



NATIONAL INTELLIGENCE SERVICE  
**ANNUAL REPORT**  
OF PRIORITIES AND KEY FIELDS OF ACTIVITY



September 2022 - August 2023

# INDEX

<b>Foreword by the Director-General</b>	3
<b>MAIN CHALLENGES AND DEVELOPMENTS AND NIS'S KEY FIELDS OF ACTIVITY OVER THE PAST YEAR</b>	
<b>A. A complex environment of multifaceted crises</b>	6
<b>B. Main threats and their origin</b>	7
1. External threats	7
2. Espionage activity	8
3. Terrorism and violent extremism	9
4. Illegal migration	10
5. Organized crime	11
6. Cyber security and new technologies	12
<b>C. Finding the right balance between security and civil rights</b>	13
<b>D. The Service's Evolution</b>	14
1. Structure and functions reform	14
2. Upgrading of personnel	15
3. Openness to society and improvement of the Service's image	16
<b>E. Preparing for the challenges of tomorrow</b>	16
<b>Epilogue</b>	18

## FOREWORD BY THE DIRECTOR-GENERAL

In August 2022, when the Prime Minister entrusted me with EYP's leadership, which, came at an, admittedly, difficult time for the Service, the objective set was crystal clear, targeting the improvement of the Service's operational performance, while reassessing, at the same time, the monitoring and oversight of its activities. Besides, the Prime Minister himself had just announced that changes were to be introduced with a view to render the Service more effective, modern, extroverted, with control mechanisms and high-level trained personnel.

During the past year, the new Leadership was fully aligned with these guidelines, having as a priority to enhance the Service's status and credibility and to ensure that its activities are carried out efficiently and in full compliance with democracy and rule of law principles.

In light of the above and in accordance with the Law 5002 that came into force in December 2022:

- a) An **Intelligence and Counter-Intelligence Academy** was introduced to provide contemporary and continuous training to EYP's personnel, as well as to employees of other governmental agencies;
- b) An **Internal Audit Unit** was formed to ensure that the entire organization operates in full compliance with legal requirements;
- c) A **Press and Communications Office** was set up to help the Agency become more extroverted and visible to the public for its role;
- d) Additional legal safeguards were defined for the waiving of communications privacy.

*At the same time, a reform of the Service's organizational structure is underway, which will allow a more effective intelligence gathering and information analysis, and the establishment of merit-based and transparent procedures of personnel's recruitment, promotion, transfer and appointment to positions of responsibility. Moreover, EYP has intensified efforts aiming at upgrading its technological capacities, which also include methods, means and measures associated with cyber security, thus consolidating its essential role in this crucial and rapidly evolving sector.*

*In the past year, EYP intensified its contacts with foreign partners, expanded its network both in Greece and abroad, and made rational use of its contacts, resources and means, being this way in a position to fulfil its mission and provide the competent authorities with intelligence, that enabled the implementation of appropriate measures to counter threats, protect national security, uphold democracy and fight crime.*


*Unveiling the presence and the modus operandi of a special genre of spies in Greece, thwarting terrorist activities against a specific group of Greek citizens and dismantling the network behind it, uncovering the way human smuggling networks and certain NGOs exploit the migrants' suffering -occasionally even deceiving the country's authorities and public opinion- are only a few of the Service's operations that garnered considerable public attention. Remarkable attention was also given to the Service's role in uncovering the aims and covert schemes of third countries in sensitive border regions, in detecting organized crime activity, and in better understanding the causes of the man-made disasters that hit Greece. EYP does not seek for credits for its work, since most of its operations are not made public, due to the nature of the Service. However, these are known on a need-to-know basis, to officials that are fully aware of the Service's vital role in protecting national security.*

*EYP's first-ever annual report of priorities and sectors of activities between September 2022 and August 2023, is an innovation and an endeavour to introduce the Service's work and its significant contribution to the current situation, as well as to make its role understood by officials, professionals and experts in the field, as well as for the broader public.*

