NATIONAL INTELLIGENCE SERVICE

ANNUAL REPORT 23/24

OF PRIORITIES AND KEY FIELDS OF ACTIVITY

SEPTEMBER 2023 – AUGUST 2024

NATIONAL INTELLIGENCE SERVICE

ANNUAL REPORT

OF PRIORITIES AND KEY FIELDS OF ACTIVITY

September 2023 - August 2024

INDEX

FOREWORD BY THE DIRECTOR-GENERAL

The threats to our country's national security are well-known and, unfortunately, persistent. Regardless of any positive developments in specific matters in our bilateral and international relations, or any favorable circumstances, the National Intelligence Service (EYP) cannot afford even a moment of complacency regarding potential external threats, regardless of their origin.

Nor can it afford to be anything less than constantly vigilant domestically, against possible acts and intentions related to espionage, terrorist attacks, organized crime activities, cyberattacks targeting critical sectors, networks supporting illegal migration, as well as threats against our freedoms and democratic governance.

As recent international experience has shown, even the slightest oversight, negligence, misjudgment, or illusion – no matter how reasonable or well-founded an optimism may be – must never lead to a reduced state of readiness. Concerning timely monitoring, risk analysis and assessment, as well as dealing with any potential threat. Moreover, our immediate and broader neighborhood remains complex, marked by contradictions, inequalities, and bilateral relations under strain, while being in constant interaction with a wider region where pressures of all kinds are multiplying.

When, within this already challenging framework of threats and in this very neighborhood, not one but two wars have taken place – both of which significantly affected the lives nearly of all of us, throughout the period covered by this report – it is evident that a Service dedicated to safeguarding National Security, especially in a country like Greece, must also address the various threats arising as a direct or indirect consequence of these armed conflicts.

Furthermore, domestic developments such as elections – held three times between September 2023 and August 2024 – as well as major political, social, religious, sporting, or artistic events, which increased significantly in the past year, also required constant vigilance. This was necessary to counter those, both inside and outside the country, who would attempt to exploit such occasions to promote their own malign objectives, thereby threatening National Security.

In response to both the nearly constant threats of recent years – though continuously evolving and adapting – and those emerging from recent developments, the EYP had to be well-prepared during this period. Its contributions included the deterrence of threats, the exposure of networks, the prevention of malign actions, a better understanding of risks, and the improved preparation of national positions on all matters concerning our National Security.

To address these challenges, the EYP, leveraging its own resources and personnel, collaborations with domestic agencies, and increasingly intensified international partnerships, played a distinct and crucial role, as described in the pages that follow. Many times, throughout the past period, various competent authorities were able to fulfill their missions more effectively due to intelligence provided by our networks, personnel, and means by our role, and should not be, visible to the general public.

Particular emphasis during this period was placed on cybersecurity, with the EYP gradually establishing itself as the primary entity responsible for countering attacks on ministries and the organizations under their supervision.

Beyond its core mission, the past year also saw continued structural reforms aimed at modernizing EYP – making it more efficient, more accepted by citizens as a fundamental pillar of national security, and fully integrated in the new technological universe as shaped by the rapid technological progress. The goal: a more effective, meritocratic, and outward-looking intelligence service, always dedicated to fulfilling its national mission while upholding democratic principles and the rule of law.

The Priorities and Areas of Action Report for the period September 2023–August 2024, published for the second consecutive year, provides a detailed picture of the key issues EYP had to deal with over the past year – within the constraints imposed by the nature of an agency whose public interventions must never jeopardize its work or mission. However, this report is also part of EYP's ongoing efforts to foster a culture of security, a mindset of vigilance, and a mentality necessary for defending the national security. Given the new opportunities and threats emerging daily, such an approach must now extend beyond government officials and public servants to encompass all citizens.

We are not here to claim that we have achieved a lot, or that we have done everything perfectly. Quite the opposite. We are fully aware that there is still much to learn and much more to do. We have not yet become what we aspire to be, nor what we must become. However, the one thing we can say and which I believe is clearly demonstrated in the detailed presentation that follows – is that, even in this challenging period, we have taken decisive steps in the right direction: the one demanded by our times, dictated by the interests of our people and befitting a European democratic nation.

The Director-General
Themistoklis Demiris

MAIN DEVELOPMENTS, CHALLENGES AND PRIORITIES OVER THE LAST PERIOD

A. EYP IN THE SHADOW OF TWO WARS

The period from September 2023 to August 2024 was a highly demanding one for every Intelligence Services, as they were faced with a series of national security challenges caused by two large-scale simultaneous and enduring wars, which lead to a series of new needs at national and international level. Particularly regarding Greece, the two armed conflicts in our wider neighbourhood, in the North and South, imposed readjustment of priorities, vigilance towards new risks, shielding against new or upgraded threats, as well as enhanced cooperation with national and mostly foreign actors.

The conflicts in Ukraine and the Middle East increased threats and risks due to the effects of war onto populations living in the war-affected areas. Nevertheless, they also impressively increased attacks against critical infrastructure, communication, and energy networks, even on territories far away from the war zones, while the number of cyber-attacks against state structures and systems skyrocketed too.

Our country's proximity to the conflict zones, its key role in transports, communication, energy, goods and arms transport networks, as combined to its position in the Western world and its commitment to the democratic values and liberal lifestyle of an open tolerant and inclusive society, could be exploited by malign actors seeking to cause various kinds of damage: from symbolic, undermining the country's prestige and credibility, to dynamic and violent, individual and collective, causing concrete damage to Greece, or its allies and partners, on our soil.

Yet the two wars and their consequences do not at all allow any complacency towards other long-standing external and internal threats; faced with these, EYP may not for a moment ease attention, vigilance and reflexes to take immediate action. The attitude of third and especially neighbouring countries, the long-term objectives and means they use in pursuit of these objectives, regardless of any positive developments that may prove conjectural, remain in our Service's sights, such as any internal vulnerabilities prone to exploitation. Thwarting espionage and terrorist activities – wherever they may come from – fighting organized crime, especially in its international dimension, as well as illegal immigration, have also been top priorities in our fields of action, as provided by the law in our statutory responsibilities.

In the previous year, particular emphasis was also given to Cybersecurity. And this was only natural given that cyberspace is increasingly becoming a privileged field for malign activities, where groups or individuals, sometimes linked to state actors, may not only seek easy profits, but also exploit vulnerabilities at an insignificant cost, causing a disproportionate cost to be paid by public institutions and critical infrastructure, and eventually impairing National Security.

Yet, in order to deal with evolving new challenges as well as existing ones that keep upgrading, appropriate groundwork in terms of structural organization and equipment is a sine qua non. During the last year, EYP stepped up efforts to evolve into a modern agency at the service of national security and the Greek citizens: through legislative initiatives, internal regulatory acts, administrative restructuring, elaborating policies on various fields of action, training programmes, but also thanks to the acquisition and the creation of new advanced technology tools, EYP has been constantly adapting to the requirements of our time, as these are determined by geostrategic, economic, social, as well as environmental developments, so as to fulfil its mission in the best possible way.

The following pages give a detailed description of fields of action, priorities, as well as the philosophy of our Service vis-ŭ-vis these challenges and our responses to that marked the last year.

B. MAIN THREATS IN THE NEW REALITY

1. The consequences of the armed conflicts

Although the Ukraine war was in its second year in 2023, or perhaps for this exact reason, namely because this war has been lasting far more than the period obviously anticipated by those who planned and imposed it, within the period under review in this report, there were intense collateral consequences for Europe and our country.

The challenges particular to our country, which of course go beyond countering or preventing traditional espionage, consist in detecting likely efforts of disinformation and malign influence operations aimed at spreading fake news and confusion over the developments of the war or our country's attitude and interests. International experience has in fact shown that the academic environment and the communities originating from the war-affected areas make a privileged target for such purposes.

Attacks against critical infrastructure and networks in third countries have sounded alarm bells regarding also the need to protect our own structures – similar or other– whilst there

were repeatedly detected cyber attacks linked to both conflicting parties, a fact that imposed vigilance in our country too, which has already generated positive results in terms of timely identification and response.

The religious dimension of the Russia-Ukraine war, should not be overlooked either, seeing that, churches, monasteries and orthodox cult areas have been transformed into fields of religious conflicts and influence operations, with clear political and geostrategic repercussions.

Risks and threats arising from the crisis in Gaza were and are different in nature:

First of all, in relation to terrorism: the anti-Israeli feelings of pro-Palestinian groups and population accentuate tendencies of organized groups or "lone wolves" to strike blows against Jewish or Israeli targets, or even against countries that, in their view, are pro-Israeli. At the same time, relevant propaganda inspires terrorist acts even for reasons unrelated to the Middle East question. What is more, the possibilities offered by social networks, encrypted communications and the latest technology devices, such as 3D printers, multiply risks as they dramatically widen the circle of elements who could pose threat.

The radicalization of groups in the population, as a result of developments on the battlefield, is a major source of concern too, in particular when our country has been receiving migratory flows consisting mostly of young men from war-affected zones.

In addition, as a general consequence of the crisis, illegal migration has further surged, whereas the problem may deepen further should the extra 1.5 million of the internally displaced persons still remaining in Lebanon and Gaza feel even more threatened, or further in despair, and set off towards a better and safer life elsewhere.

The currently increasingly active involvement of organized crime elements in migrant smuggling networks and terrorist cells further aggravates the problem.

2. Our immediate neighbourhood

The Service's interest in what is happening in our immediate surroundings and any resulting threats may not at all wane under the pressure of developments in Ukraine or the Middle East, however dramatic these may be. Even in periods of detente or progress in multilateral and bilateral relations, even in calm periods when there is no concern over resurging of tensions or frictions, a Service, fully committed to the protection of national security, timely identification of risks and steady vigilance over all kinds of threats cannot be complacent. Particularly when bilateral problems are not being resolved, or are getting worse, agreements

seem to be negated, disputes over rights, and unfounded claims continue to be fostered.

It is obvious that, identifying priorities, sensitivities and each side's "red lines" facilitates, mutual understanding and allows possible cooperation in areas where all sides deem useful to exchange views, experiences and know-how.

In this framework, in the period 2023-2024, EYP again mobilized human and other resources for the best possible monitoring and understanding of developments in our immediate neighbourhood. Moreover, the Service strengthened cooperation with counterparts in the region on issues and sectors of common priority, with a view to a coordinated and combined response against phenomena that pose threats to all of us.

In the period under consideration, EYP continued to closely monitor every development in the border and nationally sensitive regions that could affect our national security, whether related to activities of individuals, groups, legal persons,companies or to transports, transfer of goods, or to provision and installation of equipment which could pose threats to our national security.

On all these issues, including all national security-related ones, in relation to the two wars and within the framework of its distinct role, EYP has been systematically providing the competent national institutions with intelligence reports, opinions and recommendations, for them to act the framework of their powers and responsibilities. Furthermore, the Service has provided important intelligence on the intentions, capabilities, and plans of countries of our interest, which allow for our best possible preparation for any scenario.

3. Classic and new types of espionage

The nature of espionage has now changed drastically. The well-known traditional methods of individuals infiltrating into nationally significant mechanisms, or of acquiring classified information and documents, are now added cyber-attacks aiming at extracting data from state institutions, impairing critical infrastructure, penetrating energy networks, transports, telecommunications and financial institutions, influencing decision-making within crucial stakeholders, etc. EYP has been playing a key role in countering these threats by deploying of counterespionage operations.

In order to address traditional forms of espionage, EYP mostly invests in prevention. Another top priority during last year was to promote heightened awareness across all national institutions, over any form of covert and malign activity, by providing constant intelligence updates.

In terms of prevention timely identifying suspicious conduct, cross-checking data with multi-

ple sources, systematically exchanging information, collaborating on the field and via capitals, have proved to be of vital importance. It is via these methods, separately or jointly, that Services like ours discover the real identity of individuals who, acting in an irrelevant seemingly innocent and usually convenient professional capacity, are actually operating or intend to adversely operate in order to extract classified information, or exercise influence to the benefit of a third country. The cancellation of residence permits or the refusal of entry visas prevent (and indeed prevented last year) espionage activity against our country.

Infiltration methods used by third actors for gaining know-how include, inter alia, acquisition of cutting-edge technology-related companies. Furthermore, according to international experience, malicious actors may also target academic institutions, think-tanks and corporate research departments, in order to obtain valuable scientific information, circumventing European statutory restrictions.

That is why, in the same framework, the activities of cultural institutions of specific countries and certain scholarship exchange program are being investigated on a global scale, for potential gathering of sensitive information, knowhow transfer, talent scouting and recruitment on behalf of foreign actors. Travels of Individuals with knowledge, experience and knowhow in areas of special strategic sensitivity, who travel to specific third countries in order to provide educational or other services, are also subjects of our attention.

During the same period, EYP also remained alert to the use of social media by Services of non-friendly countries for recruiting persons of interest. The “recruiters” frequently appear as researchers, think-tank members, human resources or consulting executives, and seek to attract individuals they deem able of providing key information in exchange for various benefits.

In order to effectively address such threats, EYP has upgraded its analytical and technological capabilities, being now able to analyse vast amounts of data and using advanced algorithms detect suspicious activities. Moreover, EYP remaining to constant contact with the relevant Greek authorities to promote their awareness and vigilance against the installation of technological equipment which, although highly advanced, could be of suspicious origin, particularly within critical infrastructure.

4. Terrorism: traditional threats, marginal elements and “lone wolves”

Countering terrorism is always a core priority for EYP. Especially following the to recent developments in the Middle East and terrorism incidents that took place or were foiled across Europe, as of October 2023, the Service’s vigilance has sharply increased.

In light of, inter alia, the findings of counterpart Services, our targeting of suspicious elements has been mostly sighting smaller autonomous and self-acting groups, marginal individuals easily to be bought out and lone wolves adherent to specific ideologies.

The international contacts of extremist elements, the interaction observed between local radicalized extremists and ''foreign fighters'', as well as the ease with which they may gain access to hazardous material, also call for constant vigilance. Moreover, since radicalization, recruitment, guidance and direct handling of individuals is now largely carried out via the Internet, tracking down suspicious processes and detecting potential terrorists is a difficult task which requires a combination of appropriate technological research and information analysis tools, effective use of human sources, as well as intelligence exchange mechanisms among counterpart services.

