COMMENTARY

VOLUME 5

MACEDONIA MUST DEVELOP A CYBER SECURITY STRATEGY

www.analyticamk.org

Cyber security has been high on the agenda for many governments as well as companies all across the globe. Cyber security is important due to increased reliance on interconnectivity and IT infrastructure for the everyday functioning and providing of services of schools, hospitals, airports, electricity companies, internet providers etc.

The Republic of Macedonia has a relatively modest experience when it comes to cyber security and threats. There have been several cases of defacement of websites of the institutions, and cybercrime has also been on the rise. Due to the lack of cyber attacks that Macedonia has faced, the concept of cyber security has not been high on the agenda of stakeholders in the country. The area of cyber threats that has received most attention by stakeholders has been cybercrime.

For the successful combating of cyber threats, it is required that a country has a clearly defined national cyber-security strategy. Such a document would establish a frame that will guide, direct and coordinate the efforts of relevant and other relevant non state stakeholders, such as academia, private companies and CSO's.

Authorities in Macedonia are currently working on a cyber security strategy, in which the lead role will be within the MOI. For the drafting of this strategy many various stakeholders have been included[1]. These stakeholders fall under three categories:

- **State Institutions** (Ministry of Interior, Ministry of Defense, Intelligence Agency, Centre for Management of Crises, Directorate for Protection of Clasified Information, Directorate for Protection of Personal Information, Ministry of Education, Agency for Electronic Communication and Public Prosecution)
- **Private Sector** (Macedonian Chamber of Information and Communication Technologies (MASIT), in which 69 IT companies are included)
- **NGO Sector**

It is important to further involve CSOs in the process of drafting the strategy and be more transparent in general, as this would add legitimacy to the Cyber-security strategy and increase the level of trust the public has in it, a characteristic that is especially necessary after the eruption of the political crisis in Macedonia after the release of the tapes proving illegal wiretapping by the state, which gave good reason for the public not to have trust in the state.

It is also important that

1 Interview with member of the working group on drafting a Cyber Security Strategy. Conducted on 28.12.2016

this strategy is drafted as soon as possible, which a holistic approach, thus including all relevant stakeholders. It is crucial important to not stall the process, so that all actors involved can start working on the implementation of the strategy. A major cyber-attack on Macedonia's infrastructure could cause millions EUR worth of damage, and generally paralyze the country. This can happen even in a country that has a more developed cyber resilience, let alone a country like Macedonia that has not even developed a comprehensive strategy yet.

www.analyticamk.org

FILIP STOJKOVSKI,
RESEARCH FELLOW,
FOREIGN AND SECURITY POLICE PROGRAM
fstojkovski@analyticamk.org