*In many other countries with a similar democratic tradition, Intelligence Services are fully supported by the public and appreciated as an institution that is critical to the country's security and well-being. In Greece, however, because of a number of reasons associated with the country's turbulent history, marred by civil wars, military and authoritarian regimes, there is no denying that EYP has still a long way to go in order to bolster public perceptions of its work and to take the position it deserves as an institution serving the state and the people.*

*We expect that this publication, an initiative in the footsteps of many counterpart agencies abroad, will become a standard practice by annually announcing the priorities and outcomes of selected activities, providing this way useful information to institutions, officials and experts in the field of national security, in Greece and abroad, and primarily to the Greek people, who have the right to receive a picture, as clear and complete as possible, around the Service's crucial role in protecting their vital interests.*

The Director-General  
Themistoklis Demiris



# MAIN CHALLENGES AND DEVELOPMENTS AND NIS'S KEY FIELDS OF ACTIVITY OVER THE PAST YEAR

## A. A complex environment of multifaceted crises

Between September 2022 and August 2023, the international security environment remained complex, multifaceted with dynamic changes. The challenges that Greece has been facing, as a country with a distinctive recent history, a regional power, geographically located at the European external borders, a democratic state, under the rule of law, and a modern European country, are influenced by geostrategic factors, political, economic and social variables, religious and ideological rivalries, rapid technological developments, and environmental and climate parameters.

Our world is rapidly and dynamically changing and global challenges, such as the climate crisis, population displacements and pandemics, create conditions that profoundly affect almost the whole world. The rapid pace of technological innovation, the challenges posed by artificial intelligence, and the new dimensions offered by the Internet of Things, have transformed countries' needs and capabilities, their infrastructure resilience and, most of all, citizens' daily life.

Over the last years, our country has faced successive crises at various levels (economy, politics, security, climate, migration). There have been times that multiple crises were unfolding simultaneously; a notable one being the pandemic and the border crisis along the Evros River, in February-March 2020. Multiple crises reverberate on many sectors, including internal security.

Moreover, against the backdrop of a complex, interconnected and globalized world, the concept of hybrid threats is of paramount importance for all states. Intelligence Services play a key role in identifying, analysing, and dealing with this new type of threats that combine conventional and

unconventional tactics. These threats could challenge the national security on various fronts, from cyber-attacks and disinformation campaigns to proxy conflicts and economic coercion. Greece's geostrategic position, its political system and administrative structure, and the way its society and economy operate, make it an attractive target for this kind of threats.

EYP must maintain a complete understanding of emerging technologies, geopolitical shifts and strategies of state and non-state actors to adequately predict, assess and mitigate hybrid threats and attacks. This requires cross-border cooperation between flexible, interdisciplinary teams, since these threats transcend traditional borders. The Service has already embarked on the necessary work to achieve this aim. The successful tackling of hybrid threats is vital not only for the national security, but also to maintain stability and resilience in an increasingly complex landscape.

The new security challenges include inter-state tensions, ethnic and religious violence, terrorism, authoritarianism, human rights abuse, gender violence, and organized crime. Additionally, poverty and social exclusion, pandemics, energy insecurity, migration pressure, environmental degradation and climate crisis, as well as issues relating to cyberspace exacerbate the situation.

EYP, fully aware of the ever-increasing risks and challenges to the rules-based international order, has been promptly and constantly adapting to this wide range of challenges, by using all means at its disposal, in order to fulfil its national mission in the most effective way. Considering that many of these challenges have an international impact, EYP has been strengthening the cooperation with counterpart Services, constantly enhancing the already high acceptance of its work.

## **B.** Main threats and their origin

### **1.** External threats

In tandem with intensive diplomatic efforts to resolve bilateral issues, and promote peace and security across the wider region, our country needs to stay on high alert against external threats. Understanding the scope and the nature of these threats, as well as the tactics and the means related to them, remained the main priority on the Service's Agenda over the past year. In that regard, EYP has been providing regular and timely input to the competent authorities and the political leadership on the intelligence gathered and the findings of its investigations. Particular attention was given to sensitive border regions and policy areas, where third actors frequently carry out activities that undermine national policies, priorities and internal security, in order to serve their own interests, which pose a threat to the country's national security.

