John M. Nomikos
DOI:10.33179/BSV.99.SVI.11.CMC.22.3.6

ASIMETRIČNE GROŽNJE V GRČIJI: DESKRIPTIVNA ANALIZA

ASYMMETRIC WARFARE THREATS IN GREECE: A DESCRIPTIVE ANALYSIS

Povzetek Eden največjih izzivov današnjega časa je naraščanje asimetričnih groženj. Nato in EU sta tarči politično motiviranih nedržavnih in razvitejših državnih akterjev ter združenj, ki se ukvarjajo s kibernetskim kriminalom. Sovražna kibernetska kazniva dejanja spodkopavajo vse družbene ravni v državah Nata in EU ter ogrožajo politično, gospodarsko, civilno in vojaško varnost. S podobnimi grožnjami se spoprijema tudi Grčija. V članku so preučeni grška strategija kibernetske varnosti ter vzroki in posledice organiziranih terorističnih združb za nezakonite migracije v Grčiji. Prav tako je izpostavljen pomen izmenjave obveščevalnih podatkov med grško varnostno in obveščevalno skupnostjo.

Ključne besede ***Grčija, asimetrično bojevanje, kibernetska varnost, trgovina z ljudmi, migracije.***

Abstract One of the biggest challenges of our time is the rise of asymmetric warfare threats. NATO and the EU are targeted by cybercrime syndicates, politically motivated non-state actors, and sophisticated state actors. Hostile cybercrime undermines all levels of society in NATO and the EU states, threatening political, economic, civil, and military security. Greece faces similar threats. This article focuses on the Greek cybersecurity strategy and analyses the causes and consequences of the terrorism-organized, illegal immigration nexus in Greece, and how essential it is to highlight the importance of collective intelligence sharing among the Greek security and intelligence community.

Key words ***Greece, asymmetric warfare, cyber-security, human trafficking, migration.***

Introduction

As the security and intelligence community inexorably works its way into the 21st century, it faces an unprecedented time of challenges (Nomikos, 2014). The chaotic world environment of the post-Cold War (the Arab Spring, Syria, the Libya crises, the Iran nuclear issue, illegal immigration, human trafficking, Islamic radicalization, money laundering and transnational organized crime) covers a wide range of different issues to be understood, and a variety of new threats (e.g. biological viruses) to be anticipated. The rapidly developing information age presents advanced and complex information technology and methodologies to be mastered and integrated to make cyber-security and Human Intelligence (HUMINT) more efficient in combating terrorist incidents on critical infrastructure in Greek society (Nomikos, 2018).

In 2020 the coronavirus Covid-19 entered our vocabulary with a passion and the devastating power of a galactic big bang (Symeonides, 2020). As we speak, the impact of the pandemic is upending government policies, international and domestic economic relations, defence and world health policies, public confidence in those who rule, and the established states themselves. Inevitably, the "post-pandemic" world will be changed to its core.

Greece is located in the Balkan and Mediterranean region and is an active member of the EU and NATO. Today, one of the biggest challenges for Greece is to modernize its intelligence community and its cyber-security public institutional framework to efficiently confront cyber-attacks.

It is in this context that the present policymaking article highlights the asymmetric warfare threats that Greece now faces. The article emphasizes the problems and prospects of Greek HUMINT, cyber-defence, and the strategic significance of intelligence sharing cooperation between the Greek Intelligence Service (NIS-EYP), the law enforcement anti-terrorism squad (EKAM), military intelligence, and the coastguard counter-terrorism units. The article concludes that collective action is the most important tool for the security and intelligence community, depending on shared intelligence and joint assessment to prevent prospective major terrorist acts in Greek society.

