Kosovo's Take on Cybersecurity

Author: Vesa Kroçi, KCSS

August, 2023

BACKGROUND

In 2014, there was a notable surge in cybercrimes in Kosovo. The advancement and widespread adoption of technology during this period brought about a more pronounced occurrence of cyber-related offenses. Fadil Avdyli, the head of the Cybercrime Investigation Sector in the Kosovo Police, reported that eight individuals were apprehended in 2012, eleven in 2013, and seven in 2014. The rising cyberattacks in Kosovo provided an impetus to build a new policy framework dealing with cyber security, resulting with the adoption by the Kosovo government of the National Cyber Security Strategy and Action Plan 2016 – 2019.

Program of the Kosovo Government 2021-2025 notes that "cyber security is a growing problem, we will engage in professional capacity building for the prevention of cyber-attacks, completion of the legal framework and modernization of cyber protection equipment". The Kosovo Security Strategy 2022-2027, puts significant relevance to strengthening cyber security capacities of Kosovo and notes that the government "will invest in the field of cyber-security, critical infrastructure, innovation and technology and capacity-building". The strategy also includes the Global Cybersecurity Index as an impact indicator, but Kosovo has not been included.

In 2023 Kosovo Assembly adopted Law No. 08/L-173 on Cyber Security, which among others, foresees the establishment of the Cyber Security Agency as well as partially transposes Directive (EU) 2013/40 of the European Parliament and of the Council of 12 August 2013 on attacks against information systems.

CHALLENGES

With Kosovo's population being highly connected to the internet, the country is highly exposed to heightened vulnerability for cyberattacks. Services are the primary employment sector in Kosovo and majority of these services are online and digital services, which are outsourced to Kosovo companies from the EU and United States markets. Successful cyberattacks against Kosovo can have significant impact on economy as well as societal peace. With respect to economy, they can undermine the confidence of American and European companies to do business in Kosovo, as well as cost Kosovar companies lucrative contracts, which can exacerbate unemployment.

Furthermore, due to Kosovo's fragile relations with Serbia and lack of normalization of relations, cyberattacks through disinformation campaigns can lead to interethnic incidents and violence. The state computer network system, user accounts, the financial system, websites, and the private sector are the main targets of cyberattacks in Kosovo.

The Challenges to Cybersecurity Education in Developing Countries: A Case Study of Kosovo highlights the five main factors that pose a barrier for maintaining a progress on cybersecurity. Starting with the most prominent, the lack of cybersecurity education in Kosovo's primary and secondary schools. As cybersecurity remains a nascent field of study, the country's academic curriculums have been unable to provide it as a standalone educational program, resorting to condensing it into a singular module in existing Information Technology courses. Despite a rapid increase in Computer Science and Information Technology startups in Kosovo, there is a noticeable lack of professionals who are entirely focused on cybersecurity, resulting in an environment where future cybersecurity experts receive lessons and mentorship from IT professionals with limited knowledge and exposure to the field. Although there is considerable interaction between academics and private business in the areas of software engineering and information technology, cybersecurity is not included in this partnership. The Kosovo HEIs are having trouble comprehending what the industry needs in terms of cybersecurity expertise. Fourth, there is a lack of coordinated and centralized cybersecurity training.

WAY FORWARD

- Introduce digital learning in schools as well as support funding for informal education opportunities on cybersecurity for youth across Kosovo.
- Establishment of the Agency for Cyber Security is very important, and should be done in a manner that includes experts and consultations with the IT sector in Kosovo
- Amplify public awareness on cybersecurity. With the rapid development of technology, it is important that the public is aware of the threats of cybersecurity, safe online practices, as well as reporting incidents.
- Reform legal and policy frameworks, fund cybersecurity capacity development, and provide active training to public institutions and stakeholders.
- Actively participate in international and regional cooperation initiatives and opportunities on cybersecurity