Main duty of our Service is also the consistent monitoring of the developments happening in countries with a crucial role, the exploration and analysis of intensions, and the detection of vulnerabilities related to the threat sources.

In this context, EYP has supported the work of the Government and the Prime Minister, as well as the mission of several governmental institutions (including the Foreign Ministry, the

Hellenic National Defence General Staff, the Hellenic Police, the Fire Service and the Coast Guard) by providing intelligence and accurate assessments of the current situation, decreasing this way the risk of any unwanted surprise. Furthermore, considerable and classified intelligence has been provided to national bodies and cooperating agencies to support the decision-making procedures around vital national interests.

Moreover, EYP made a significant contribution in countering specific external threats, neutralizing malicious activity, and disrupting shadowy practices and economic penetration in sensitive border regions. At the same time, the Service has regularly informed the Greek authorities about security risks emanating from using and installing IT equipment of suspicious origin, in critical national infrastructure, urging them to remain alert.

## 2. Espionage activities

Espionage and foreign agents' activities have become major security threats on a European level, reflecting global trends. The National Intelligence Service is fully aware of the inherent risks they included and the importance of effective and timely response to them, since if not confronted nor treated properly, they can undermine the national sovereignty and security, and the European cohesion as well. When hostile foreign actors attempt to gain access to crucial information relating to our country's defence capabilities, tactics and strategic goals, to potential vulnerabilities in critical infrastructure, to national economic priorities, and to technological capabilities in sensitive areas, we need to remain particularly vigilant and alert. EYP addressed these challenges, both by using its own networks and means and by cooperating with its European and international partners. Since the performance in this sector is mostly connected with prevention and deterrence, the earlier relevant operations are carried out the better. And of course, they should be carried out immediately when the threats occur, and without publicity.

However, one of the cases that attracted public attention is a typical example of how the effective use of various means and capabilities can disrupt espionage activities. Last spring, EYP uncovered the modus operandi and intrusion technique of a foreign spy infiltrated in the country under deep cover. The said case reveals the way foreign intelligence agencies think and operate, since they worked methodically for years, skilfully exploiting people, procedures and institutions, to build a fake identity. It is obvious that this spy's activity would not have been limited to Greece, but would have been expanded across Europe and beyond, where she would have been able to travel and operate easily and safely, using her Greek passport. This explains why this special case drew public attention and attracted the interest of many counterpart Services

Another interesting case is that one of a foreign national who had acquired Greek citizenship by submitting forged documents. Specifically, a Counterpart European Service informed EYP that the said individual had ties with foreign Intelligence Services. Therefore, EYP cooperated closely with the competent Greek authorities on this case and the result obtained was the revocation of the Greek citizenship.



### 3. Terrorism and violent extremism

Even though several terrorist groups, including ISIS, currently appear to have been dealt blows that have led them to curtail their operations or adapt their tactics, it is a fact that regional groups with links to them or other distinct terrorist organizations have emerged in their place and now operate in some of their former domains. At the same time, the “lone wolf” phenomenon has gained spread.

In any case, terrorism is still one of the major global and international challenges. The capabilities offered by the internet and social media platforms, the possibility of immediate action on the battlefield, and the expansion of terrorist radicalization and recruitment pool, have mobilized many people across the world and led them to join terrorist groups. Online jihadist propaganda has evolved and is now primarily waged through encrypted communication channels, several fora on the dark web, social media networks, and online gaming platforms.

Given that global terrorism remains a significant threat to international and domestic security, Greek authorities are constantly on alert. Greece's geographical location at the EU's external borders, and its geopolitical footprint, are additional reasons to remain vigilant, primarily because the country could become a transit point for suspected terrorists moving back and forth across conflict zones.

The extremist activities in Greece over the past decades were perpetrated both by far-left and anarchist groups, and by violent far-right extremists. These groups interact with and have ties to foreign extremist groups in Europe and other continents. There are also violent activist and extremist groups inspired by radical views, as well as by specific conspiracy theories, which gained traction during the COVID-19 pandemic, and frequently act against law and can even resort to violence.