As to potential targets of terrorists, our Service's heightened attention is mostly focused on vulnerable and highly symbolic ones. A telling incident in the period under review in this Report was the attempted arson attack on a building of such relevance, in a case where once again the perpetrators were linked to guidance centres in a specific country.

Another source of concern is the reactivation of organisations such as DAESH (I.S./I.S.I.L./I.S.I.S.) and AL QAEDA, particularly in the countries of Sahell, these organisations taking advantage of local problems and the ensuing security gap, enhance their presence and networks while intensifying psychological and intelligence operations against selected countries, as well as efforts to lead sympathizers on an international scale.

But in addition to the Middle East, there were also threats and attacks originating from organisations such as ISIS-KP (Khorasan Province), which – despite its strong natural presence in Afghanistan and South Asia, has given emphasis on recruiting from Central Asia. In this way, it is in a position to mobilize Europe and Turkey-based adherents, who can easily reach our country.

There is also constantly heightened vigilance over migratory flows and domestic refugee accommodation centres which could be infiltrated by terrorist elements, or where carefully selected inmates could be manipulated into perpetrating terrorist acts.

Lastly, as prevention always takes precedence over a posteriori suppression, EYP has stepped-up efforts on the issue of terrorism financing, especially through the crypto-economy, as well

as monitoring terrorism content on the Internet. Furthermore, following recent legislative initiatives, EYP was entrusted with the responsibility of processing orders, even for the removal of such content from the Internet.

5. Illegal migration: Smugglers and their accomplices

As long as its causes are not being dealt with in a decisive manner, illegal migration results in human tragedies that the international community is called to and must cope with. But as long as this phenomenon is allowed to carry on and grow bigger, it unfortunately unfolds into one of the most severe and multilayered threats to the economy, society and national security of transit and host countries. It is a telling fact that, already in 2023, the number of illegal entries in the country had reached 72,104 as compared to 49,061 for the whole of 2022, whereas in the eight-month period from January to August 2024, there was an increase of about 20% as compared to an already increased number in the respective eight-month period of 2023.

In the previous year, EYP enhanced both its operational initiatives and its international co-operation towards an improved understanding and handling of this situation, drawing useful conclusions, and better preparing towards emerging trends and actions.

In this spirit, the Service provided enhanced input to the relevant national bodies to assist in addressing this phenomenon.

More specifically, our efforts focused on both intelligence gathering and analysis, via the use of appropriate technology and human sources, and cooperating with foreign counterparts and Security Services aiming mainly at limiting the activity of those who exploit the tragedy of people in need in order to profiteer with complete indifference to the broader consequences of their acts, but – most importantly – to direct risks to human life.

In the same context, the Service has broadened cooperation especially with neighbouring countries in an effort to further mobilize their local authorities. And, although in certain cases there was an actually keen response, in other cases, special conditions prevailing in several countries of origin have created a barrier to the progress sought by our side.

Our Service's attention has also been drawn by the constantly updated modus operandi applied by smugglers networks; depending on requirements and capabilities, these networks use fishing or speed boats, and constantly change routes and destinations, aiming at a safer and most profitable outcome. The findings of EYP's investigations and researches are notified to the competent authorities on a constant basis, thus decisively contributing to detection and

arrest of smugglers, as well as to pre-emptive action. Thanks to this cooperation and further to information provided by EYP, a number of Turkish coast-based smuggling and forgery networks, which were operating inland and on islands, were identified and dismantled.

As indicated by the previous year's analyses, there is particular interest in the link between illegal migration and organized crime, as criminal networks increasingly exploit migrant flows in order to increase their illegal activities and profits.

6. Organized crime: The international dimension and the internal parameter

Through activities such as trafficking of arms and human beings, and apart its known effects, Organized crime also poses a complex and ongoing threat to the country's stability and national security. For this reason, tackling organized crime is a matter of vital importance to every country, and particularly to our country, especially when certain organizations have direct links to foreign actors, even state ones, thus are able to serve geopolitical and political targets of third countries, through their own actions and operational networks.

Furthermore, the vast profits made by organized crime are often used to penetrate in the lawful economy (e.g. petrol stations, real estate), causing perturbation in the markets and de-stabilizing trends in the financial systems. In any case though, apart from compromising financial stability overall, damage is made to law-abiding businesses.

Finally, money-laundering and related tax evasion by such networks, affect the level of state revenue, causing loss of billions of Euros every year.

On all the above-mentioned issues, in addition to gathering information, EYP focused on analyzing political, financial and social procedures that favour the activities and growth of such networks, in order to facilitate a comprehensive and long-term response by the competent bodies.

Particular emphasis was placed on organized crime networks with ties to foreign countries. In this regard, EYP provided the relevant law enforcement authorities with specific information and comprehensive presentations of crime networks, which either originate in direct neighbours and countries of the wider neighbourhood, or act autonomously, copying the methods of similar groups abroad.

