PER CONCORDIAM ILLUSTRATION

Building ALBANIA'S CYBER CADRE

A look at gaps in education, professional training and certification in cyber security

By **Dr. Vilma Tomco**, director general, and **Klorenta Janushi**, information security expert,
National Authority for Electronic Certification and Cyber Security, Council of Ministers, Republic of Albania

Cyber security is a national priority. With the proliferation of communication technologies advancing at such an unprecedented speed, cyber security, interoperability and digital transformation have become the primary topics of the digital world.

Considering the brain drain phenomenon, we are already in a crisis in which we do not produce the number of skilled experts that the industry desperately needs. Investing money may not be the major obstacle it used to be, but organizations still need to map out the resources, assets and the competencies that they have to see what is missing.

The current attitude toward the overall skills shortage is to find short-term patches to the problem. Universities have added cyber security undergraduate or graduate degrees to their curricula. But curriculum designers must recognize the challenges they face as the digital environment evolves at exponential rates. Because of the dynamism of the field, it needs to be well understood that it is fundamentally different from any existing curricula. This understanding is essential to reducing the shortage of cyber security experts, involving more women, and creating more diversity in the cyber domain.

Regulatory framework

The European Union emphasizes the field of cyber security through the development of a common regulatory framework that consists, in part, of the adoption of the Directive on Security of Network and Information Systems (NIS Directive). Albania, as part of its engagement as a candidate for EU membership, has partially adopted the NIS Directive through Law No. 2/2017 on Cyber Security. The law entrusts the National Authority for Electronic Certification and Cyber Security (NAECCS) with oversight and fulfillment, and NAECCS acts as the national Cyber Security Incident Response Team (CSIRT), pursuant to the law. To fulfill these functional tasks, NAECCS has adopted a methodology for the organization and functioning of CSIRTs at the national level. The methodology defines the obligation to establish a CSIRT in each critical and important information infrastructure operator (CIIIO). The list of operators is approved by the Council of Ministers and updated every two years.

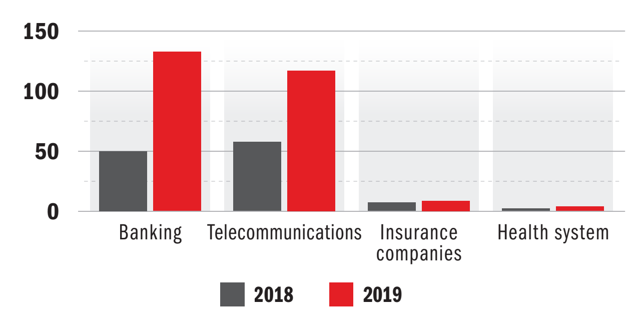
The Law on Cyber Security and its bylaws define the obligation for each CIIIO:

- Create dedicated cyber security positions through the establishment of sectoral CSIRTs.
- Improve system functionalities by implementing additional measures to increase security levels and coordinate with the national CSIRT for real-time handling of cyber incidents.
- Increase the technical and professional capacities of human resources through the organization of specific training in the field of cyber security, cyber drills and so forth.

Enforcement of the law and its bylaws is reflected in Figure 1. After completing the regulatory framework on cyber security, the CIIIOs increased the number of positions dedicated to cyber security. Figure 1 represents some of the most dynamic sectors based on the NIS Directive. NAECCS periodically conducts cyber drills and tabletop exercises to improve the skills of the experts, aiming to create a safer cyber ecosystem in Albania. For the same period, CIIIOs increased their commitment to cyber security projects by investing 1.1 million euros.

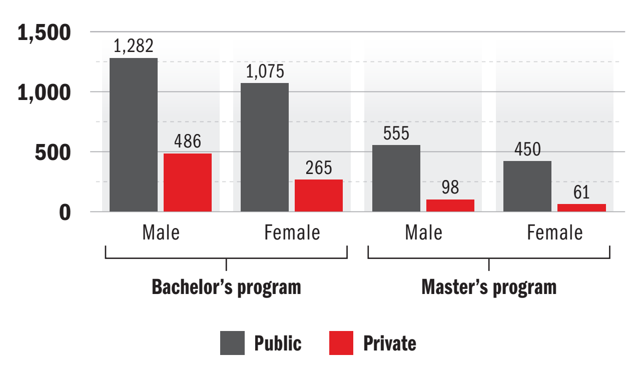
There is a threat common to public institutions that may quietly erode their defenses: cyber security brain drain. Contributing factors are low salaries at public institutions and manual processes for maintaining existing systems — boring manual work for highly skilled experts often results in dissatisfaction and brain drain. The results of the survey found that only 35% of cyber security experts in the sectors analyzed hold a valid international certificate, such as Certified Chief Information Security Officer (CCISO), Certified Information Security Professional or ISO 27001 (International Organization for Standardization).

Figure 1: **Number of cyber security experts in CIIIOs**



Sources: Dr. Vilma Tomco and Klorenta Janushi

Figure 2: **Students studying cyber security in higher education in Albania, 2019**



Sources: Dr. Vilma Tomco and Klorenta Janushi

Water gushes from the dam in Vau i Dejes on the Drin River in northern Albania. A qualified cyber security workforce is essential to protect critical infrastructure, such as this dam. REUTERS

Dea Rrozhani and Jonada Shukarasi, both 16, created GjejZa, an application to fight domestic violence. More women seeking careers in information technology will help offset the human capital shortage. REUTERS

Cyber security students

A survey of institutions of higher education in Albania conducted by NAECCS in 2019 analyzed the student demography, categorized by gender and level of study (bachelor's degrees and master's degrees). Figure 2 shows the difference in the number of males and females and how after graduation, they will increase the level of cyber expertise in the market.

Lectures on cyber security are in 20% of the total curricula in public universities, 15% in private universities and 10% in professional training centers. NAECCS plays a fundamental role in increasing the number of cyber experts in Albania by increasing the number of students trained in the field. Since 2017, NAECCS has organized the Albanian Cyber Academy (ACA), aiming to increase student interest in the field of cyber security. ACA invites local and international experts on cyber security and students of information and communications technology (ICT) to deepen their knowledge and to network within the field.

Every year NAECCS organizes a conference themed "Women in ICT Day" to have successful women from the ICT field share insights and motivate young people to choose a career in cyber security. Women in Albania hold the highest decision-maker positions in ICT, as directors general, CIOs and CISOs.

Conclusions

Organizations have a clear responsibility to improve their information technology security staff training and retention programs, and particularly to attract junior staff. In the future, we will see an expansion of cyber security content across all curriculum, as all students represent potential new entrants into the cyber security workforce. Professional development is critical because the nature of the threat evolves quickly. Professionals can use many options to augment their skills, including certificates, additional university degrees and hands-on courses to develop specific technical skills.

Since university curricula has a long process for approval, professional training centers can help address the needs by organizing short-term courses for information security technicians, analysts and auditors.

As the data in Albania show, women are more focused and loyal to their work, so it is crucial to invest in and attract more women to the cyber security domain. This can be achieved with awareness campaigns and activities, such as competitions, hackathons, conferences and university guidance, among other efforts. □