Our Service cooperated closely with international partners and governmental agencies, acting both proactively and repressively, to combat terrorism and prevent the internal security from attacks.

In many cases, based on the intelligence gathered and forwarded to the competent services of the Hellenic Police, relating to preparatory actions for terrorist attacks, joint operations were launched in Athens and other cities across the country that led to arrests of foreign nationals. At the same time, EYP played a significant role in supporting and documenting the charges against foreign nationals for affiliation to a terrorist entity and participation in terrorist activities; after EYP tracked them down, the above-mentioned individuals were arrested by the Hellenic Police on terrorism charges and were sentenced accordingly.

With a view to preventing incidents that could be linked to international terrorism, the National Intelligence Service remains constantly vigilant to potential radicalization of individuals in migrant accommodation facilities, informal places of worship, correctional institutions and detention centres.

It is our Service's responsibility, in cooperation with national and international partners, to provide timely information on terrorists that could infiltrate through migrant flows, using the

Greek territory as a transit point to another European Country. In that regard, EYP monitors potential risks for national security and/or links to third countries connected with individual and/or group activities in migrant accommodation centers. Additionally, it provides useful insight on specific situations and risks in order to tackle such incidents and with a view to taking measures, which range from surveillance to deportation and/or relocation of distinct and/or organized groups to different facilities.

## 4. Illegal migration

The migration issue is perhaps the single greatest challenge the world is facing with today. The causes behind forced displacement are varied, whereas an array of different policies and means is required to control and manage migrant flows. It is a complex security web in which national and European security overlaps with human rights, with impacts stretching across many areas.

Following the dramatic rise in migrant arrivals over the past years, which culminated in the 2020 Evros border crisis, Greece saw a relative drop in illegal entries; however, at the end of the period concerned, the country once again experienced a surge in arrivals, with migrant flows across the Greek land and sea borders being on the rise, giving rise to financial and social issues and posing risks to national security. The instrumentalization of thousands of people seeking a better life, by ruthless traffickers and organized crime rings, whose actions are tolerated, encouraged or even abetted by third actors, be they state-sponsored or not, results in particularly challenging situations, with a broader social and profoundly human aspect, which require subtle handling on the basis of timely and valid findings.

The National Intelligence Service provided intelligence and assessments about this critical issue, to aid the timely management and tackling of migrant flows towards the Greek territory and mainly the islands of the Eastern Aegean and the Evros region, contributing in combating disinformation campaigns waged by foreign actors.

During the period under review in this report, the Service's work, based on its intelligence network and the thorough and discreet operational research conducted, has been instrumental to uncovering the truth, in cases that could mar the country's reputation, in dismantling transnational human trafficking networks, in mapping new migration routes, as well as in identifying and registering certain NGO's staff members who were engaging in controversial or even criminally punishable activities.

Besides these issues, which naturally fall within the Service's policy areas, other priority concerns which EYP focused its attention on over the past year are: attempts of terrorist infiltration into migrant populations, radicalization trends and the use of migrants for perpetrating destabilizing acts; cooperation with the competent Greek authorities and foreign services on these cases, was particularly effective.

The high-profile cases set out below illustrate, by way of indication, how the Service's decisive role contributed to the detection and investigation of several criminal offences:

- In November 2022, over the course of an information operation, it was revealed that

claims related to the alleged death of a young refugee girl stranded in the middle of the Evros river was in fact a fake story. Additionally, it was revealed that NGO members and associates played a key role in fabricating the false claims that made headlines at the time, with the ultimate goal to exert pressure on Greek authorities, in order to secure that the migrants would be rescued and granted asylum.

- In April 2023, the modus operandi of a human smuggling ring was exposed on the island of Lesbos. Our investigation revealed the tactics used to smuggle the migrants into the country and shed light on the traffickers' modus operandi. Based on this information, the Hellenic Police was able to initiate proceedings against 21 individuals, including the migrant traffickers and NGO members.
- In June 2023, following a thorough analysis of intelligence collected, our Service was able to dismantle a transnational migrant trafficking ring, whose members were operating in Turkey and used the island of Kos as a primary entry point into Greece. During the ensuing investigation, the members comprising the criminal ring were identified and arrested by the Greek Coast Guard.

