INTELLIGENCE REQUIREMENTS FOR CYBER DEFENSE, CRITICAL INFRASTRUCTURE AND ENERGY SECURITY IN GREECE

John M. Nomikos

Introduction

The end of the Cold War more than a decade ago created a world in which the relative stability between the two superpowers has disappeared. During the Cold War, a country's every action was conducted in the light of the adversary relationship between the United States and the Soviet Union. The cataclysmic changes that took place in Central and Eastern Europe as well as the Arab Spring in North Africa and Middle East changed the face of politics in Europe and in the Western world as a whole.[1]

In the age of globalization and Information technology the use of internet has rapidly increased influencing the functioning of governmental and private bodies. An important aspect of critical infrastructure protection is the understanding of the concept of energy security, arising from the impact of energy on the overall economic life and ordinary life of contemporary societies.[2]

This article focuses on the cyber defense of Greece, a medium-sized European Union member state aspiring to establish a National Cyber Defense Authority; the role of

---

[1] John M Nomikos, "Transatlantic Intelligence Cooperation, the Global War on Terrorism, and International Order", in Yannis A. Stivachtis (ed) International Order in a Globalizing World, Ashgate Publishing Ltd, UK, 2007, p.161.

[2] Klemen Groselj, "Critical Infrastructure Protection and the Energy Sector", in Denis Caleta & Paul Shemella Counter-Terrorism Challenges regarding the process of Critical Infrastructure Protection, Institute for Corporative Security Studies, Slovenia and Center for Civil-Military Relations, USA, 2011, p.136.

intelligence sharing through the Fusion-Centers on endorsing energy security in the Mediterranean region; and as a concluding remark points out the challenges Greece faces in its critical infrastructure, cyber defense and energy security sector.

Nowadays, the United States, European Union Member States and NATO members face the risk for a large-scale cyber-attack on oil platforms that could damage their critical infrastructure provoking havoc and panic. Furthermore, twenty-eight European Union member states need to agree on a collective and coordinated intelligence sharing strategy. The European Commission has proposed concrete initiatives for combating cyber-attacks as well as the protection of European Union Member States critical infrastructure.

In the case of Greece, the cyber exercise "Pomastis 2010" is considered a significant effort by Greek authorities. In the "Pomastis 2010", the driving force for the energy security and defense critical infrastructure in Greece was the cooperation between engaged actors, governments and private companies.

Greek Cyber Defense: Problems and Prospects

In 1999, the Greek Minister of Defense decided to establish an Office for War Information which was placed in Greek National Defense Staff. Since them, civilian experts and military officers have been educated, trained and managed to create a specialized force. Nowadays, in Greece, the vast public sector cyber security umbrella that has the responsibility for the prevention of cyber-attacks includes the following agencies:[3]

- National Intelligence Service (NIS-EYP): It is characterized as the Authority of International Security (INFOSEC) and it ensures the security of national communications and information technology systems. Moreover, the NIS-EYP is responsible for the certification of classified material of national communications. It was designated as the National Authority for the Protection of Cyber-Attacks and

[3] Manolis Stavrakakis, "Alert in Cyber Crime Unit", Greek Financial Newspaper, Investor World, 16-17 July 2011, Greece, p.4

prevents cyber-attacks against communication networks, storage facilities and information systems.

- National Computer Emergency Response Team: In accordance with the decisions of the Governmental Council for Foreign Policy and National Defense, 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 and intelligence staffs supervised by it. Moreover, the National Computer Emergency Response Te4am collaborates with the Department of Military Intelligence on the issues of drafting regulations, certifications systems, prevention and treatment of cyber-attacks.

- General Secretariat of Communications of the Ministry of Infrastructure, Transport and Networks: It collaborates with the Directorate of Banking Supervision. It operates as the Authority of Telecommunications and shapes the national security strategy, materializing the implementation of the security of public networks, energy security and cyber communications.

- 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 system security and quality control.

