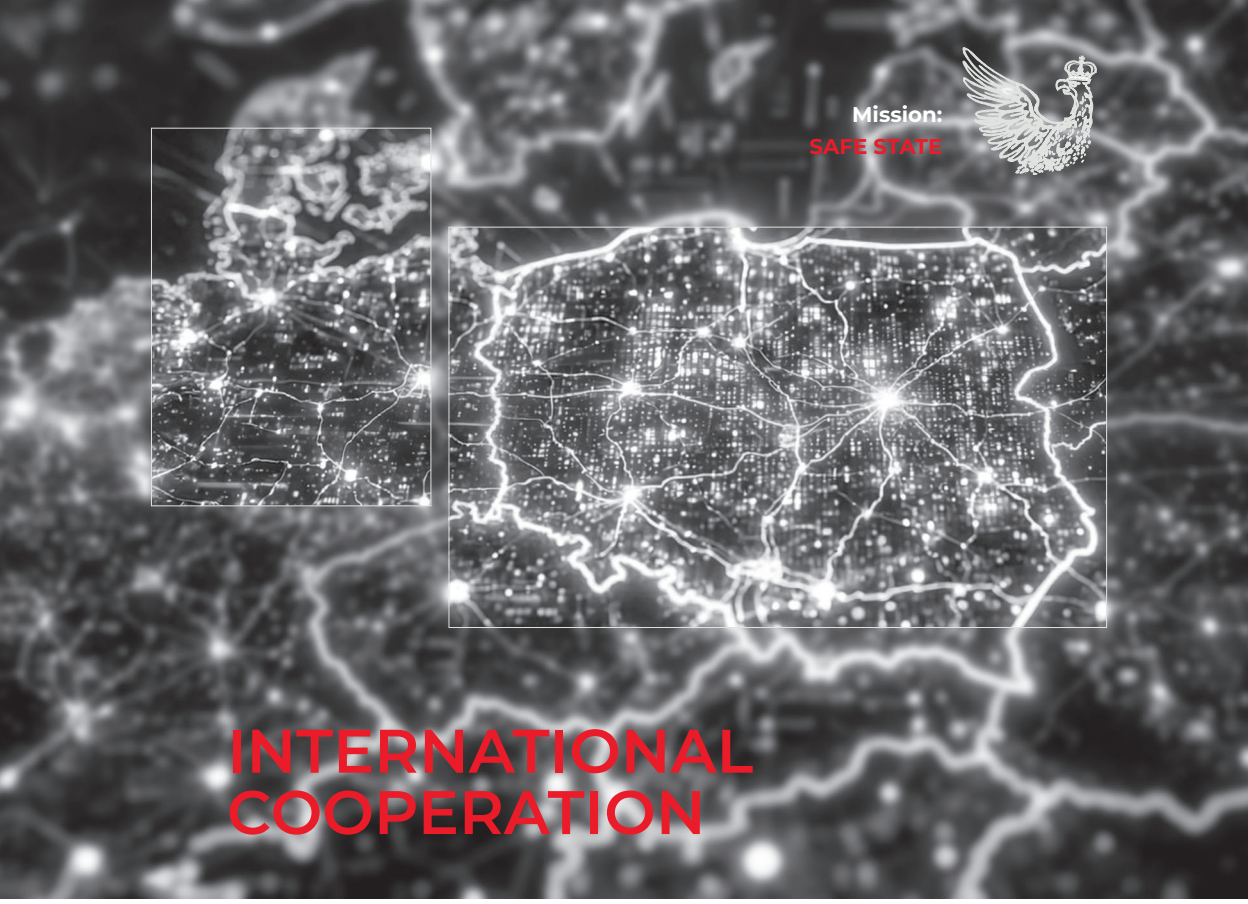
- over **1 tys.** accreditation certificates issued for ICT systems
- **3** pillars of protection

IT SYSTEM SECURITY INSPECTIONS

80 inspections carried out

Over **70** system audits (scheduled and preventive measures)

4 ad hoc inspections (rapid response to identified risks and errors)



INTERNATIONAL COOPERATION

The Internal Security Agency engages in **extensive international cooperation**. This encompasses partners from around the world, with relations with European countries and transatlantic allies – particularly NATO, the EU and Ukraine – being of key importance.