## 5. Organized crime

Our policy agenda could not fail to include organized crime; this is a complex phenomenon which emerges, evolves and takes shape, constantly and rapidly adjusting to political and socio-economic conditions, which are in fact the ones that give rise to opportunities to pursue activities of low risk and high profit. Very Often, these activities also touch on issues of national security.

The most dangerous forms of organized crime in Greece are illegal migrant smuggling, drugs and weapons trade, smuggling of goods, human trafficking and activities of criminal groups that control certain industries, and are organized and operate in a mafia-like manner (forced prostitution, protection racket, extortions, kidnappings etc).

Apart from the aforementioned types of organized crime, corruption, money-laundering, crimes against property and the infiltration of criminal organizations into the country's legal economy are also regarded as especially significant.

The connection between organized crime and terrorism, along with its cross-border dimension, constitute crucial components of our interest. With the intelligence that our Service discovered, collected, cross-checked and utilized on the basis of its discernible expertise, it contributed significantly to the dismantlement of networks by the competent authorities and consequently, to the persecution of those involved in illegal activities. In the time period concerned, the activities our Service whose role is always to assist the competent authorities were effective and resulted in the solving of homicide cases, the detection and confiscation of large quantities of illegal cigarettes, the detection and seizure of military material and dual-use materials, the dismantlement of criminal networks, even networks specialized in illegal adoptions.

## 6. Cyber security and new technologies

The rapid development of technology, the possession and use of advanced tools by a growing number of actors who turn against or could potentially turn against our country's systems and infrastructures, thus deterring their smooth function and conducting activities which would ultimately threaten our national security, render it imperative to shield our country against such malicious activities. EYP has a key role in these efforts too, as it has been assigned relevant obligations through legislation.

During the past year, our Service was able to ascertain many such attacks and helped to successfully deter and confront them. At the same time, it makes sure to follow technological developments and to upgrade the means available to it, aiming to effectively confront not only cyber-attacks, but also activities threatening the smooth functioning of state institutions and the security of state officials' communications. The National Intelligence Service constitutes a crucial component of the country's cyber security. In particular:

As an INFOSEC authority, EYP is competent for compiling security policies and directives on how to manage classified intelligence and networks, it undertakes a coordinating role in protecting state institutions in every kind of relevant security incidents and is reinforcing its capabilities with technologies and advanced tools. Additionally, it provides advice, directives and technical support to Public Sector structures for the security of their communication and IT systems, while it edits policies on graded governmental systems, evaluates and certifies graded products for IT and communications. Within this framework, a large number of actions were taken in the time period concerned.

EYP systematically forwarded national contributions for the configuration of NATO's and the EU'S relevant agendas, compiled technical guidelines on the management and processing of classified intelligence by national structures, drew up guidelines for the safe use of computers in government structures and companies, while it conducted a series of inspections at critical infrastructures and forwarded the relevant, applicable technical specifications.

As a CRYPTO national authority, EYP, this past year, once again supported the Public Sector and the Armed Forces on crypto security issues and produced the national codes and safety keys, while at the same time, it published numerous security policies regarding the use of all kinds of crypto products, evaluated and certified crypto systems and produced national Military Security Editions, codes and safety keys for various crypto tools.

As a TEMPEST authority, EYP conducted inspections at critical infrastructures to ascertain if TEMPEST security measures were upheld and certified respective laboratories. It also supplied relevant technical know-how for the protection against electromagnetic and non-electromagnetic transmission leakages from IT systems, reinforcing the security of the country's sensitive data and communications, in numerous Ministries and Precincts.

