

**RIEAS Copyright @ 7 February 2021 ([www.rieas.gr](http://www.rieas.gr)) Athens, Greece.**



***Strategic Report***

**"The role of Intelligence Services in shaping the Greek National Security Policy in the Information Age"**

**Dionysios Dragonas**

*(Postgraduate Student, MSc Crisis and Security Management, Leiden University, the Netherlands & RIEAS Senior Analyst)*

**RIEAS E-Publication**

*February 2021*

**ISSN: 2241-6358**

## **A. Preface**

Thomas Jefferson once said that “information is the currency of democracy”. But what happens when the currency is misshaped, manipulated and dubious enough to lead to its denial? Is this when democracy collapses? This is not the case when powerful allies exist, within the spectrum of the public sphere, remaining vigilant and confronting challenges invisible to the public eye. For decades national intelligence services have incarnated a crucial role in assisting leaders to acquire and utilize information that reassures the survival of the State, by protecting it against all threats, foreign and domestic (Stout & Warner, 2018).

The paper at hand takes a closer look to the perils brought about by the Information Age, revisiting its impact to national intelligence apparatus at first, and consequently to national security. The discussion is put into context via the deployment of the Hellenic Intelligence Community (IC) case study, focal point of which is the National Intelligence Service (NIS). The selected case study is chronologically confined to the last three decades (21<sup>st</sup> century onwards).

The theoretical background used to map the characteristics of Information Age is provided by Marcos Degaut, while several definitions provided by esteemed authors are borrowed to complete the mosaic of the digital era. The development of the case study lays its foundations on publications provided by Apostolidis, Nomikos and Liaropoulos. The recommendations section corresponds to the personal opinion of the author of the paper at hand.

## **B. The intertwined nature of intelligence and National Security in the Information Age**

Marching into the third decade of the 21<sup>st</sup> century, information establishes itself as the most impactful product of the increasing interconnectedness provided by the continuous developments in the use and application of information and communications technologies (ICTs). Part of this process is known to the academic

discourse as Information Revolution (IR), which is better understood with Teitelbaun's working definition of the *'ongoing social, political, and economic change brought about by technological advances in computing and telecommunications'* (Teitelbaun, 2004, p. 80). This change has proven powerful enough to have transformed developed nations from industrial to information-based societies. To put the latter into context, *"pieces of data have become the building blocks of many modes of human interaction and activity"* (Copeland, 2000, p. 2), marking a social penetration that allows to speak for a "network society" (Maniscalco, 2012, p. 13) that revolves around the dictations of technological advancements. Economic development, human interaction, education, politics, entertainment and trade are just a few of the areas IR has revolutionized (Degaut, 2016).

These advances and improvements do not come without setbacks, however. Rival governments, criminal organizations, terrorist groups and individuals find breeding ground in the IR era, to engage into new kinds of activities, opposed to global security and national interests. The 'new threat environment' as described by Degaut (2016, p. 510), is defined by accelerating change, deep complexity and constant uncertainty. Under these circumstances, the national intelligence services are tasked to monitor threats that are more dynamic, diverse and interconnected than ever before. The vast influx of information has rendered the intelligence collection an extremely challenging endeavor. According to Liaropoulos, *"the Information Revolution affects every step of the intelligence cycle; it adds new issues in the intelligence agenda, alters old ones and brings profound organizational and cultural changes in the art of intelligence"* (Liaropoulos, 2006, p. 7). The Intelligence Community (IC) needs to adapt to the new environment, which, according to Degaut, is defined by four traits: interactivity, speed, proliferation and feedback.

Interactivity captures the generation of unintended consequences from ostensibly isolated events, often unpredictable. Everything that takes place in the real world creates an immediate impact on the Web, mirroring the impact back to society. Specifically, through the Web, actors are instantly notified for the actions and intentions

of other actors, resulting in the emergence of an unpredictable and complex system of interactions. The Arab Spring is a textbook example of this feature, given that the unleashed domino effect from the Tunisian riot caused the direct overthrow of governments throughout Maghreb, leading to the destabilization of the wider region (Maniscalco, 2012, p. 14).