1 GREEK CYBER SECURITY: PREVENTION AND RESILIENCE

In 1999, the Greek Minister of Defence decided to establish an Office for War Information which was placed in the Greek National Defence Staff. Since then, civilian experts and military officers have been educated, trained, and managed to create a specialized force (Stavrakakis, 2011). Over the past months of 2020, the Greek government has faced serious problems, as many websites have been attacked and as a result some of them went offline. The websites affected by the cyber-attacks included, among others, the Greek Parliament, the Ministry of Athens Stock Market and several Greek businesses (Liaropoulos, 2020). Media reports have attributed the attacks to Turkish hackers. Today Greece is called upon to provide *security and*

become resilient. In Greece, the vast public sector cyber-security umbrella that has the responsibility for the *prevention* of cyber-attacks includes the following agencies:

- The National Intelligence Service (NIS-EYP). Characterized as the Authority of International Security (INFOSEC), it ensures the security of national communications and information technology systems. The Greek Intelligence Service is also responsible for the certification of classified material of national communications. It was designed as the National Authority for the Protection of Cyber-Attacks, and prevents cyber-attacks on communication networks, storage facilities and information systems.
- The National Computer Emergency Response Team: in accordance with decisions by the Government Council for Foreign Policy and National Defence, the National Computer Emergency Response Team coordinates the activities of Intelligence Services related to the collection and disposal of information. It cooperates with the Department of Military Intelligence (E-5 branch) on issues of drafting regulations, certification systems, and the prevention and management of cyber-attacks.
- The General Secretariat of Communications of the Ministry of Infrastructure, Transport, and Networks collaborates with the directorate of banking supervision. It operates as the authority of telecommunications and shapes the national security strategy, managing the implementation of the security of public networks, energy security and cyber-communications.
- The General Secretariat for Information Systems of the Ministry of Finance: the Office of Information Systems Security and Data Protection and Infrastructure is responsible for drafting the standards for plans, development and operation of the information systems' security and quality control.

In the past ten years, Greece has faced dramatic austerity measures. In 2017 the Greek government decided to establish the National Cyber Security Authority (NCSA), which is being created to bridge the organizational and coordinative gap between the stakeholders (the Ministries of Defence and of Digital Policy and the Media, and the National Intelligence Service) involved in cyberspace security in Greece, in both the public and private sectors. The National Cyber Security Authority evaluates, revises, and updates the National Cyber-Security Strategy in order to make Greece a safe and resilient state (UNIDIR 2020).

2 ILLEGAL IMMIGRATION AND HUMAN TRAFFICKING: A GREEK NATIONAL SECURITY THREAT

In April 2020, Greece experienced a major resurgence of illegal alien arrivals, replicating the worst moments of the 2015 mass invasion of illegal immigrants, primarily via the Greek islands in the northern Aegean Sea. Human traffickers, operating along Turkey's Aegean shores, often with the collaboration of the Turkish authorities, have perfected their system of pushing the immigrants across the narrows: the inflatable boats are shoved into the water in broad daylight, their passengers are well-equipped with life jackets, and smugglers of different nationalities, carrying

the latest technology mobile phones, steer directly to the Greek island of Lesbos, where Non-Governmental Organization (NGO) receivers are waiting in order to immediately disembark the arrivals and move them to the interior of Lesbos (Symeonides, 2019).

Because of the overburden of illegal immigrants, the critical situation was dramatically highlighted by riots in late September 2019 at the Moria hotspot, which was holding nearly 24,000 people when its original capacity was put at 3,000. The current onslaught from Turkey does not only bring in tens of thousands of uninvited and undocumented aliens, it also promises infiltration by Islamist terrorists seeping out of Syria, with Turkey's tacit approval (Symeonides, 2019).

In the specific case of Islamic terrorism, Greece has been in a lull for a long time, judging that "Greek-Arab friendship" is enough to preclude large-scale Islamist terrorist incidents on Greek soil. This impression is outdated for many reasons: the times have changed radically, especially since the Arab Spring and the rapid rise of ISIS/Daesh; the steady flow of Muslims into Greece has come with an increasing resentment of the newcomers towards the host country; Turkey's subversive tactics and constant hostile probing of the Greek domain make this resentment a potent "unconventional" weapon against Greece; and the possibility of a "lone wolf" action is always present and must not be overlooked (Symeonides, 2019). There is little evidence of the Greek government trying to change to specifically face this highly likely threat. The open border alone invites those who may be planning to hit "infidel" Greece in a demonstration of Islamic might. Greece's convergence with the USA and Israel provides additional political and ideological incentives to potential terrorists in the post Covid-19 era.