The operation of companies appearing to be legal but, inter alia, are actually channelling unlawful money in the real estate market, offers the possibility of a residence permit in Greece as investors, even to third country citizens who could be carrying out illegal activities. As a matter of

fact, in the framework of preventing such practices, through international cooperation and joint operations with other Greek competent authorities, our Service has detected cases of significant sums of money transferred on behalf of leading figures of transnational organized crime.

More specifically, our Service's actions and researches exposed links between locally active elements and similar foreign groups, as well as activities of groups and/or leading members of transnational criminal organizations in our country. Just in spring 2024, precisely thanks to Service intelligence, such individuals were arrested whilst others were prevented from entry and return to action, in our country.

Furthermore, in regards to developments in the field of organized crime, we should point out the upward trend in organized crime group members who often travel to our country from abroad and present themselves as members of "Friends Societies/Clubs" of e.g. various sports and hobbies while there are traces indicating that these "clubs" actually operate in drug trafficking and money-laundering.

Finally, the Service also played a significant role in revealing corruption in the public sector, since the information gathered and timely shared with the competent authorities as part of EYP's investigations lead to dismantlement of corrupted public officials' rings who, in abuse of their positions, were availing personal benefits, adversely affecting state interests and the prestige of state institutions.

7. Cyber-attacks: the international and national experience

The speed of technological development and the increasing reliance on digital networks and systems have exacerbated the challenges in the field of cybersecurity. In the past year, our country has seen a multiplication of cyber-attacks against state and private targets, with the majority of them targeting information systems of Ministries and critical infrastructure, but also concern sensitive functions and personal data of citizens.

In the period covered by this report, EYP, having been entrusted with the relevant responsibility as the «Computer Emergency Response Team» (National CERT), has dealt with 31 distributed denial of service (DDoS) attacks targeting public and private entities (Ministries, airlines and shipping companies, energy companies) and have proven to be effective. In addition, there were 13 attacks to falsify website content, 9 attacks to breach infrastructure by leaking data, 7 ransomware attacks, and 4 phishing campaigns, aiming at deceiving users and collecting data. These attacks represent the most serious cases of cyber-attacks on record and not the totality of those that occurred. Of the above-mentioned recorded attacks, some were of particular intensity and scope, and the perpetrators were linked to decision centers in foreign countries.

In the effort to combat cyber-attacks, a key aspect is to increase the capabilities to prevent such digital threats. EYP has insisted in the past year on developing specific technological solutions, strengthening intrusion detection systems, developing training programs and implementing strict data security protocols.

In addition, in autumn 2023, the operation of the Security Operations Centre (SOC) was launched, which will gradually integrate the digital service delivery systems of the Ministries and their supervised entities. The degree of integration of the Ministries into the SOC is already progressing smoothly. The main objective is to provide integrated prevention, early warning and response to cyber incidents. The infrastructure of the Security Operations Centre offers automatic attack detection and increased incident investigation capability, through interconnection with national and international authorities and the European Cybersecurity Agency (ENISA).

However, as, in addition to technological development, public awareness is also of key importance, EYP issued 3 specialized guides on cybersecurity, with the precautionary measures to be taken at an individual level by public sector employees handling sensitive or classified data.

At the same time, information and training programs for civil servants were carried out, with the aim of developing a strong cybersecurity culture, which is an indispensable objective on the Service's priority agenda, in the context of the defense of National Security.

C. OPERATIONAL, TECHNOLOGICAL, ORGANIZATIONAL UPGRADING AND EXTROVERSION

1. Restructuring and operational reforms

While the period 2022-2023 was one of planning and preparing for the evolution of the Service, the period 2023-2024 marked the commencement of the implementation of this reform, with EYP entering a new phase of modernization and restructuring, following entry into force of Presidential Decree 17/2024. The main purpose of this restructuring was and is to build up operational capability of the Service, upgrade the means and methods of intelligence gathering and analysis, and better adapt vis-ũ-vis current challenges and threats, as these arise mostly from developments in technology and cyberspace.

In this spirit, the main aspect of the EYP restructuring concerns the reinforcement of the Operations Directorate with human resources, in order to ensure that, provided with modern tools and staffed with highly specialized personnel, it can operate in the most effective way in intelligence gathering and utilization, so as to prevent threats in all areas of Service competence.

At the same time, the establishment of a single Analysis Directorate will enhance the Service capability for thorough and combined studies as well as conclusion-making on the basis of information from both the Operational Directorate and the partner Services and Agencies.

Constant interaction between these two Directorates shall prevent fragmentation of information and overlapping of responsibilities, whereas enhanced interoperability will lead to optimum information-sharing with leadership and competent institutions, over the wide range of threats targeted by the Service. This particular purpose of interoperability will be served by the Mission Centres, which will be operating as focal coordinating hubs on matters of priority.

