A COLLABORATIVE APPROACH

Serbia's Cyber Security Education, Training and Workforce Development Strategy

By **Jelica Vujadinović** and **Dr. Marko Krstić**
Serbian National Computer Emergency Response Team

The Serbian government's significant digitalization efforts have resulted in increased efficiency and more transparency in its public services but have also exposed the country to cyber attacks. Addressing this problem inadequately could degrade the public's well-being by destroying economic gains and disrupting the services crucial to everyday operations, such as electricity production and delivery.

Since formal education in the field of cyber security is still emerging — with a few master's programs currently available — the government identified this gap and appointed the Serbian National Computer Emergency Response Team (SRB-CERT) as the authority to develop nonformal education for critical infrastructure operators. SRB-CERT has some experience in providing education; one of its members helped design a cyber security course and is now an information-technology industry lecturer for the course at Master 4.0 Advance Information Technology Applications in Digital Transformations, a program provided by a consortium of faculties.

Education Strategy

The strategy adopted by SRB-CERT combines two principles: Act promptly and be proactive about emerging threats. New amendments to the Law on Information Security were adopted in 2019, instructing the Ministry of Trade, Tourism and Telecommunications to create a list of critical infrastructure operators. Even before the ministry created the list, SRB-CERT began to provide training to local governments, which are the stakeholders with the least specific information and communications technology infrastructure. Communication and cooperation with local governments were facilitated by the National Alliance for Local Economic Development. Cooperation and information sharing were further enhanced through a public-private partnership with Microsoft, which was selected because it is the principal vendor of operating systems for local governments.

Artificial intelligence (AI) had been recognized as the emerging technology that could most significantly increase the benefits of digitalization, but it also introduces new attack vectors. To prepare for future e-government challenges, SRB-CERT started examining the implications of AI for the threat landscape. At the time, the working group formed by the government was drafting the Strategy for the Development of Artificial Intelligence in the Republic of Serbia for 2020-2025, and it was vital for them to consider the AI security aspect. It was good timing for the SRB-CERT team to present results of their research on the potential impact of AI on cyber security at the 2019 International Telecommunications Forum in Belgrade.

Educating Local Governments

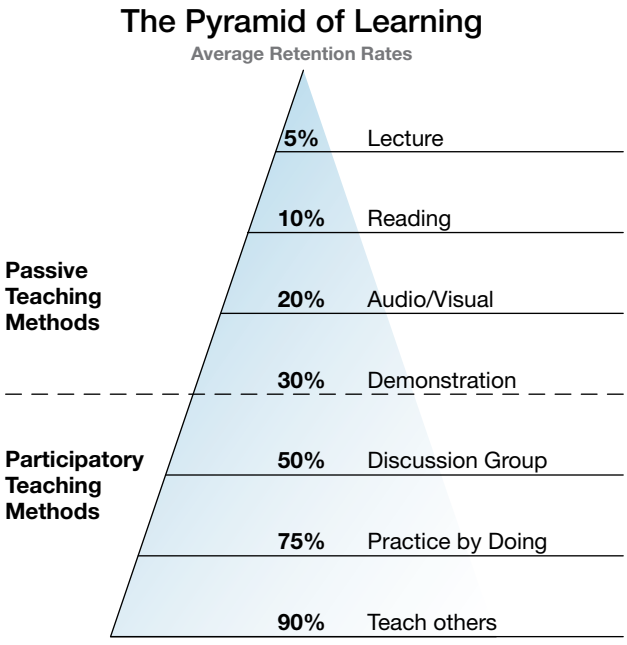
Training for local governments consisted of a legal component, intended for managers and technical staff, and a technical component for system administrators.

The legal component was organized to consider theoretical and practical aspects. Participants had the opportunity to find out more about a Confidentiality-Integrity-Availability concept, active threats, cyber security incidents, security measures, a Plan-Do-Check-Act model and to get familiar with the Law on Information Security. The practical part focused on the Cybersecurity Act model, developed by SRB-CERT to support critical infrastructure operators in delivering this document, which is mandatory for their organizations under the legislation. During the training, the participants had the opportunity to write a procedure to address one of the 28 security measures adopted by the Law on Information Security from the ISO/IEC (a joint technical committee of the International Organization for Standardization and the International Electrotechnical Commission) 27000 family of standards and described in the Cybersecurity Act model.

System administrators from local governments learned about common attacks in a Windows environment, authentication protocols, credential theft opportunities and the systematic defense approach proposed by Microsoft's experts through a series of theoretical presentations and practical exercises on the Cyber Attacks Simulation System, which was specially developed for this purpose.

Concepts of training were selected to combine the passive and active teaching methods of the pyramid of learning. The participants could attend lectures, read, access audio and visual content, observe demonstrations and participate in discussions and practical work. Furthermore, because SRB-CERT members rotated as trainers, they all benefited from the role of educator, which gave them a chance to improve their knowledge.