Speed is one of the most significant features. Policymakers have to act in a timely manner, adopting a proactive approach towards real time events. Speed affects all the other traits and constitutes a multiplier of interactivity, as virtual real-time communications increase the impact of IR, hence generating interactivity in much shorter time intervals (Degaut, 2016, p. 516).

Proliferation corresponds to the emergence of new and unfamiliar actors in international relations. The State does not have the monopoly of threat towards global security or other nations anymore. Multilateral institutions, international business, think-tanks, NGOs, criminal organizations, terrorist and interest groups are, among others, potential source of threat to national security. For instance, during the second decade of the 21<sup>st</sup> century, the Islamic State (IS) undertook sophisticated social media campaigns, spreading their ideology, fostering support for their cause, expanding their network, communicating and plotting terrorist attacks throughout the globe (Weimann, 2010).

Feedback, being the fourth characteristic, results from the flow of accurate information delivered to policymakers via both traditional and information age channels. Namely, the IC is called upon to outperform the new age information brokers or utilize them to provide legitimate intelligence products. The vast amount of Open-Source Intelligence (OSINT) deriving from mass media and social media platforms challenge the credibility of the monopoly of intelligence provided by the IC. Traditional methods of collection, analysis and dissemination may render intelligence obsolete, damaging the ability to inform policymakers. The IC has to adapt to the dynamics of the competitive and complex information environment and provide comprehensive, timely, accurate, adequate and reliable intelligence to policymakers (Degaut, 2016, pp. 518-525)

Degaut's theory vividly demonstrates that the maintenance of capable intelligence agencies holds the key to national security within the fluid environment of information age, where change is the only constant. The paper continues by examining the case study of the Hellenic Intelligence Community, emphasizing on the role of the National Intelligence Service (NIS) within the context of the information era.

### **C. Revisiting the 21<sup>st</sup> Century Hellenic Intelligence Apparatus**

The NIS constitutes the only autonomous intelligence agency in Greece, responsible for the collection of both internal and external intelligence. The Military Intelligence Bureau of the three-armed forces (Army, Air Force, and Navy) focuses on the collection of external intelligence. The Ministry of Foreign Affairs (MFA) collects external intelligence through overt action.

Internal intelligence is a responsibility of the Hellenic Police (HP), alongside the NIS. The Antiterrorist Branch of the HP collects terrorist affiliated intelligence, while the Second Bureau of the Coast Guard gathers intelligence related to its competencies (Apostolidis, 2007).

Steering the focus towards the cornerstone of the Hellenic IC, namely the NIS, it is imperative to note that since the conception of NIS in 1926 (Nomikos, 2004) up until the present day, there has not been an open debate regarding the kind of Intelligence Service that Greece needs. The NIS, despite the plethora of reforms that has undergone throughout the past decades, upholds responsibility for the collection of both internal (counter-espionage, counter-terrorism) and external intelligence collection (political and military). This broad scope renders NIS's duty nearly impossible to carry out, let alone efficiently and effectively (Nomikos, 2004).

Furthermore, the NIS's Intelligence Cycle is indicative to the weak institutional environment surrounding the Service. As far as orientations are concerned, given the inadequacy of the Greek public sector planning, the NIS does not operate under specific time frame orientations provided by its clients. Orientations and goals on major issues are debated and decided in planning meetings with the Ministries of Foreign Affairs,

Internal Affairs and National Defence, where the NIS is present. According to the former Director of the NIS, Pavlos Apostolidis, human intelligence (HUMINT) processing procedures are in need of improvement in order to unlock the full potential of human sources and their handlers. The NIS managed to digitalize its files in early 2000s, minimizing past practices of employees who claimed property over files and carried them off Service or destroyed them. Apostolidis stresses the importance of the establishment of two distinct branches comprised of analysts and field agents respectively. However, these officers should not be chosen with political criteria, deemed to serve for a limited period and waste the acquired knowledge and expertise (Apostolidis, 2007). When it comes to distribution, the NIS delivers intelligence to the policymakers in an official level and only in exceptional cases in a political one. This way intelligence is better protected, while its identity remains hidden as officials absorb it and present it as their own. That being said, Apostolidis suggests that *“a clear distinction between specific intelligence needed at the official level and analyses or estimates which must be addressed to Ministers is perhaps in order”* (Apostolidis, 2007, pp. 19-20) contributing to a better understanding regarding the needs of NIS’s clients.

