Espresso.Insight
No.21 /2020 December 23, 2020

SPECIAL EDITION – SERIES OF ESPRESSO INSIGHTS

Cybersecurity

–

Aurora Mullatahiri

GROUP FOR LEGAL AND POLITICAL STUDIES

GROUP FOR LEGAL AND POLITICAL STUDIES

Group for Legal and Political Studies

is an independent, non-partisan and non-profit public policy organization based in Prishtina, Kosovo.

Our mission is to conduct credible policy research in the fields of politics, law and economics and to push forward policy solutions that address the failures and/or tackle the problems in the said policy fields.

legalpoliticalstudies.org

SPECIAL EDITION – SERIES OF ESPRESSO INSIGHTS

2020 has been a year to remember, especially in Kosovo. In this Espresso.Insights series, GLPS recaps and analyses the main events in the fields of politics, law and society that have affected the country this year and identifies the challenges ahead of 2021. In part 5, Aurora Mullatahiri explores the risks that Kosovo has faced in the field of cybersecurity in 2020, and what lies ahead with the development of the technology and the increase of cybercrimes as a social phenomenon.

#KOSOVOin2020: Cybersecurity

By: Aurora Mullatahiri - Group for Legal and Political Studies

One would associate 2020 with the spread of COVID-19, undoubtedly. However, this year will also be recognized for the normalization of virtual life. The pandemic has interfered with the way we organize our social interactions, cultural activities, our habits, work and study environments. Internet has been an important discovery, but its significance was emphasized in 2020, holding the key toward reorganizing society while adapting to the invisible threats of the pandemic. With the development and overload of the virtual space, the risks for cybercrime have increased. During the pandemic, the International Criminal Police Organization (Interpol) reported that people's rising online dependency should be seen as a new opportunity—nevertheless, it poses a risk of future boost in cybercrimes. In this regard, the citizens of Kosovo have plenty to remember this year, from virtual crimes to the tiny efforts of the government and justice system towards combating them.

Cybercriminals exploiting the COVID-19 pandemic

At the beginning of the pandemic in March, Kosovo was in a lockdown. This forced many businesses and individuals to go online and work from home, while not taking steps to ensure safety in their cyberspace. This vulnerability was used best by cybercriminals. By the end of March, the Kosovo Police was already reporting an upward shift of cybersecurity breaches and penal crimes occurring in the virtual space. Among the most common ones were identity theft and intrusion of computer systems. As more cases appeared, the intruders were shifting from attacks toward individuals to bigger companies. Amidst these victims were online newspapers, oil companies, and financial institutions.

One of the most serious attacks was the one to Kosovo's Economic Bank in April, when hackers extracted personal data from the bank's customers. Meanwhile, other cases of cyber attack were aimed at online news portal Gazeta Express and petrol company HIB. However, the most intriguing case was one regarding the disappearance of two million Euros from the Treasury of Kosovo, a department that falls under the management of the Ministry of Finance. Shortly after the money disappeared, the Minister of Finance, Hykmete Bajrami, held an extraordinary media conference and declared the offense as an act of economic cyber crime. The conclusion was based on the way that this criminal act had occurred, namely through creating false users in restricted access computer systems of the Treasury of Kosovo.

The prosecution is currently investigating the defendants under suspicion of abuse of official duty and authority.[1]The Law on Prevention and Fight of Cybercrime, especially Article 8, which sanctions the unauthorized access and misuse of restricted category computer systems, was not taken into account by the prosecution—even though a fake user account, under the name of Hasan Krasniqi, was created in the electronic system where the money of the entire state budget was managed, and from which the illegal transfer was successfully completed.

While the above-mentioned are cases reported or under current investigation, 2020 also featured two criminal cases that were represented at the courts from January to December. Both cases emerged in 2007. According to the indictments, the first case concerned the interference with computer systems of US-based Yahoo users, illegally obtaining and selling financial data while gaining 73,000 Euros; whereas the second one regarded the issuing of fake bank cards and entering in computer systems of banking institutions, managing to benefit the amount of 198,000 Euros. The judicial addressing of these cases was characterized by serious delays on procedural aspects and court hearings, while also risking statutory limitation. One can argue that, since cybercriminals were fast and sophisticated in their attacks, the prosecution was indeed slow in bringing action against these virtual offences.

The binary of cybersecurity legislation and the tall National Cybersecurity Coordinator

During 2020, Kosovo's government has taken action to improve the legislation on cybercrime protection. The inclusion of cybersecurity as a priority in the Government Program 2020-2023, as well as in the Legislative Program of 2020, is indicative of that. However, this should be taken with a pinch of salt, since amending the legislation to improve cybersecurity in Kosovo has been a priority of every Government since 2016. Also, the Law has remained the same from 2010. Hence, the legislative structure that governs cybersecurity in Kosovo continues to be guarded simultaneously through policies on the protection of electronic communications and on the prevention and fight of cybercrimes. Regardless of this, the legislative framework has not been implemented, and this has been known by the Ministry of Internal Affairs from 2018.

The institutional structure watching over Kosovo's cybersecurity field has remained intact since it was firstly presented by the National Cyber Security Strategy and Action Plan 2016-2019. The institutional bodies that are supposed to mandate, coordinate and monitor the implementation of the policies have continued to be the National Cyber Security Council and the National Cyber Security Coordinator. In October, the government appointed Zafir Berisha as new National Cybersecurity Coordinator. The designation of Berisha, who both was a political figure and held the position of deputy minister of internal affairs, was followed by opposing public reactions and, even, by the hack of his personal Facebook account. The argument that Berisha was not the most suitable official for the job was also accepted by himself, after declaring "that he had been chosen for the position because he is 1.83m tall", when asked about the qualities that made him appropriate. The appointment of persons that are not known for mastery in the field have shown the lack of seriousness of government bodies in implementing strategies aimed at increasing cybersecurity.

[1]The indictment is accusing the defendants under Article 414, Par. 2, and Par 3 Point 3.4 in conjunction with Money Laundering under Article 302 of the Criminal Code of the Republic of Kosovo.

Cybersecurity in 2021: what are the prospects ahead?

As it appears that computer systems are being used worldwide for work, regardless if one is engaged in the public or private sector, for organizing events, holding lectures in universities, and even organizing poetry and theater plays, it is important for Kosovo to take cybersecurity seriously ahead of 2021. The rising number of new cyber attacks during the months of COVID-19 might have been the last wake-up call for the state and the judicial power to start dealing with such acts faster, more accurately and genuinely.

In Kosovo, the pandemic has heavily impacted the implementation of reforms. The expected resumption of legislation enforcement will pose a constant challenge for 2021 on how to provide means, mechanisms, legislation, and awareness campaigns that are up to date. In this sense, it will be fundamental for Kosovo to work towards securing safety in a cyberspace where the country's institutions, business, and individuals will be operating in the future.

Espresso.Insights

Espresso.Insights are aimed at decoding the policy research of our Fellows to a broader audience. Espresso.Insights present short summary of analysis and information that help readers and policy-makers in particular, to understand the relevant research, as they suggest possible policy options and argue for certain path of action. Aiming to intensify the debate about policy issues and general public concerns, Espresso.Insights will, in addition, serve as gears to aid an informed decision-making process.

GROUP FOR LEGAL AND POLITICAL STUDIES