Greece needs to grow serious about the critical issues of national security. With Islamist radicals entering Greece in, most likely, increased numbers, the official response to the threat is to send out intelligence (HUMINT) and police officers (EKAM) with lists of names and photos to monitor the crowds freely trudging into Greece. Even the most casual observers cannot but be amused at the "lists and photos" approach to this key security threat, which requires advanced monitoring and detection methods.

The Greek government must take the following recommendations on board immediately in order to tackle non-traditional threats and protect the safety of the Greek and European citizens in the European Union member states (Bruske, 2016):

- Declare a state of national emergency and close the land and sea borders to illegal immigrants;
- Move legislation through parliament post-haste to severely tighten asylum laws and enable the re-vetting of asylum-seekers suspected of fraud with the question of deportation;
- Accelerate deportations and the evacuation of squats;

– Immediately allow stop-and-question police operations in urban centres;
– Tighten the rules pertaining to NGOs and immediately prohibit foreign NGOs from operating inside Greece in support of illegal aliens;
– Intensify and expand intelligence cooperation (HUMINT) with other EU/NATO countries in pursuit of jihadis hiding within the throngs of illegal aliens;
– Increase funding for human resources and training for Greek law enforcement personnel.

In the post Covid-19 era, the above list of recommendations represents the minimum the Greek government should be doing in trying to stem the flows of illegal immigrants to Greece.

3 GREEK INTELLIGENCE SHARING COOPERATION IN COMBATING NON-TRADITIONAL THREATS

Human Intelligence (HUMINT) and cyber security threats are both an internal and an external problem. The Greek intelligence service (NIS-EYP), the police anti-terrorism squad, and the department of defence are responsible for domestic security. However, there is not a "security and intelligence culture" in Greece, and this makes it difficult for security and intelligence services to overcome governmental obstacles (lack of evaluation of human resources and nepotism) in order to establish a productive and effective HUMINT and cyber-security intelligence sharing (Nomikos, 2008).

It was not until the Madrid (2004) and London (2005) terrorist attacks, which deeply shocked the European Union member states and served as a terrible reminder of the threat posed by terrorism, much like its American counterpart, that the European approach to understanding Islamic terrorism changed from ascribing the attacks to the failure of intelligence or even imagination to a failure of education (Nomikos, 2007). It is worth pointing out that the Western Balkans has also been considered the home of Islamic extremists. Professor J**ó**zsef Kis-Benedek, a Hungarian security expert, states that "followers of conservative and extremist Islam endanger the secular system by labelling normal, moderate religious people as apostates. Many radical people are organized in small groups, in a heterogeneous environment, under the subordination of a radical imam" (Benedek, 2018).

Despite the swirling changes that the Greek law enforcement and intelligence community has undergone in the past few years, enough is known of the world that intelligence will confront beyond 2020 (e.g. biological threats) to begin the reshaping (Nomikos, 2014). The world will require intelligence to be dispersed, sharing its information and analyses with a variety of would-be-coalition partners, including foreigners and people outside governments such as specialized think-tanks which focus their agenda on intelligence studies.

Furthermore, the key element for a successful and efficient Greek HUMINT and cyber security strategy against non-traditional threats (biological warfare, CBRNE,

transnational organized crime networks) is the coordination and quick response of public institutions and the private sector (Nomikos, 2018). A systematic collaboration could manage to *establish a scientifically superior multi-disciplinary HUMINT and cyber security expert team* which could cope with large scale cyber-attacks and terrorist incidents on Greek critical infrastructure. Easy access to the internet, the use of a billion computers and the vast digital networks prevent strict control of the state authorities of the internet.

Concluding remarks

The non-traditional asymmetric threats of the 21st century require intelligence-sharing cooperation, which is the most important weapon in the battle against terrorist acts in order to protect the safety of Greek society and Greece's critical infrastructure in the public and private sectors. Today every state's enemy is not a conventional one, but a faceless and remote entity such as the pandemic (Covid-19).