On the whole, for relatively small states, like Greece, it is extremely challenging to uphold efficient Intelligence Services. A surgical balance between qualified personnel, sufficient resources, government interest and political oversight is hard to achieve and even harder to maintain. Greece, in contrast with most European states, has adopted the more challenging concept of a single Service, relying on the NIS for both internal and external intelligence. Whether this model was chosen because it suits the country’s needs or because of cost-efficiency remains questionable.

#### **D. Chronic Inadequacies and Inefficiencies: The case of NIS**

Taking the abovementioned into consideration, it does not come as a surprise that the NIS has not lived up to its expectations. From the 1986 restructuring which marked NIS’s establishment as a self-standing civil public agency (Nomikos, 2004), the Service counts more failures than successes. Among the most striking intelligence failure

examples of the post-Cold War era, as summed up by Nomikos and Liaropoulos (2010), one may find the Öcalan Affair (1999), the assassination of the British defence attaché Stephen Saunders (2000), the ‘telephone tapping’ (2004-2005) and the ‘Pakistani Affair’ (2005). On the contrary, the NIS is accredited for the dismantlement of the ‘17 November’ terrorist group (2002) and the successful host of the 2004 Olympic Games. It is important to note that the aforementioned cases do not constitute a scoreboard for the assessment of the role of the NIS over the past three decades. It is rather a timeline that explains the two attempts for an intelligence reform that took place in 2002 and 2008 respectively.

The 2002 reform suggestion was brought about as a response to the back-to-back failures of the Öcalan affair and the Saunders assassination. It came in a time when the NIS was sidelined by the Hellenic Police (HP) in the combat against domestic terrorism. The focal point of the reform revolved around the broadening of the NIS agenda, including organized crime, illegal immigration and drug trafficking, areas formerly controlled by the HP. The new operational framework was reinforced by augmented electronic surveillance capabilities, while civilian personnel was increased at the expense of police and military staff. Last but not least, the NIS became accountable to the Hellenic Parliament, compelled to submit an annual report of activities, increasing oversight and institutional transparency (Nomikos & Liaropoulos, 2010).

The first reform attempt, although it marked a step to the right direction, it was no more than a ‘tip of the iceberg’ approach. The understaffed and ill-equipped NIS was not ready to undertake such a broad scope of responsibilities, let alone elevating to an all-purpose service dealing with internal and external threats. Admittedly, the Service made its first steps towards the digital era, however the reform proposals were shallow at best and did not promote a meaningful structural reform that would improve the Service’s capacity and capabilities. According to Nomikos and Liaropoulos, the 2002 reform can be characterized as a rushed response to external pressures for the increase of the effectiveness of the security apparatus in view of the 2004 Olympics (Nomikos & Liaropoulos, 2010).

The 2008 reform bill laid the ground for a deeper and more meaningful reform. Among the most important proposals one may find the establishment of a Sub-Directorate for Organized Crime and Terrorism, the creation of a training Directorate, the establishment of a cyber-defense unit in cooperation with the HP, the creation of a “Mini-National Security Council” (Nomikos & Liaropoulos, 2010, p. 36) within the NIS charged with filtering the information flow from Ministries that comprise the national security apparatus, the cooperation with scientific organizations and the augmentation of international cooperation.