As part of the restructuring under way, combined with the ongoing logistical upgrading, the Cyberspace Directorate and the Information and Communication Systems Directorate will be reinforced too, seeing that cyberspace has proven to be one of the most crucial threat-generating fields of our time, whilst sophisticated and secured communications a permanent goal for all Intelligence Services. Regarding this threat, our Service is undergoing a switchover to satellite communications.

With regard to personnel, an important novelty has been introduced, i.e. the creation of new Staff Categories such as intelligence officers, intelligence analysts, cyberspace officers, cyberspace analysts, with a view to recruiting and utilizing specialized personnel who will now be able to professionally evolve on meritocratic criteria and on the basis of established upward steps for each category.

There were also steps to enhance digitisation both within the Service and in its contacts with counterparts. In addition to innovations concerning the Service's internal program, an important step to resolve a long-standing problem was the launching on 1.1.2024 of the electronic platform stipulated by Law 5002 of 2022, through which the Attorney's General orders for communication waivers are transmitted to Telecommunications Providers and the Hellenic Authority for Communication Security and Privacy (ADAE).

What is more, as the Service restructuring places emphasis on accountability, respect of the rule of law, and extroversion, an Internal Control Unit was set up to ensure respect of the law and integrity among staff. The Unit is responsible for investigating any reprehensive behaviour, breaching of security procedures, as well as any case of corruption. A Code of Conduct specifying the basic directives for professional and personal conduct has been introduced and is now in force all staff members.

The implementation of the new Staff Grade and Task Description Charts is also expected to help ensure professional integrity and consolidate a sound working environment.

Lastly, the operation of the Press and Communications Office has already enhanced the Service's extroversion, whereas, particularly during the past period, it has strengthened cooperation with the Media by making appropriate contacts and issuing press releases that kept the general public informed about selected activities of our Service. There was also better use of our webpage potential, a fact confirmed by the increased number of visits.

2. Cyber-security tools and structures

The security of communications, in the light of the recorded attempts to violate their confidentiality, which are taking place all over the world, is a huge challenge of our time and requires the adoption of appropriate measures and the purchase of the necessary technical means. At the same time, the cases of cyber-attacks observed in our country in the past year have highlighted the need to strengthen the means and the Agency's capabilities against cyber threats.

In an effort to respond more fully to its relevant tasks, EYP invested significant financial resources in the past year on technical means of protecting the confidentiality of communications, security controls, threat prevention, malign actions detection while devoting significant resources to advanced data analysis systems and cutting-edge technologies such as Artificial Intelligence. In addition to what it has acquized, EYP has also manufactured and developed technical tools of its own invention and construction, using its own resources and in cooperation with specialized Agencies, always with the aim of safer communication and the timely detection of intrusions and threats against government Agencies and critical infrastructure.

The key pillars of the Service strategy are early detection of attacks, the implementation of strict data protection protocols and risk assessment. However, as the management of cyber-attacks should not be limited to reaction, but should mainly be about active surveillance and prevention, an important objective of the Service has also been, over the last period of the time, to educate and raise awareness in the public sector in order to develop a strong cyber-security culture.

Implementing the above principles, EYP, as the competent authority for technical information security issues (INFOSEC National Authority), has carried out a series of suitability checks on systems handling classified information, providing technical advice public and private Institutions. In addition to distributing instruction manuals handling classified information in computers or mobile phones, it systematically provided specific recommendations for securing classified information, conducted market research to protect national communications, and acquired devices and software for checking malignant interference and vulnerabilities.

In the context of its operation as the National Tempest Authority, i.e. as the Authority re-

sponsible for securing the state's electronic telecommunications equipment from leaks due to unwanted, electromagnetic and non electromagnetic, transmissions, EYP has carried out a series of checks in Ministries and Regional Administrations in order to detect any omissions in physical and electronic security issues, while the procurement of new equipment to improve its capabilities is underway.

An important part of cybersecurity is the use of reliable cryptographic products. In this area too, EYP, as the National Crypto Authority, has been in constant contact with operators using such devices to update old cryptographic products and has developed a new cryptographic application for the management of confidential information.

At the same time, the period covered by the report has seen an upgrading of efforts to develop a national encryption algorithm and innovative approaches to increase the resilience of encryption systems to future threats such as quantum computers. Procedures are also underway to establish Infosec, Crypto and Tempest laboratories that will be able to certify products of third parties that are interested in informing their public that they comply with international security protocols.

Lastly, a special technical protection team has been established to shield the communications of high-ranking officials and critical facilities in Greece and abroad, including through periodic checks.

3. Intelligence and Counter-espionage Academy

The Intelligence and Counter-espionage Academy which was established pursuant to Law 5002/2022, reflects the Service's commitment to upgrading its staff training through a new educational philosophy and practical courses, with a view to dealing with increased needs in fighting future threats. The Academy is structured in four basic components (Studies and Coordination, Research and Evolution, School of EYP Staff and National Security and Intelligence Training Centre).

