Strategic, Legal and Doctrinal Consideration for a Better Cyber Defense in the Region of South-East Europe

Metodi HADJI-JANEV[a] and Mitko BOGDANOSKI [a,1]
[a]*Military Academy "General Mihailo Apostolski", Skopje*

Abstract.
Much of the social, economic and political activities in the region of South-East-Europe (SEE) take place via so-called cyberspace. Even though there is evidence of growing dependence of cyberspace in SEE countries the practice shows that there is no parallel match to security. Giving that no one is safe in the cyberspace the main argument of this article is that in order to provide effective defense from malicious and aggressive actors against their own citizens, the SEE countries should focus on building cyber resilient societies. In doing so they need to focus on building an effective strategy, adjust the law and develop appropriate doctrine.

Key words: Southeast European Countries, cyber war, Strategy, International Law, Doctrine

Introduction

The global security trends and the challenges from cyberspace have urged South-East-European (SEE) countries to prioritize their security and defense focus on cyber security. This trend complements SEE countries' Euro-Atlantic aspirations too. So far only Bulgaria, Croatia and Slovenia have developed a national cyber security strategy. The rest of the SEE Countries are in the process of concluding similar documents. Nevertheless, a closer look at the approach toward cybersecurity indicates that SEE countries have not considered military involvement in accordance to the existing threats. Precisely, authorities in the respected countries are hesitant to address the cyber warfare threats that might affect the defense of the nation.

The main argument of this article is that if SEE countries are about to protect their citizens from cyberspace they need to focus on building cyber resilient societies. This process must among other, focus on threats from potential cyber warfare activities toward respected SEE countries' nations. The article argues that to achieve the desired end-state, i.e. build cyber resilient societies SEE countries' authorities need to build effective cyber security strategy that will address the cyber warfare threats. SEE countries also need to reconsider existing legislations and make some adjustments in the context of the existing threats and *ius ad belum* and *ius in bello* principles and standards. Finally, SEE countries should develop adequate doctrines to accomplish the strategic

[1] Corresponding Author.

guidance and build effective cyber resilient societies that will defense the respected SEE nations.

For the purpose of this debate in the article, the term South – East – European (SEE) countries will refer to both NATO countries from the region of Southeast Europe (Albania, Bulgaria, Croatia, Montenegro and Slovenia) and PfP countries (Bosnia, Macedonia and Serbia).

To prove the above mention theses the article will first briefly address the global security trends and the cyber warfare challenges to SEE countries. Then the article will address strategic, legal and doctrinal considerations for effective cyber defense “as a means to an end” in building cyber resilient societies in South-East-Europe.