As a CERT national authority EYP played a crucial role, providing prevention, timely warning and confronting cyber-attacks against Public Sector structures. It compiled dozens of technical analyses on incidents in the Greek cyber space, regarding DDOS, Phishing E-mail, Malware, Data Breach, Defacement, Ransomware, DNS hijacking, Suspicious traffic and

breaching of electronic infrastructures, while at the same time, it published a series of Vulnerability Assessments on websites and the applications of public structures.

Finally, all these actions will be now supplemented and improved by the impending operation of the Security Operation Centre – SOC, which will constitute a significant tool for the fortification of cyber space security and the state's protection against cyber-attacks, thus upgrading the country's position in Cyber space and supplying it with technologies and advanced tools, corresponding to international standards.

## C. Finding the right balance between security and civil rights

Intelligence Services play a decisive role in protecting national security and defending the rule of law, while at the same time they contribute to the work of the Law Enforcement Authorities. To this end, it is necessary that the security strategy developed and applied is based on the utter respect of civil rights and fundamental liberties, aiming to be fully compatible with law while at the same time, effective and viable. The Service not only continuously tried so that the above-mentioned aims were not in conflict, but on the contrary, that they support each other.

The security and respect of fundamental rights must not collide with one other. On the contrary they must go hand in hand and be mutually supportive to each other. The values and fundamental rights of Greek citizens must constitute the base of security policies, so as to consolidate all necessary provisions for transparency and accountability, aiming to fully protect all citizens.

Within this framework, by Law 5002/2022, "Procedures of confidentiality communication waivers, cyber security and protection of citizens' personal data", innovative and effective regulations were modulated, with strict guarantees and provisions for the overall operation of the National Intelligence Service.

More specifically, special requirements were introduced for the selection of Director General, who can now be, exclusively, a diplomat or a high-ranking official. At the same time, the hearing, as well as the opinion for his/her appointment by the Transparency Committee of the Greek Parliament, was established.

Additionally, the framework for confidentiality communication waivers was made stricter, with the procedure involving now two (2) high ranking Prosecutors, while the term "national security" was legislatively determined. As "reasons of national security" are described now the reasons referred to the protection of the basic functions of the state and the basic interests of Greek citizens, especially reasons related to national defence, external policy, energy security and cyber security.

What is more, especially for the communication waivers relating to political figures, it is now demanded that a direct and extremely possible risk against national security must be ascertained and additionally, permission must be granted by the President of Parliament, while after three years, the citizen may request to be notified on the restraining order (communication waiver on national security grounds), providing that the reason for which it

was imposed, is not jeopardized.

Finally, the distribution of surveillance hardware and devices was prohibited, while their use by civilians has been converted into a felony, while simple possession and trafficking are characterized as misdemeanours. Additionally, malware and surveillance devices are recorded in a special catalogue, while the provision of surveillance hardware by the Public Sector and the terms of its use will be only allowed through the introduction of the relevant legislation.

## **D.** The Service's Evolution

### **1. Structure and functions reform**

It is adamant that the structures and functions of an Intelligence Service correspond to the needs and challenges of our times, adapting to ascertainties and conclusions from its activities and performance. This is the reason why the Administration's basic priority during the time period concerned, was the recording of weaknesses and the assumption of initiatives to tackle them. Within this framework, the Service's organizational modernization is already under way, with the creation of new internal structures, as well as structural functioning changes of existing ones, through the induction of innovative procedures on an operational level, adoption of modern standards for the functioning of the Service, as well as digital and administrative upgrading. The aim is to place the human factor -its personnel- in the epicentre.

To the direction described above, there was a change in the number (from three to two) of Deputy Director Generals but also to their appositeness'. They received the portfolios of Foreign Affairs and Internal Security correspondingly, thus strengthening EYP's function and operational upgrading, as well as its distinct dual role, as EYP is a Service which is active both in the sectors of Intelligence and Security, its mission focusing in external, as well as internal threats.

What is more, Liaisons have been appointed in selected capitals abroad for the promotion of cooperation in the sector of intelligence, as well as for acquiring a better knowledge of countries of interest. At the same time, a program for upgrading its presence in the Greek territory has already been applied for EYP's more efficient operation.