Verily, the designated proposals carried a lot of promise for the realization of a comprehensive reform that would render the NIS competitive and competent on the threshold of the IR era. Although, the rhetoric was not accompanied by the necessary political will to carry out tangible changes. The NIS remained in the sidelines, while the burst of the 2007 financial crisis deprioritized the concept of a holistic revision within the IC. All the more, intelligence collection suffered a deep fragmentation and a lack of sharing and cooperation among the parties involved. The Hellenic Police, the Hellenic Coast Guard, the NIS and the Military Intelligence single-handedly collect and manage intelligence leading to a “*bureaucratic infighting*” (Nomikos & Liaropoulos, 2010, p. 37) damaging the Hellenic security apparatus.

Overall, it would not be an overstatement to admit that the NIS has long been a prey for its precarious entourage consisting of political instability, party cycles and petty partisan politics. Despite the initial rhetoric and appearing will, the NIS always ended up subordinating to cabinet of ministries, leading to the lack of continuity and the inability to perform its role as an independent and reliable intelligence service. Needless to say, the positive impact of the two reforms was minimal, given that the NIS, while being the flagship of the Hellenic IC, still lacks strategic vision.

### **E. Recommendations**

After having laid out the ugly truth regarding the evolutionary trajectory of the Hellenic IC, and specifically the NIS, in the 21<sup>st</sup> century, it is important to elevate the conversation in today's context.

Greece, as a developed industrialized nation, does not escape the tendency of leaning towards an information-based society. Simultaneously, its active presence both in the European Union (EU) and the North Atlantic Treaty Organization (NATO), demands an increased level of “*management efficiency, effectiveness, economy, and employment criteria*” (Nomikos, 2004, p. 436). Within the information age environment, the Hellenic IC is called upon to master the abovementioned challenges and uphold its role as a reliable intelligence provider to the decision-makers. The following recommendations are classified into four distinct categories, corresponding to the four characteristics of the information age, according to Degaut.

#### ***Interactivity***

Adapting to interactivity falls under the category of personnel requirements. In the modern day, analysts must familiarize themselves with the concept of non-linearity by anticipating discontinuous change. To support decision-makers, analysts must hone practical, qualitative techniques to deal with the dynamics of Complex Adaptive Systems (ex. Arab Spring). The interconnectedness of modern societies calls for a systemic approach against every threat, or else the analysis enters the threshold of reductionism and oversimplification. This endeavor requires the assemblage of a group of experts who are able to cut across traditional organizational lines, monitor the complex systems that are related to national interests, report on the behavior of the actors involved, identify trends, track and fill information gaps, constantly reassess dynamics among systemic variables and update the officials with analytic reports on the possible future scenarios. This ‘synthesis’ constitutes an antidote to interactivity, ensuring the pro-activeness of the Intelligence Services and the State as a whole.

### *Speed*

Interoperability and jointness emerges as the key to respond in a timely manner to the rapidness of information age threats. In order to achieve this, all the intelligence actors of the IC, namely the NIS, the HP, Military Intelligence and the Coast Guard, must agree upon a single alphabet on intelligence cooperation and sharing practices. The ultimate goal is the mitigation of unwanted competitiveness and the smooth cross-sectoral flow of intelligence.

### *Proliferation*

The optimal route to deal with the proliferation of threats is to embrace the proliferation of available means. Universities, scholars, institutes and think tanks or even media must be perceived as repository of knowledge available to Intelligence Services. Information is no longer a privilege, it is a common good which is being successfully used by a plethora of institutions or individuals outside of the IC. The latter has to defy its institutional rigidities and filter the voices that wish to contribute to a fruitful dialogue regarding the future of the IC in Greece.

Proliferation does not limit itself to the existing means. Via the continuous education and training Greece can create a plethora of young professionals able to correspond to the highest of standards set by the Service. Mirroring to Nomikos's proposal, the establishment of an Intelligence Academy (Nomikos, 2020), staffed by intelligence experts can create a valuable repository of analysts and field agents representing a hopeful future for the Hellenic IC.