Furthermore, the Academy's Knowledge Centres were set up as another important novelty. These Centres operate as a focal point for the exchange of knowledge and experience among experts in different fields, such as intelligence analysis, terrorism, organized crime, cybersecurity, and counter-espionage. The Knowledge Centres already play an important role in the planning and implementation of training programmes and the drawing up of training manuals.

To further support the Academy's mission, the establishment of special infrastructures in its facilities, such as a cybersecurity lab, a virtual reality booth has been planned while the train-

ing village, which is under construction, will provide staff with practical training in a controlled environment under realistic conditions.

4. Historical Archive and Museum

Over the years of its operation in various forms and under various names, EYP has compiled an important Archive which pertains to crucial periods of our history. With a view to raising awareness, both at national and EYP level, the Service has initiated procedures for partial disclosure and utilization of archival material, in compliance with statutory regulations, as well as with a strong sense of both its historic responsibility and mission to defend national security.

As a first step, on the completion of 50 years ever since, the Service has proceeded to disclosing archival material regarding one of the most tragic periods of our modern history, i.e. the period of July-August 1974, in an effort to contribute to better understand the tragic events in Cyprus, which sealed the fate of the entire Greek nation.

Other steps will follow for specific, carefully selected periods, always in compliance with procedures provided under the laws, and in collaboration with specialized scholars.

At the same time, the establishment of the Museum of EYP (Visitors Centre), is underway. It will be a place that, through its exhibits and interactivity, will offer visitors an opportunity to understand the Service's mission and work, to experience its evolution during the various phases of our recent history, but also become familiar with key issues of our National Security.

5. International Cooperation

Developing International Cooperation is an integral and essential part of an Intelligence Service's function since the problems encountered are often common and their successful solution requires collaboration of a number of Services. Especially when a Service plays a "dual" role (as EYP and another eight Services in the EU), i.e. it is responsible for both internal security and external threats, there are multiple opportunities and advantages in international cooperation, which may touch upon a wide spectrum of issues, useful to many national institutions.

In the previous period, EYP broadened its physical presence, particularly in countries vital to our security, strengthened cooperation with other Intelligence Services, the EU and NATO, whilst kept active participation in several multilateral structures at both European and regional levels. Furthermore, in the context of "Intelligence Diplomacy," EYP participated in a series of

trilateral, quadrilateral and quintlateral structures, whereas it held numerous bilateral contacts with counterpart Services in various countries. Besides, thanks to contacts with counterpart Services from many different countries, there is often exceptionally useful messaging, particularly in emergency situations or when other communication channels are not in operation.

Moreover, in addition to contacts at Head of Service level, cooperation with other Services was further extended to the level of officers and experts of various Directorates, thus enriching knowledge and improving practices in addressing threats. International cooperation goes of course far beyond paying visits. It mostly relates to exchanging information, cross-checking data and submitting proposals, further to which action is taken in different countries in order to serve common purposes. In one telling example, further to information provided by our side to third countries, the latter succeeded in dismantling networks that were adversely acting against them but also against our country.

Lastly, it is worth noticing that, as part of its participation in various multilateral structures, our Service organized several successful multilateral meetings in Greece, which garnered very positive comments by all participants.

D. THE CHALLENGES OF A FUTURE THAT HAS BEGUN

With two wars raging in our neighbourhood and the efforts for cessation of hostilities running into numerous obstacles, it is obvious that even if the efforts prove to be more or less successful, the consequences of the phenomena and traumas caused by the fighting will take a long time to heal. Not only in the countries and regions directly involved in the conflicts, but also in countries which, for political, economic, energy, social, and geographical reasons, such as our country, can easily be affected by any relevant development. Therefore, alertness and resource mobilization on issues arising from what has happened and will happen in the conflict zones is expected to keep preoccupying for the Service and the European Union in the coming year and beyond.

At the same time, as the problems with certain neighboring countries are not resolved, and on the contrary, some of them are even intensified, vigilance with regard to any kind of threat that may be linked to them is also expected to characterize the activities of the EYP in the near future.

However, in addition to issues such as external threats and internal developments relating to them, terrorism, violent extremism, human smuggling, organized crime, etc., that are among the common and expected/foreseen threats that an intelligence agency is called upon to deal

with, what will perhaps require the most intensive efforts to readjust actions and redefine priorities in the near future is the evolution of technology, which gives, easily and sometimes almost costlessly, new capabilities to an increasing number of institutions, organizations, networks as well as small groups or individuals.

Hybrid threats, such as disinformation, information manipulation and cyber-attacks, which are already a major concern for the Service, are expected to require more active monitoring of relevant phenomena and data, in order to identify their origin, to build defence against them or counter them in any way. In particular, Foreign Information, Manipulation, and Interference (FIMI), which involves systematic campaigns of spreading fake news and, through them, manipulating public opinion and ultimately destabilizing society, is a new asymmetric hybrid threat that is expected to be of ever-increasing concern.