However, the biggest problem for the Greek Authority Cyber Defense is the continuing austerity measures because of the lack of funding. Therefore, the prospect for the Greek Authorities is not so bright regarding the effectiveness of the Greek Authority Cyber Defense. There is also a lack of collaboration among the Greek Authority Cyber Defense the

private sector, specialized think tanks as well as private universities.[4]

The Role of Mediterranean Fusion Center in the Energy Security Sector

On 11th September 2001 (9/11) the international community was introduced to a new type of terrorism, one that was truly global in its organization and its impact. In the Europe, United States and Asia, it was immediately clear that an effective response would require new level of cooperation across the Atlantic and around the world. The post 9/11 era has challenged governments, policymakers, religious leaders, the media and the general public to play both critical and constructive roles in the war against international terrorism.[5]

Furthermore, the post 9/11 also confirmed how critical national, regional and local agencies and public safety and private sector entities are collecting important intelligence and information that ultimately impacts the state's overall ability to prevent terrorist acts against critical infrastructure and criminal activities.

The United States has initiated with the establishment of the Fusion Center in national, state and local levels in order to facilitate the sharing of homeland security by collecting intelligence and maximize resources, streamline operations as well as improve the ability to combat terrorism, crime by analyzing data from a variety of sources.

Nowadays, in the Mediterranean region, one explores the proliferation of illicit human smuggling and trafficking on the maritime route from Turkey to Greece and from Libya to Italy. Many long-established transnational organized criminal groups have switched from heroin and weapon trafficking to the highly lucrative practice of smuggling humans. The situation is exacerbated by a

[4] Manolis Iliadis, "In front of National Authority Cyber Defence", Greek Financial Newspaper, Investor World, 16/01/2010, Greece, p.30.

[5] John M Nomikos, "Transatlantic Intelligence Cooperation, the Global War on Terrorism, and International Order", in Yannis A. Stivachtis (ed) International Order in a Globalizing World, Ashgate Publishing Ltd, UK, 2007, p.161.

lack of consensus and cohesion by the European Union (EU), and Spain, France, Italy and Greece.[6]

Moreover, the article proposes the establishment of Fusion Centers in the Mediterranean nations (Spain, France, Italy and Greece). The ultimate goal of the Fusion Centers in the Mediterranean region is provide a mechanism through which government, intelligence services, law enforcement, public safety, and the private sector can come together with a common purpose and improve the ability to safeguard their homeland and prevent terrorist incidents against oil platforms. The Fusion Center enhances energy security and it employs the core of collaboration among different agencies in order to support Open Sources Information and Intelligence-Sharing.[7] As a result, a Fusion Center refers to managing the flow of information and intelligence across levels and sectors of government and private industry. It goes beyond establishing an intelligence center or creating a computer network. When combined with appropriate analyses, it can result in meaningful and actionable intelligence and information.

Concluding Remarks

The asymmetrical threats of the 21st century require intelligence-sharing cooperation which is the most important weapon in the battle to protect critical infrastructure in energy security areas and endorse collective Cyber Defense in the European Union member states. Today, the enemy is not a conventional enemy but a faceless and remote entity.

The twenty-eight national governments in the European Union need to collaborate on Cyber Defense by introducing cyber security standards in order to protect their critical infrastructure and endorse energy security policies.

Regardless of the eight year recession, Greece, as a NATO and EU member has managed to found the National Authority of Cyber Defense under the auspice of

---

[6] Lacey Bruske, Michael Nair, Travis Parrot, Maria Elena Pino, "Organized Crime's Goldmine: Combating Maritime Smuggling Routes from Turkey to Greece", RIEAS Monograph, May 2016, Athens, Greece, p.5

[7] Fusion Center Guidelines Report – Developing and Sharing Information and Intelligence in a New Era, U.S. Department of Homeland Security, U.S. Department of Justice, 2005, p.4

the Department of Defense to protect its own critical infrastructure and collaborate on energy security issues with the governments of Cyprus, Israel, Lebanon, Egypt, and Italy in the Mediterranean Sea.

At the end, the proposed Fusion Centers in the Mediterranean region could be a necessary tool for collective action among the intelligence services depended on shared intelligence and ***common assessment*** in order to prevent prospective major terrorist acts against critical infrastructure in our home states!