### *Feedback*

There is a dire need for a reset in the relation among the IC and national authorities. The most efficient approach to achieving this, it is via the revival of a stronger NIS, as an organization "umbrella" under the auspices of which internal and external intelligence dynamics are scrutinized. The greatest challenge in this endeavor would be for the NIS to regain governmental trust. Simultaneously, government officials must invest in the power of a strong, unified Intelligence Community under the NIS. It may

sound as a wishful thinking, but the problem is there, and it is one of organizational nature. Clientelism and party cycles have obliterated the trust of the public sphere to the NIS. The element of distrust towards the NIS is deeply rooted to the public perception. It is important for officials to grasp that a useful Intelligence Service is the most powerful ally to have in the era of Information Revolution.

A far-fetched proposal that could renew interest in a truly groundbreaking reform of the NIS, would be its establishment under the auspices of the Highest Authority, namely the Presidency of the Hellenic Republic. In this regard, the staffing and oversight of the NIS would carry less political burden, while the Service may no longer be susceptible to short-term political agendas.

#### **F. Epilogue**

Arguably, the NIS is the last to blame for its failures. From the author's standpoint, "*it is pointless to get your hands on a tool that you have not decided how to use it*" and the NIS is a too powerful tool to discard. All the reforms in the world would be in vain unless an open debate regarding the actual role and the strategic vision of the NIS takes place.

In conclusion, the increased interconnectedness of threats (disinformation, terrorism, political violence, transnational crime, illegal migration, human trafficking, environmental degradation, pandemic etc.) blurs the distinction between internal and external security nexus, calling for a holistic intelligence approach to serve as the backbone of the Hellenic National Security Apparatus. The NIS, if invested with the necessary political capital, has the potential to become the 'umbrella' organization that orchestrates the intelligence policy among legislative and executive branches, Military, Police, Coast Guard as well as not traditional intelligence sources such as mass media, think tanks and the academia.

## **Bibliography**

Apostolidis, P. (2007), *Intelligence services in the national security system: The case of EYP*, ELIAMEP Occasional Paper, 7(3). Athens: Hellenic Foundation for European & Foreign Policy, pp. 1-22

Copeland, T. (2000), *The Information Revolution and National Security* (Carlisle, PA: Strategic Studies Institute, US Army War College 2000)

Degaut, M. (2016), *Spies and Policymakers: Intelligence in the Information Age*, *Intelligence and National Security*, 31:4, pp. 509-531

Liaropoulos, A. N. (2006), *A (R)evolution in Intelligence Affairs? In Search of a New Paradigm*, Research Institute for European and American Studies, Athens, Greece, Research Paper N. 100, pp. 1-19

Maniscalco, L. M. (2012), *Living in the Cyber Era: Reflections on Security in a Hybrid World*, Mediterranean Council for Intelligence Studies Yearbook

Nomikos, J. M. & Liaropoulos, A. N. (2010), *Truly Reforming or Just Responding to Failures? Lessons Learned from the Modernisation of the Greek National Intelligence Service*, *Journal of Policing, Intelligence and Counter Terrorism*. Volume 5, Number 1, pp. 28-41

Nomikos, J. M. (2004), *The Internal Modernization of the Greek Intelligence Service (NIS-EYP)*, *International Journal of Intelligence and CounterIntelligence*, 17:3, pp. 435-448

Nomikos, J. M. (2020), *Modernizing the Greek Intelligence Service (NIS-EYP): An uphill battle*, Research Institute for European and American Studies, Publication date: 31 May 2020

Stout, M. & Warner, M. (2018), *Intelligence is as intelligence does*, *Intelligence and National Security*, 33:4, pp. 517-526

Teitelbaun, L. (2004), *The Impact of the Information Revolution on Policymakers' Use of Intelligence Analysis* (Santa Monica, CA: Rand Corporation)

Weimann, G. (2010), *Terrorist Facebook: Terrorists and Online Social Networking*, in M. Last and A. Kandel (eds.) *Web Intelligence and Security* (Amsterdam: IOS Press), pp.19–29

## **RIEAS E-Publication**

***February 2021***

**ISSN: 2241-6358**