SERBIA TIGHTENS CYBER-SECURITY AS INTERNET CRIME RISES

- 28.09.2018

Balkan Insight (28 September 2018)

Serbia's government plans to strengthen the country's cyber-security and the capacity of the police and military to prevent hacking attacks amid a marked rise last year in hi-tech crime.

According to the Cybercrime Strategy, Serbia will establish several units within the police, military and customs to fight online crimes.

The strategy is a continuation and expansion of activities aimed at strengthening the efficiency of all entities in the field of suppression of high-tech crime in ... Serbia, the Strategy, obtained by BIRN, reads.

The document, which covers the period between 2019 and 2023, says that by 2020, Serbia will form anti-cybercrime units within the intelligence agency, the BIA, Military Police and Customs Bureau, and also employ more people in existing units with the police.

It also added that Serbia will purchase new IT equipment but also specialised software for the police and prosecution, for which about 100,000 euros has been allocated.

It states that Serbia will also adopt operational procedures to collect and provide electronic evidence.

Civil servants will participate in training, which will be also held for parents, in schools, in the media, and for bank clients, focusing also on child pornography and internet security.

The strategy ☀ determines the institutional response to emerging forms of high-tech crime, defines the roles and responsibilities of state bodies, identifies goals and determines the basic directions for action to suppress all types of high-tech crime, it says.

The document notes that Serbia saw a 15-per-cent increase in cybercrime in 2017 compared to the year before.

From 2013 to 2017, the most common cybercrimes noted were computer fraud (43.9 per cent) and unauthorised access to computers and networks (37.4 per cent). Forgery and abuse of payment cards were also common.

Criminal offences in which information and communication technologies are abused are increasing, as a consequence of the rapid development of IT technology, such as those related to the security of computer data, sexual abuse of minors and children for pornographic purposes on

the Internet, fraud via the Internet, unauthorized use of copyright and related rights, threats to security, terrorism and violent extremism leading to terrorism, it recalled.

Andrej Petrovski from the Serbian SHARE Foundation, an NGO dedicated to protecting peoples digital rights, told BIRN on Thursday that the adoption of the strategy is a positive step, but only if its implemented in the way it is defined.

It is good that Serbian authorities want to harmonise local [law] with the EU legislation, especially when it comes to Criminal Law, and laws on misdemeanours and criminal proceedings, he said.

Petrovski further explained that harmonising the legislation will mean harsher sentences for criminals in Serbia, as currently they receive lesser sentences than the EU enforces.

But what I see as the potential problem is not in the strategic documents, but in its implementation, as since 2014, about 20 criminal charges filed by media organisations, which were noted in the SHARE register, received no result, because of the lack of the political will [to do so], Petrovski noted.

On September 20, the Interior Minister, Nebojsa Stefanovic, told a conference in Belgrade on cybercrime that in 2018, the ministry's Special Department for Combating High-Tech Crime filed 77 criminal charges against 82 persons.

He added that in the previous ten years this department filed 881 criminal charges against 1,906 persons.

http://www.balkaninsight.com/en/article/serbia-to-form-anti-cyber-criminal-units-09-27-2018

Kaynak/Source: