AFP/GETTY IMAGES

# A PRESENT CONCERN

## AS INTERNET USAGE SOARS, KOSOVO MUST HARDEN ITS DEFENSES

**By Hafize Bajrami**
IT chief, Ministry for the Kosovo Security Force

Today, the internet is part of work and life for many millions of people worldwide. With the rapid developments in technology, cyber security is a serious concern. Most services in the public and private sectors are conducted via the internet, where users are exposed to threats posed by viruses, malware, cyber espionage and phishing.

Smoke billows from the coal-powered power plant in Obilić near Pristina, Kosovo. Attacks on power plants endanger the public. REUTERS

Kosovo has experienced a rapid growth in the number of internet users and now has a market penetration similar to that of many European Union countries. Cyber crime has been identified as one of the global threats that may affect the security of Kosovo, a concern revealed in the government's 2014 report, "Analysis of the Strategic Security Sector Review of the Republic of Kosovo." Based on this, Kosovo has begun to develop greater cyber security defense capabilities. As is the case with many other countries, the most important areas in need of protection are critical infrastructure (CI) and critical information infrastructure (CII).

The protections include legal frameworks, strategies and policies, and identifying stakeholders and mechanisms responsible for various aspects of CI and CII. Because of the ubiquitous exposure to cyber threats, it is imperative that Kosovo reviews technology investment priorities, with particular attention to security and harmonization of legal frameworks for dealing with network security incidents and data protection. Legal frameworks must be harmonized along national and international vectors because cyber crime is not restricted to conventional markers such as borders, nationality, gender and age.

CII must be identified exhaustively by all governmental institutions. No comprehensive list of CII exists in Kosovo. A law on CI protection was drafted in 2016. This draft law transposes fully the EU Council Directive 2008/114/EC on the identification and designation of European CI and the assessment of steps needed to improve its protection.

According to this law, the identification and prioritization of national CI shall be led by the Ministry of Internal Affairs in consultation and cooperation with security institutions, government and nongovernmental institutions, public and private owners and operators, and key international stakeholders. It is of utmost importance to identify and assess the real CII within the country and to take all necessary measures to protect it.

## LEGAL FRAMEWORK

The National Cyber Security Strategy and Action Plan for implementing that strategy was approved by the Assembly of Kosovo in early 2016. Kosovo also has laws that cover many cyber security-related issues, including preventing and fighting cyber crime, information society services and government bodies, electronic communications and protection of personal data.

The primary legal framework for dealing with cyber crime or cyber incidents is found in the criminal code of Kosovo and the criminal procedure code. There is also an Emergency Management Agency law governing national coordination and interoperability, from which emergency response plans are derived. Security institutions respond to crises based on emergency response plans, which are more focused in responding to natural disasters and other emergencies than cyber incidents. For cyber security incidents, Kosovo must update this plan or draft a more effective one. Each institution has its respective administrative instructions and standard operating procedures or guidelines in place for the use and protection of data networks.

## STAKEHOLDERS AND MECHANISMS

As part of the national strategy, the National Cyber Security Council was established in 2016 as the highest governing body for cyber security. The council is led by the deputy minister of the Ministry of Internal Affairs and consists of representatives from the following institutions: the Ministry of Internal Affairs; the Kosovo Police; the Kosovo Forensics Agency; the Ministry for Kosovo Security Forces; the Kosovo Intelligence Agency; the Agency for Information Society; the Kosovo Security Council; the Ministry of Justice; the Kosovo Prosecutorial Council; the Kosovo Judicial Council; the Ministry of Finance; Kosovo Customs; the Ministry of Education, Science and Technology; the Ministry of Foreign Affairs; the Regulatory Authority of Electronic and Postal Communications (RAEPC); and the Central Bank of Kosovo.

The National Computer Emergency Readiness Team (CERT) was established under RAEPC and is trying to achieve needed capacities in terms of human and technical resources, infrastructure and services. Other government institutions are also establishing CERTs for their needs.