This cooperation enables joint **threat analysis and the exchange of information and experience**, strengthens the effectiveness of the ABW's operations and contributes to enhancing Poland's security.

The ABW's list of foreign partners includes, in particular:

- **foreign intelligence services** (counterintelligence and intelligence);
- **security and law enforcement agencies** of other countries;
- **diplomatic missions** accredited in Poland;
- international **organisations and institutions**;
- **forums for cooperation** between intelligence services.

The Internal Security Agency maintains ongoing relations with **nearly 100 entities from over 50 countries**. Key areas of cooperation focus on **countering foreign intelligence activities, combating terrorism, protecting Poland's strategic economic interests**, monitoring **uncontrolled migration** and addressing **cyber threats**.

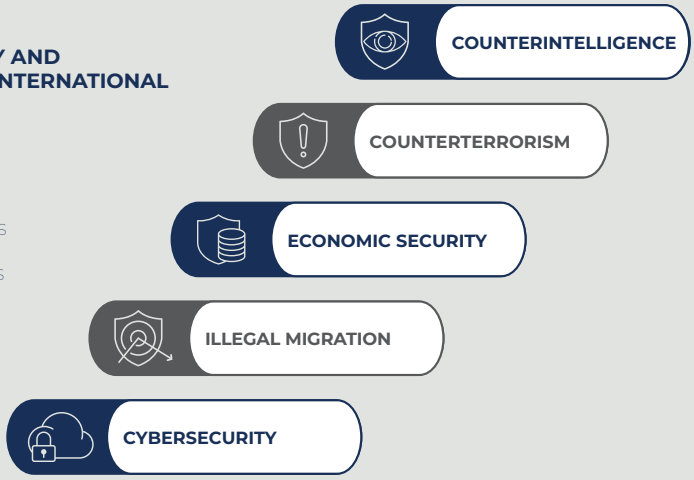
The intensity of this cooperation is reflected in the statistics. Between 2024 and 2025, ABW representatives took part in **over 3,000** expert meetings at home and abroad. During the same period, as part of its cooperation with foreign partner services and international organisations, the Agency exchanged **over 76,000 pieces of information**.

The systematic increase in the pace and scope of international cooperation observed over the past few years is a direct response to the evolution of global threats.

THREAT IDENTIFICATION AND NEUTRALISATION

THE GEOGRAPHY AND SUBSTANCE OF INTERNATIONAL COOPERATION

- **50** countries
- **100** agencies and institutions
- **5** priority pillars



THE DYNAMICS OF INFORMATION EXCHANGE AND EXPERT ACTIVITY

- knowledge sharing: **3,000** expert panels and working meetings
- data exchange: **76,000** data points

OPERATIONAL AND TECHNICAL ACTIVITIES

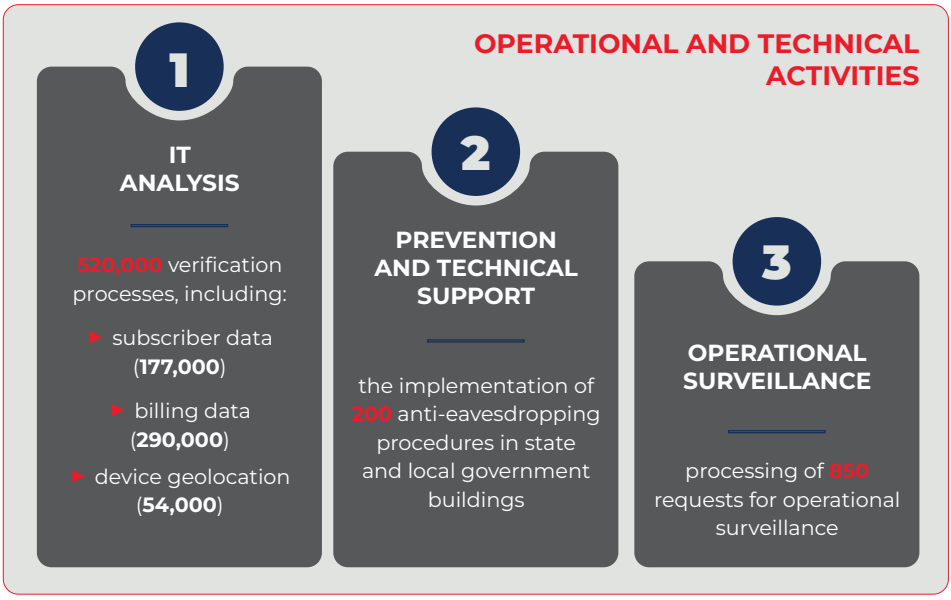
One of the priorities of the Internal Security Agency is the development of its operational and technical capabilities. This is particularly important in the context of rapid technological advancement and constantly evolving threats, which require the agency to continually adapt its tools and methods of operation. Effectiveness in this area depends not only on investment in modern technical solutions, but also on staff development and cultivation of unique, specialist skills.