In preparation for this future, which has already begun, EYP will insist on strengthening its human and material capabilities for early detection and effective countering such attacks by allocating resources and participating in relevant international programs, as well as in bilateral and multilateral cooperation schemes.

Another major challenge is the recent rapid growth of Artificial Intelligence (AI). It is clear that in the hands of responsible services and Institutions working in the interests of countries and their people, AI will become a valuable new tool that will offer significant capabilities, not only in big data analysis and threat prediction but also once a much broader scale.

On the other hand, however, its divulgation and the possibility of easy acquisition of enormous media capacity, either by malign and well-organized actors or by completely uncontrolled actors and people, poses new dangers. That is why important processes are under way in the EU and NATO, with the participation of our Service, to develop the appropriate legal framework.

The use of AI for cyber-attacks, automated data breaches on other malign actions requires constant vigilance. EYP will continue to invest in the development and adoption of advanced technologies to counter such threats, while closely monitoring all relevant developments to improve its own capabilities, ensuring its proper use, in the name of protecting National Security and Democracy, but also in the name of adherence to the Rule of Law.

In addition, other new forms of threats, such as biological and chemical terrorism, have emerged as serious challenges to global and national security, while developments in biotechnologies and interference systems in communications are providing additional opportunities for malign actors to launch attacks that can cause widespread damage to critical infrastructure, such as energy networks or telecommunications. And to counter these new forms of threats, EYP is obliged to continue to invest in the continuous information and training of its staff and in its partnerships.

However, adapting to new threats requires more than just being vigilant and monitoring developments. International and national partnerships and continuous training are not enough. A crucial challenge is to seek and embrace innovation as a constant need.

Innovation is a fundamental concept for progress and development at both individual and collective level. It expresses a culture of continuous self-improvement and innovation, which encourages the constant search for solutions to emerging challenges. In critical areas such as national security, the need for innovation is even more pressing, as constantly evolving threats, both in the physical and in the digital world, require constant adaptation and the adoption of innovative initiatives.

Realising the importance of seeking such solutions and establishing a culture of pioneering, the EYP, through the creation of the Innovation Hub and the Science and Research Experts Pool aims to mobilize staff in this direction, to familiarize the Service with the relevant needs and opportunities, to motivate the staff involved and to take advantage of the funding opportunities offered by the European Union for this purpose.

In the same context, the creation of the Tech Talent Network aims at interacting with experts or talents outside the Service for their possible participation in technological initiatives of national importance, while the establishment of the SciTech Radar will ensure the monitoring and analysis of the latest developments in the field of emerging technologies, acting as an ''innovation radar'' for any scientific or technological development that may affect national security or the Service's capabilities.

However, in addition to the threats associated with the evolution of technology, , the threats to national security that can arise from planetary phenomena, such as climate change, which affect even the stability of countries and regions through climatic changes or natural disasters, should not be underestimated. Such environmental developments also reinforce the phenomenon of climate-induced internal and transnational migration, causing, inter alia, social, ethnic or even international tensions.

The conclusions of a conference organized by EYP in the autumn of 2023, in the framework of NATO, on «The Climate Change and the security environment» confirmed the need for national and collective vigilance against the upcoming threats from climate change.

EPILOGUE

This report, like the previous one, and like every Intelligence Service report worldwide, is necessarily elliptical, as it is subject to the limitations imposed by the nature and mission of the Service: Under no circumstances can the publication of a recount contain any information that could go against national interests, undermine our national security in the slightest, or create risks for the Service's operations. Nor can actions that have been carried out or recommendations that have served as warnings and preventive measures be described, as these can be known only by a small number of authorized individuals who alone are entitled to such knowledge.

However, in the name of accountability and the need for citizens to understand its role, the annual report of the National Intelligence Service (EYP) can and should describe, with the greatest permissible accuracy, the areas in which the Service has primarily been active, the critical issues it has dealt with, and the efforts it has made to fulfil its duties – while balancing the willingness to inform with the necessity to maintaining confidentiality.

Additionally, it was deemed appropriate to include our main findings regarding the trends, phenomena, and behaviours we have encountered across all areas of activity during this period, which, as expected, has been marked by two conflicts in our broader neighbourhood and their consequences.

It is in this spirit that, we are publishing, as we did last year, not a recount of our «actions» during the period from September 2023 to October 2024, but a «Report on Priorities and Areas of Activity,» which we believe can provide the reader with a good understanding of what has concerned the Service over these twelve months, both inside and outside our country.

In a time of intensifying political and geostrategic challenges, ever-changing economic and social parameters, as well as of rapid technological and environmental developments that define a new reality, the need to safeguard National Security and shield the country against both longstanding and emerging threats is even more imperative. However, this also requires the best possible adaptation to new demands, with all that this entails in terms of structures, tools, and human resources. This will be the great challenge for the National Intelligence Service in the coming year.