CYBER SECURITY INCIDENTS AND TERRORIST THREATS IN GREECE

John M. Nomikos

Introduction

The post 11 September 2001 era has changed governments, policy-makers religious leaders, the media and the general public to play both critical and constructive roles in the war against cyber terrorism and asymmetric warfare[1]. As the security and intelligence community inexorably works its way into the 21st century, it faces an unprecedented way of challenges. The chaotic world environment of the post Cold War (Arab Spring, Syria and Libya crises, Iran nuclear issue, Illegal immigration, human trafficking, Islamic radicalization, money laundering and transnational organized crime) offers a wide range of different issues to be

[1] John M Nomikos, "Balkan and Mediterranean Intelligence- Sharing Cooperation and Counter-Terrorism Policy in Greece" in Denis Caleta and Paul Shemella (eds) Intelligence and Combating Terrorism: New Paradigm and Future Challenges, Institute for Corporate Security Studies, Slovenia and Center for Civil-Military Relations, Naval Postgraduate School of Monterey, USA, p:249.

understood, and a variety of new threats to be anticipated. The rapidly developing information age presents advanced and complex information technology and methodologies to be mastered and integrated in order to make cyber-security more efficient to combat terrorist incidents on critical infrastructure.

Greece is located in the Balkan and Mediterranean region and is an active member of the European Union and the North Atlantic Treaty Organization (NATO). Today, one of the biggest challenges for Greece is to modernize its cyber-security public institutional framework in order to confront efficiently cyber attacks.

It is in the context that the present article highlights the problems and prospects of Greek cyber defense as well as the strategic significance of the Intelligence sharing cooperation among Greek intelligence service (NIS-EYP), law enforcement antiterrorism squad (EKAM), military intelligence and coast guard counter-terrorism branch. In the conclusion, collective action is the most important tool among the security and intelligence community depended on shared intelligence and joint assessment in order to prevent prospective major cyber security terrorist acts on critical infrastructures in Greece.

Greek Cyber Defense: Problems and Prospects

In 1999, the Greek Minster of Defense decided to establish an Office for War Information which was placed in Greek National Defense Staff. Since then, 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[2]:

(1) 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 Greek Intelligence Service is 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 against communication networks, storage facilities and information systems.

(2) 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 (E branch) on the issues of drafting regulations, certification systems, prevention and treatment of cyber-attacks.

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

(3) 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.

(4) 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. 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. In addition, there is a lack of collaboration among the Greek Authority Cyber Defense, the private sector, specialized think tanks and private universities.[3]

Intelligence sharing cooperation in Greece

[3] Manolis Iliadis, In front of National Authority Cyber Defense", Greek Financial Newspaper, Investor World, 16 January 2010, Greece, p:30.

Cyber security terrorism is both an internal and external problem. The Greek intelligence service, police antiterrorism squad and department of defense are been responsible for domestic security.

However, there is not a "security and intelligence culture" in Greece and it makes difficult for security and intelligence services to overcome governmental obstacles (lack of evaluation on human resources and nepotism) in order to establish a productive and effective cyber-security intelligence sharing policy.

Furthermore, the key element for a successful and efficient Greek cyber security strategy is the coordination and quick response of public institutions and the private sector.[4] The systematic collaboration could manage to establish a scientifically superior multi-disciplinary cyber security expert team that could cope with large scale cyber attacks against Greek critical infrastructures. The easy access to internet, the use of billion computers and the vast network prevent a strict control of the state authorities on the internet.

Concluding Remarks

The asymmetrical threats of the 21st century require intelligence-sharing cooperation which is the most important weapon in the battle against cyber security terrorist acts in order to protect critical infrastructure in the public and private sectors in Greece. Today, the enemy is

[4] Georgios X. Protopapas, "Cyber Terrorism and Greek Defense Strategy" in Denis Caleta & Paul Shemella (eds) in Counter-Terrorism Challenges regarding the process of critical infrastructure protection, Institute for Corporate Security Studies, Slovenia and C enter for Civil Military Relations in Naval Postgraduate School of Monterey, USA, p:102.

not a conventional enemy but a faceless and remote entity.

The European Union Member-States need to cooperate on cyber defense by introducing cyber-security standards in order to protect their critical premises and endorse cyber security policies.

Regardless of the ten years financial crisis, Greece, a European Union and NATO member has managed to found the national authority of cyber defense under the auspice of the department of defense to protect Greek critical infrastructure and collaborate on security issues more effectively.

Last but not least,[5] collective action on intelligence sharing between Greek law enforcement, civilian and military intelligence community is the necessary solution to prevent prospective cyber security attacks in Greece!

[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. p: 180.