Activities undertaken in 2024–2025 in the area of technical support included the processing of **over 520,000 telecommunications records**, including:

- **over 177,000** subscriber-related arrangements,
- **over 290,000** billing-related arrangements,
- **over 54,000** locations of mobile devices.

During the reporting period, the Agency also processed **over 850 requests for the use of operational surveillance**.

In addition, as part of the counter-intelligence protection of state and local government bodies, **over 200 specialist anti-eavesdropping inspections** were carried out in 2024–2025, conducted at the request of authorised external entities.



Operational surveillance

Public safety requires effective action, but always within the bounds of and in accordance with the law. Operational surveillance is an extremely important tool for the Internal Security Agency's operational work, as hostile activities by foreign states and organisations are carried out with the utmost secrecy, designed to conceal unlawful acts. This is often the only mean of obtaining information that enables the identification of criminal structures and mechanisms, and consequently the implementation of effective preventive measures. This power is exercised only in strictly defined cases – when other methods are insufficient and the threat is real. The use of operational surveillance is always carried out in accordance with detailed legal regulations, ensuring that there is no excessive or disproportionate interference with civil rights and freedoms.

PREVENTION AND EDUCATION

Given the emerging threats to Poland's internal security, a merely reactive stance to dangerous incidents is no longer sufficient. **It is of equal importance to** cultivate awareness and foster attitudes **conducive to prevention**. That is why the **Internal Security Agency places particular emphasis on gathering and disseminating knowledge about hybrid and asymmetric threats**. Continuously improving the public's ability to identify the activities of foreign intelligence services, as well as methods of recruitment and disinformation, helps to mitigate the risk of intelligence and terrorist threats. For the Agency, prevention is an indispensable element of the country's counterintelligence protection.

Trainings

Between 2024 and 2025, the Internal Security Agency carried out an intensive training programme aimed at strengthening institutional resilience and enhancing the skills of staff in the public administration and strategic sector. During this period, **over 3,000 classroom-based training sessions** were held, covering issues relating to key areas of national security, such as:

- **counterintelligence prevention,**
- **counterterrorism prevention,**
- **the phenomenon of radicalisation,**
- **extremist symbolism,**
- **information security, including the protection of classified information,**
- **cybersecurity.**

The training programme has covered a total of **over 70,000 employees from several hundred organisations**, including key constitutional bodies (the Chancellery of the President of the Republic of Poland, the Chancellery of the Prime Minister, the Chancellery of the Sejm, the Chancellery of the Senate), ministries, as well as institutions of strategic importance (including the Institute of National Remembrance, the Civil Aviation Authority, the General Directorate for National Roads and Motorways, and Polish Nuclear Power Plants).

At the same time, the ABW has been developing remote learning channels, **issuing** – since its launch in May 2021 – **over 1.1 million accesses to the ABW's dedicated e-learning platform**:

https://learning.tpcoe.gov.pl/

The **training courses** were directed to **civil servants,** as well as **employees of state-owned companies, research centres, and institutions and businesses of significant importance from the perspective of safeguarding the fundamental interests of the Republic of Poland.**

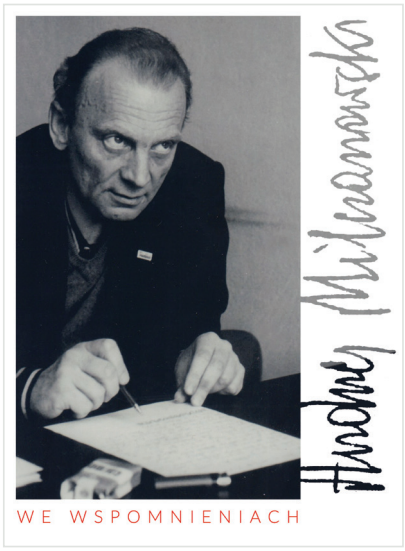
A separate, specialist pillar of the Internal Security Agency's ongoing activities consists of **training for ICT security inspectors** and **system administrators**.