## EDUCATION, TRAINING AND EXERCISES

Dealing with rapid technological developments and new information technology services is a challenge to Kosovo's public and private sectors. The Ministry of Education has underscored communication and technology as a priority. An example of this prioritization is seen in the emphasis on information and communications technology (ICT) and security issues in the curricula for all levels of education. This emphasis is reflected in efforts to build cyber security programs for primary and secondary schools.

For government users of ICT, the Kosovo Institute for Public Administration has implemented training policies developed by the Ministry of Public Administration. That ministry is conducting annual training for standard users in data security fields based on the varying requests of individual ministries and other government institutions.

An important part of national coordination and interoperability is to design scenarios and conduct joint exercises through which the institutions involved can test their capacity to respond to contemporary challenges. These exercises improve incident response capacity for various threats, whether at the national or institutional level. After the national security strategy was approved, each institution conducted cyber exercises to raise user awareness and exercises were planned to test interagency readiness cooperation.

## RECOMMENDATIONS

Improving cyber security can be achieved by understanding:

- The national cyber security strategy was drafted based on European Union Agency for Network and Information Security (ENISA) guidelines. Other laws have yet to be adopted to better synchronize strategy, technology development and international legal frameworks between Kosovo and international entities such as the EU, NATO, the United Nations and other international organizations.
- All institutions responsible for cyber security must develop and harmonize policies and procedures to protect critical data and infrastructure. Those policies should bear sufficient authority to ensure interoperability among institutions inside and outside of Kosovo.
- Greater investment in the National CERT is necessary to make it fully operational with adequate personnel, equipment and tools, and training, which in turn would make it eligible for accreditation in Trusted Introducer (established by the European CERT community to address common needs and support all security and incident response teams) and the global Forum of Incident Response and Security Teams, or FIRST.
- The National CERT should be empowered to establish cooperation with regional and international CERTs.
- A rigorous assessment to identify CII and take all necessary measures to protect it is needed.
- Public sector cooperation and information-sharing venues with key private sector partners, through effective public-private partnership models, should be encouraged.
- Organizing and participating in international cyber security activities, such as conferences, seminars and workshops, is beneficial. So are scenarios and cyber security exercises for all relevant institutions with an aim to test interoperability within the country.
- It is important to develop training curricula within civil educational institutions to teach effective data protection and privacy measures to online users with special emphasis on protecting children online, and to develop programs to raise parental awareness of online risks.
- There is a need to organize awareness campaigns and update current ICT curricula at pre-university levels with cyber security modules. ENISA's Network and Information Security Directive and the U.S. National Institute of Standards and Technology's National Initiative for Cybersecurity

A construction worker prepares to open a newly constructed highway in Kosovo that is a centerpiece of the national transport system.

THE ASSOCIATED PRESS

Education serve as ready examples for raising cyber security awareness.

- It is essential to train and certify personnel involved with information security in all government institutions and private companies dealing with ICT.

## CONCLUSION

Cyber crime continues to pose the most significant challenges for Kosovo's institutions. The country has taken concrete steps to establish the legal infrastructure to prevent and combat all forms of cyber crime, but many challenges remain, especially in technical response capabilities, which is a relatively new phenomenon in Kosovo.

There is an ongoing need to reinforce the foundations of institutions involved in protecting against and prosecuting cyber crime by modernizing their technological equipment, supporting international cooperation in information sharing, and properly empowering the agencies best-placed to address cyber threats. Another need is to improve coordination between law enforcement authorities and technical personnel to better address the complexities of cyber crimes.

Finally, a robust cyber security awareness training, education and exercise capability will need to further mature to fully identify and mitigate Kosovo's CI and CII security shortfalls. Incorporation of cyber awareness curricula into formative education venues from an early age will foster a cyber security capacity-building environment where baseline risk awareness will meaningfully add to Kosovo's cyber security architecture and opportunities. □