All structural changes are depicted in a Presidential Decree draft which describes the restructuring and which has already been appropriately processed. Once it is signed and published, the foundation will be set for a new, contemporary Intelligence Service, always in the duty of the country's national security, better adapted to today's needs.

Finally, the effort to upgrade the technological capabilities and information systems of both the Central Service and our stations across the country, was also constant aiming to exploit the capabilities of technology, in order to collect and cross-check intelligence -in the best possible way-, through the use of innovative methods and means, often

invented by us. The fixed aim is the timelier and more effective collection of data, the safest possible communications and the best utilization of cooperation capabilities with all services, cooperation with us, to which we often offer EYP's know-how.

## 2. Upgrading of personnel

These significant changes, taking place both abroad and within the country's geopolitical, social and economic environment, render the need for training, imperative. Technological development, contemporary demands, the necessary redesigning of functions and organizational structures, all call for new, specialized expertise, new knowledge and the adoption of new methods and procedures for executing our mission.

The personnel of EYP, as is the case with every other Organization, are the main means for us to function effectively. Its development, training and best possible utilization was a fixed aim of the Administration in the time period examined. A series of initiatives have already been taken, while more have been planned and are gradually adopted, aiming at constantly improving the training and performance of all personnel, so that they are as best as possible prepared to deal with the challenges a contemporary Service has to face. At the same time, the personnel is constantly participating in selected training courses organized by foreign Intelligence Services, with special emphasis on hybrid threats, cyber-espionage, tracing and elimination of inside threats, influence operations and social mechanics, counter-terrorism strategies, among others.

Equally important though, is the training that EYP provides to foreign Intelligence Services, through which its own personnel also acquire valuable experience.

Additionally, the Service, responding to developments, adopted a contemporary philosophy and a new model for the training of its personnel, through an emblematic initiative towards this goal, the establishment of an Intelligence and Counter-Espionage Academy. After all the complete scientific and professional training of personnel and the preservation of already acquired knowledge, contributes to the effective execution of their mission.

Further to the aforementioned planning, EYP, in cooperation with the academic community and foreign Intelligence Services, and taking into consideration the continuous development of its personnel, provided training courses to selected personnel of other national bodies.

However, one should not underestimate and the efforts already made and which continue to be made, not only for personnel health, but also for the improvement of working conditions, aiming to accommodate their work, create a feeling of collectiveness and finally, improve their quality of life. Within this framework the establishment of a series of infrastructures and installations at the disposal of our staff were of great importance.

### 3. Openness to society and improvement of the Service's image

One of our main goals during the time period concerned was the recognition and understanding by the wider society, of our Service's national mission. It was important, especially when a preceding crisis undermined its credibility and the public's trust, to try and strengthen the Service's credibility and to improve its image. Within this framework, particular emphasis was given to principles such as administration transparency, accountability and extroversion, adjusted of course to EYP's role and specificity.

For the reinforcement of extroversion and projection of EYP's role, with the aim to ensure public trust and to inform society about national security issues, we planned and started to operate a Press and Communications Bureau. This Bureau, among other things, is competent for the promotion of the Service's mission, for informing the public of its activities and the risks against national security. Although its operation has to be adjusted to the Service's "particularity", this Bureau has already shown tangible results, as proven by the coverage of issues which are within EYP's interest and competence framework, by the media. It was on these same lines, that the annual report was introduced.

The planning for the operation of a visitor/museum centre will also prove to be of significant importance. This centre will inform the public about our Service's historical background and its mission, thus making the visitors and the public in general, more sensitive against the critical issues this Service is dealing with. Relevant contacts and works are already under way.

We are hoping that the scheduled appropriate utilization of EYP's archives will have a similar impact.

In order to strengthen meritocracy, to establish and maintain a sense of justice as well as to promote accountability and transparency, it is expected that the operation -for which the procedures are already under way- of the Internal Control Unit, will act as a catalyst. The operation of an internal control mechanism will constitute a useful tool, which apart from investigating possible reprehensible behaviours, will decisively contribute to the timely detection of security vacuums, to the improvement of procedures and the limitation or avoidance of bad actions or omissions, which could prove to deter the Service's proper operation. Internal control will constitute an independent, objective and irreproachable function, which will help strengthen and protect EYP's authority and prestige.

## E. Preparing for the challenges of tomorrow

In a world constantly and dynamically changing, EYP's primary duty is its continuous preparation and adaptation to the agenda of coming crisis in the future, as well as the best preparation possible against arising new threats from the use of technological products, which may in any way, threaten critical infrastructures.



The Service is searching for the best ways and requirements in order to participate in a system for the effective fight against such crises and the coordination of respective actions, carefully studying all possibilities for utilizing new technologies, as well as financing tools. A decisive role in this sector has been played by the Centre of Technological Support, Development and Innovation, which constitutes a distinct department within our Service and has acquired significant experience in the best possible utilization of European funds, as well as in conducting applied research in the field of national security protection.

One of the most significant challenges of today and tomorrow is the climate crisis which may lead to international and internal conflicts or even contribute to the escalation of existing ones. The climate crisis is expected to hit the wider Mediterranean region and by extension, Greece, in various ways. The most severe long-term damage will be the desertification of that large regions. This will affect water reserves, tourism, agricultural production and the quality of living in general.

The thorough examination of climate change as a multiplying factor for destabilization and the worsening of the security situation in some geographical regions, attract the attention of Intelligence Services all over the world, as well as of international organizations. EYP has its own role in investigating the phenomenon of climate change, mainly in connection to the security environment.

Within this framework, the Service is already doing research, focusing on the development of other existing threats, as well as of those which may arise, as a result of the climate crisis. Based on the conclusions drawn from this research, there is cooperation with competent foreign Services, aiming to jointly prevent and confront the phenomena resulting by the climate crisis and which may prove to be destabilizing factors for both national and international security.

As far as the new threats are concerned, our Service has a specific interest on events which may constitute security threats, deriving from the use of technological products and the installation of surveillance systems in critical infrastructures. We also have to deal with new internet portals that may be created, through which targeted cyber-attacks may be executed. Additionally, this sector includes chemical, biological, radiological and nuclear threats (CBRN), which constitute significant threats against the modern world.

Identifying and confronting inside threats constitutes another challenge, which relates to individuals or groups of individuals with access to sensitive national resources data, graded intelligence or critical infrastructures and who intentionally act against our country's interests. The importance of these threats must not be underestimated, as they may cause leakage of state secrets or derange important services which are critical for the country's operation. Confronting inside threats constitutes one of our primary priorities in order to ensure our country's security and sovereignty.

It's needless to say that various investing activities are also challenging -and demand vigilance- for national security, especially when they relate to critical infrastructures, as well as programs which -under specific conditions- provide privileges relating to entry and stay in our country.

Besides “classic” threats against internal security, topics of the future crises’ agenda, focus on a wide spectrum of problems which may be deriving from the political, economic and social instability of Greece’s neighbouring environment, as well as internally. Therefore, it is essential to have a crisis management system and to determine updated coordination procedures of operational centres, based on the logic of holistic management. The training of competent personnel, the integration of technical know-how, the achievement of disciplinary cooperation between competent authorities, as well as international cooperation with the aim to confront, as best as possible, not only traditional, but also contemporary threats, are all expected to prove crucial. It is EYP’s duty to use all means and capabilities towards this end.

## EPILOGUE

The above report of EYP’s activity in several fields is selective, due to the nature and work of the Service. It is widely known and well documented during the time period examined by this report and even recently, that mistakes and failures of Intelligence and Security Services around the world, are excessively covered and presented by the media and, justifiably, attract public attention. On the contrary, the activities and the successes of all Intelligence Services, as their operation are mainly preventive, are usually disclosed only to those who need-to-know, even when their consequences affect us all.

Although this report’s language has, for obvious reasons to be selective, without providing details around main sectors of action and priorities, we hope that its publication will help the public realize the importance of national security, the large spectrum of contemporary threats, and the need for preparedness and resilience to them. EYP is determined to contribute to this aim using all its tools and means.