These activities are carried out in both state institutions (the public sector) and private businesses. Their aim is to ensure the correct and continuous operation of systems and networks forming part of the country's critical ICT infrastructure, in order to protect the security of the information processed within them.

Literature

An important component of the Internal Security Agency's analytical and research infrastructure is its publishing activity, which involves the publication of two academic journals. Since 2009, the Agency has been publishing **„Internal Security Review"**, and since 2022 – **"Terrorism – Studies, Analyses, Prevention"**. Both periodicals serve as a forum for the exchange of ideas in the field of broadly understood internal security and evolving terrorist threats. The selection of topics covered in these publications is closely aligned with the Agency's statutory tasks, providing substantive support for decision-making and operational processes. The authors of the articles include recognised specialists, such as officers of the ABW and other uniformed services of the Republic of Poland, representatives of the academic community, and experts involved in the protection of national interests.

In 2024–2025, the ABW published four issues of „Internal Security Review" and five issues of „Terrorism", including one special edition.



In 2025, the Agency also published „Andrzej Milczanowski in Retrospect", a book of memoirs commemorating the late Andrzej Milczanowski, who served twice as Head of the Office for State Protection.

35 years of civic intelligence services

In 2025, the Internal Security Agency marked the 35th anniversary of the establishment of the civilian intelligence services in a free Poland, counting from the date of the creation of the Office for State Protection in 1990. The ceremony organised for the occasion at the Palace of the Commonwealth provided an opportunity to promote ABW officers to higher ranks and for the Prime Minister, Mr Donald Tusk, to present letters of congratulations.

GOOD PRACTICES

The security of classified information and the physical protection of facilities depend on the effective integration of systemic procedures with staff vigilance. Every employee in the public administration and strategic sectors must recognise that they are a **potential target for foreign intelligence services**, which operate continuously and on multiple fronts. In response to these challenges, this chapter sets out a set of fundamental security principles. Their aim is to provide practical guidance to enable the effective identification of intelligence and terrorist threats and the implementation of optimal response protocols in day-to-day duties and work.

Remember! You may possess information that is of interest to foreign intelligence services. The modern security environment requires those handling classified and sensitive information to exercise particular vigilance and to be aware of the manipulation techniques used by adversaries. **Foreign intelligence services employ** a wide **range of tools, methods and means** in their operations – from psychological manipulation techniques in the real world to advanced operations in cyberspace – with the aim of obtaining data critical to the security of Poland. The readiness to take immediate action in the event of terrorist incidents is equally important.

The summary provided on the following pages is a compendium of knowledge on desirable attitudes and procedures – clear guidelines on **what behaviour to avoid and how to respond effectively** to identified threats.

Counterintelligence prevention

Recommended actions 😊

- **Switch on your „information filter”:** remain vigilant if someone asks you too many in-depth questions about sensitive matters or work-related details.
- **Keep an eye out for unusual interest:** be wary of people who show excessive curiosity about your permissions, access to systems or the specifics of your work.
- **Apply the principle of limited trust:** treat any unexpected favour or assistance from outsiders as a warning sign and a potential mechanism for creating dependency.
- **Share knowledge sparingly:** limit the sharing of work-related information to the bare minimum – too much knowledge in the wrong hands is a real threat.
- **Be the ‘shadow’ of your equipment:** whilst on business trips, keep your documents, laptop and phone under constant, personal supervision.
- **Maintain healthy relationships:** use common sense and avoid ambiguous situations that could become a basis for blackmail or manipulation in the future.
- **React immediately:** if you notice any signs of interest from foreign intelligence services, contact the Internal Security Agency without delay.

