CAN GREECE DEFEND ITSELF IN CYBER ATTACKS?

Choutea Eleana
(Security Analyst, & RIEAS Research Associate)

More often than ever to Greek standards the term "cyber-attack" is used, based on the latest developments and attacks by Turkish hackers. Joseph Nye is topical- especially in the last two years at the global level - with its formalities on hybrid war, which he described it as "*that form of war that requires the development of new weapons, the use of innovative technologies and the use of non-weapons*".

The forms of the hybrid war include: terrorism, political and economic pressure, and cyberwar. A future cyberwar could undoubtedly lead to redistribution of former traditional power roles. The more a country relies on technological achievements or Internet, the higher the risk of invasions.

Since the definition of cybercrime has not yet been fully clarified, considering the UN Charter, the following question arises: since the Charter does not specify "armed attack" or "aggressive action", why not include the concept of cyber attack ; And if it is included, does it mean that the right to legal defense is activated, and then in the form of cyber-attack?

If we consider that, according to the prevailing interpretation, the term "attack" refers to actions taken by a state to threaten the territorial integrity or political integrity of another state, and then we think about

cyber attacks in critical infrastructures, can we talk about "micro-episodes" of war with non-conventional means?

Due to the incidents that have taken place over the last few days and Nye's words can only confirm what is being said: how Turkey is using and operating incrementally increasing attacks, without the use of conventional weapons, against Greece. The initial attack on the Athenian-Macedonian news agency, on other websites and later on the site of Suzuki.gr leaves no room to talk about but for Turkey's cyber attacks against Greece.

Therefore, it is necessary to examine the actions that Greece should take, since the primary task of the government is to protect the country, the citizens, the critical infrastructure and the economy from the attacks by establishing a framework of protection. The areas covered by this framework are three: defense, deterrence and development.

Infrastructures that are important and need to be defensive are:

· Energy and vital infrastructure: hospitals, electricity networks and power stations, water supply and distribution systems for medicines and food.

· Communications: Mobile and Fixed Telephony Networks, Army Telecommunications, Radio Stations, the Internet and 'Smart Devices'.

· Economy: stock exchange and banks

· Means of transport: air traffic control towers, lanterns and bridges, cars and computer systems on terrestrial and underground railways.

The protection of these will be achieved by developing security levels in each sector. The gathering and distribution of threat and risk information should be done rapidly to ensure a prompt response to any incidents. Even in cyberspace, interests and national sovereignty should be protected.

The government should develop such a range of capabilities that will enable it to repel the threats or attacks to be attempted by foreign enemy actors who intend to harm, disturb or destroy political, economic and military security. These actions will result from a defensive framework involving the participation of major ministries and will be based on the exchange of know-how and tools among them. Encryption, of course, is a

fundamental tool for protecting most sensitive information and choosing the way we develop our national security capabilities.

Concerning the short term policy, the skills and technologies of the private sector are required to maintain and strengthen ways of preserving national data. Then, given the government's desire to work with the private sector, a strong legal framework and oversight should be ensured. In the long term, a strategy should be put in place to incorporate cyber security into the education system, as in the years to come all citizens' actions and transactions will be done digitally.

That is precisely why computer science should also be upgraded. Everyone who studies computer science should be able not only to know fundamental principles governing the internet and cyber but also to be able to apply what they learn at any time. This could be achieved by creating an academy where the best computer operators will work to secure government structures. This will be to attract investment in companies active in the security sector. So far, the Cyber-Threat Center (CIS) - which is under the Cyber Security Directorate of the National Defense General Staff - is responsible for the protection of critical communications and IT systems.

A pioneering and innovative cyber security sector is a necessity in the modern and digital era we are. As Ernst & Young states in a report "*cyber security is the key to paving the way for innovation. Building trust in a successful business on the Internet of Things, which fully supports and protects people and their personal mobile devices, is a key competitive feature and should be a priority.* “Technology is not a simple power factor, it is a power amplifier.