Cybersecurity and defence have long been part of the EU and NATO, and they have begun to see each other as complementary partners in building their cyber resilience. Similarly, Greece shares intelligence with the EU and NATO member states as part of the agreement on a technical arrangement on Cyber Defence in February 2016 between NATO's computer incident response capability and the EU's Computer Emergency Response Team (Lete, 2017).

Furthermore, the EU member states must explore ways to collaborate more on human intelligence by introducing a *"common European Intelligence Culture"* as well as cyber security standards by endorsing European cyber security policies in order to enhance critical infrastructure within the European Union.

Regardless of the ten-year financial crisis and the pandemic (Covid-19), Greece, a EU and NATO member, has managed to form a National Cyber Security Authority (NCSA) under the auspices of the Ministries of Defence and of Digital Policy and Media, and the National Intelligence Service, and to reconsider further reform of its security and intelligence community.

Finally, ***collective action*** on intelligence sharing between Greek Law Enforcement and the civilian and military intelligence communities is a necessary weapon in the battle to *contain illegal immigration by sealing the European Union's borders and support the safety of the citizens in the European Union member states!*

Bibliography

1. *Benedek, J. K., 2018. Jihadim and radicalization in selected regions of Europe, the Middle East, and North Africa – a case study. Sodobni vojaški izzivi, 2018, pp 75–91. Ljubljana: Ministrstvo za obrambo, Generalštab Slovenske vojske.*
2. *Bruske, L., 2016. Organized Crime's Goldmines: Combating Maritime Smuggling Routes from Turkey to Greece, Research Institute for European and American Studies Monograph, 2016, pp 5–33.*
3. *Lete, B., 2017. EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions, 15. 12. 2017. https://www.gmfus.org/publicatons/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions, 4. 8. 2020.*
4. *Liaropoulos, A., 2020. Is Greece ready for the Digital Era?, 18. 7. 2020. https://www.rieas.gr/researchareas/homeland-security/4505-is-greece-ready-for-the-digital-era, 3. 8. 2020.*
5. *Nomikos, J., 2007. Transatlantic Intelligence Cooperation, the Global War on Terrorism, and International Order, 2007, pp 161–181, in Yannis A. Stivachtis (Ed.) International Order in a Globalizing World. Ashgate Publishing Ltd, Hampshire, UK.*
6. *Nomikos, J., 2008. Greece, 2008, in Stuart Farson, Peter Gill, Mark Phythian & Shlomo Shpiro (Eds.) PSI Handbook of Global Security and Intelligence – National Approaches Vol Two – Europe, the Middle East and South Africa, Prageger Security International, Connecticut, USA, pp 465–478.*
7. *Nomikos J., 2014, Balkan and Mediterranean intelligence sharing cooperation and counter terrorism policy in Greece, 2014. In Denis Čaleta and Paul Shemella (Eds.) Intelligence and Combating Terrorism: New Paradigm and Future Challenges. Ljubljana: Institute for Corporate Security Studies, pp 249–257.*
8. *Nomikos, J., 2018. Cyber Security Incidents and Terrorist Threats in Greece. National Security and the Future, pp 9–14, Vol 19, No. 1-2, 2018. Zagreb: St. George Association.*
9. *Symeonides, T., 2019. Greece: Illegal Immigration Emergency, 6. 10. 2019. https://rieas.gr/researchareas/editorial/3172-greece-illegal-immigration-emergency, 25. 5. 2020.*
10. *Symeonides, T., 2019. Greece, Threats and the "One Percent Factor", 20. 10. 2019. https://rieas.gr/researchareas/editorial/3180-greece-threats-and-the-one-percent-factor, 26. 5. 2020.*
11. *Symeonides, T., 2020. Thinking of a Post-Pandemic World Order, 20. 4. 2020. https://www.rieas.gr/researchareas/editorial/4462-thinking-of-a-post-pandemic-world-order, 27. 5. 2020.*
12. *United Nation Institute for Disarmament Research (UNIDIR), Greece, 1. 4. 2020. https://cyberpolicyportal.org/en/states/greece, 3. 8. 2020.*