Undesired behaviours 😵

- **Don’t fall for the „novelty effect”:** never, under any circumstances, disclose sensitive information to people you’ve only just met, no matter how trustworthy they may seem.
- ▸ **Don’t get involved in „quid pro quo” arrangements:** never accept help or gifts in exchange for sharing work contacts or seemingly trivial information.
- ▸ **Do not act as a courier for strangers:** when travelling abroad, never carry parcels or accept gifts from people you have only just met – this is a classic method of compromising and recruiting.

Information protection

Recommended actions 😊

- **Ensure continuous protection:** actively protect classified documents and media containing sensitive data against loss, accidental destruction or unauthorised access.
- **Ensure data is permanently destroyed:** before disposing of documents containing personal data (e.g. personal identification number, address), physically shred them using a shredder. Scraps of paper can be a valuable source of information for third parties.
- **Check printing points:** limit the printing and copying of sensitive documents at public service points where the memory of the devices does not guarantee confidentiality.
- **Maintain supervision in public spaces:** outside the workplace, keep constant, personal control over documents in your possession that contain sensitive information.
- **Use authorised tools:** process classified information exclusively in dedicated and certified ICT systems.

Undesired behaviours 😵

- **Do not discuss work matters in public places:** Avoid having sensitive conversations in cafés, on public transport or in lifts, where there is a high risk of being overheard.
- ▸ **Do not display the contents of documents:** refrain from reading sensitive material on trains, buses or aeroplanes. Bystanders can easily see what you are reading.
- ▸ **Do not underestimate drafts:** do not treat notes or rough drafts as unimportant. They often contain key data that requires the same protection as final documents.

Cyberhygiene

Recommended actions 😊

- **Protect your digital identity:** keep the sharing of personal data to a minimum.
- **Keep your software up to date:** regularly update your operating system and the apps on your computer and smartphone.
- **Verify software sources:** install apps and programmes only from legitimate, trusted platforms and official app stores.
- **Separate device access:** if other people use your computer, set up separate user profiles for them.
- **Use advanced access security:** create long, unique and complex passwords; where possible, enable multi-factor authentication.
- **Manage your passwords carefully:** regularly update your access credentials and do not use the same password for different services and applications.
- **Secure your critical data:** regularly back up your most important files and use data encryption.
- **Be a sceptical recipient:** always check the sender's address, the validity of links and the contents of attachments before opening them.
- **Follow the principle of limited trust:** never trust by default; always verify every request or unusual message.

Undesired behaviours 😵

- **Do not connect unknown storage devices:** never plug found or unknown USB sticks or hard drives into your devices.
- **Do not share passwords or scans of documents:** do not send access passwords or scans of your ID electronically.
- **Do not act on impulse:** do not succumb to pressure from 'urgent matters' or strong emotions accompanying messages.
- **Avoid transactions outside official systems:** when shopping online, never make payments or conduct conversations outside the official platform of the shop or auction site.

Terrorist threats

Recommended actions 😊

- **Stay aware of your surroundings:** familiarise yourself with the evacuation plans for places you visit regularly (your office, a shopping centre, a train station). Knowing where the emergency exits are is key to reacting quickly.
- **Maintain situational awareness:** actively observe your surroundings and pay attention to behaviour that seems unnatural or causes you concern.
- **Identify unattended items:** pay particular attention to parcels, bags or rucksacks left in public places.
- **Prioritise a quick and safe evacuation:** in the event of a threat, leave the danger zone immediately, if possible.
- **Follow the „hide" procedure:** if safe evacuation is impossible, find shelter, barricade yourself in and switch off electronic devices.
- **Alert the emergency services:** once you are in a safe place, immediately call the emergency number 112 and provide a brief description of the situation.
- **Defend yourself as a last resort:** if you cannot escape or hide, and your life is in immediate danger, try to defend yourself using whatever means are available.

Undesired behaviours 😵

- **Avoid approaching the source of danger:** never go near the scene of an incident simply to satisfy your curiosity or to see what is happening. Every second of delay increases the risk.
- **Do not ignore warning signs:** do not downplay suspicious situations or anomalies in public spaces. It is better to raise a false alarm than to overlook a real danger.

ABW field structure

ABW HEADQUARTERS IN WARSAW

Address: ul. Rakowiecka 2A, 00-993 Warszawa

ABW DUTY OPERATIONS OFFICER:
phone +48 22 585 82 21, fax +48 22 585 84 88

www.abw.gov.pl

Warsaw 2026