Participants listen to a panel at a seminar for local governments in Kragujevac in October 2019. SRB-CERT



Source: Adapted from the National Training Laboratories, Bethel, Maine

Special attention was paid to standardization, in line with Global Forum on Cyber Expertise efforts to adapt and adopt the National Initiative for Cybersecurity Education (NICE) Workforce Framework in Europe. The technical component combined the important knowledge, skills and abilities (KSAs) from the system administrator, cyber defense analyst, system security analyst, cyber defense incident responder and vulnerability assessment analyst roles. This resulted in the following KSAs, which describe the competencies developed through the training:

Knowledge of:

- Cyber security and privacy principles.
- Cyber threats and vulnerabilities.
- Specific operational impacts of cyber security lapses.
- Organizational information technology user security policies.
- System administration, network and operating system hardening techniques.
- Application vulnerabilities.
- Cryptologic capabilities, limitations and contributions to cyber operations.
- Current software and methodologies for an active defense and system hardening.
- Methods and techniques used to detect various exploitation activities.

Skills in:

- Maintaining directory services.
- Extracting information from packet captures.
- Verifying the integrity of all files.

Abilities to:

- Apply cyber security and privacy principles to organizational requirements.
- Monitor system operations and react to events in response to triggers and/or observed trends or unusual activity.

Nearly 200 participants from 79 local governments have attended training by SRB-CERT. The training was made available in every region of Serbia: the Central and Western region, the Southern and Eastern region, the Northern region and the Belgrade region. After each session, the participants were interviewed to measure their satisfaction and to identify room for improvement.

Future Threats From AI

Future threats from AI were analyzed using possible applications of machine learning (ML) in CERT operations. This topic was selected for three reasons:

- To inform the academic audience about the jobs and tasks of the cyber security workforce in a CERT team.
- To describe how ML could increase the efficiency of CERT operations.
- To raise awareness about the security aspects of AI.

Even though the focus remains on the development of specialized training, the presentation revealed important facts for further workforce development. The potential of ML for CERT services became evident, including security-related information dissemination, incident handling, malware analysis and cyber exercises. However, using this technology comes with a risk. Although the National Institute for Standards and Technology is still working on the ML attack taxonomy, not all attacks are equally probable, nor do they lead to the same consequences. This means that models of attackers' realistic capabilities need to be considered during threat analysis, and the secure software development life cycle must include vulnerability scanning and model hardening.

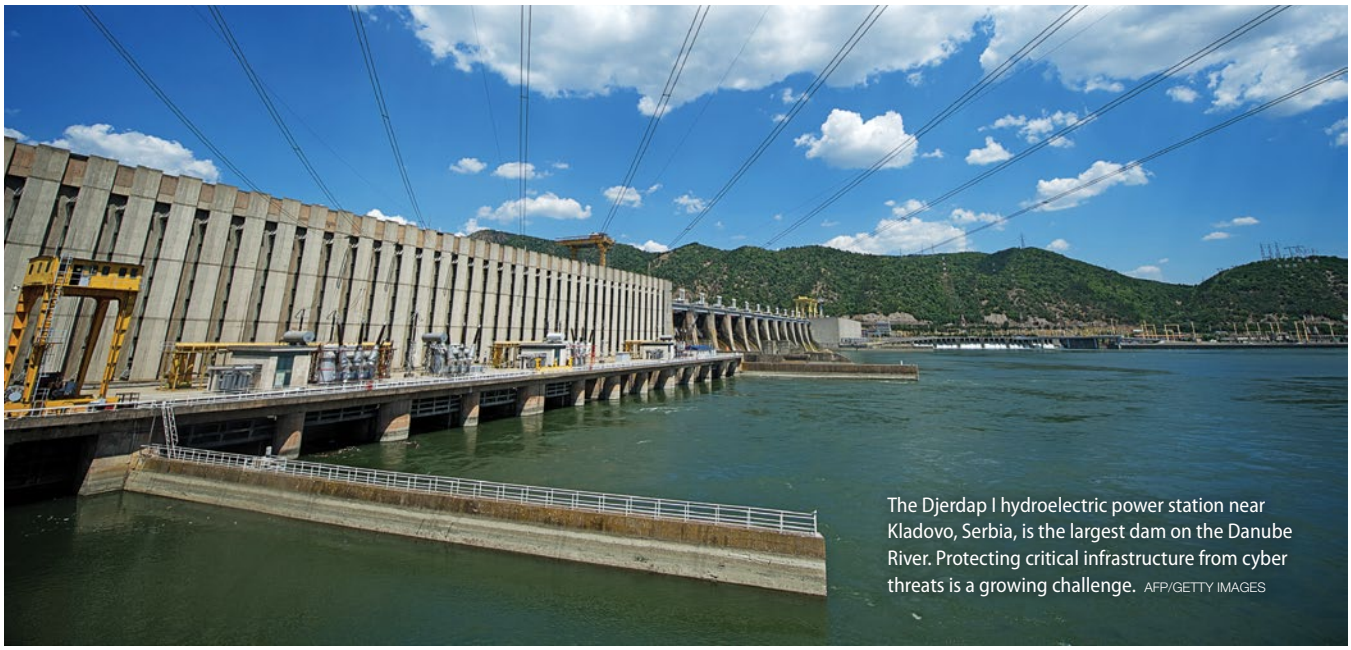
Even though, so far, the current version of the NICE framework recognizes ML theory and principles only as an important aspect of the data analyst role, it has a much greater potential to transform many other work roles as well.

The positive impact of the presentation cannot be overstated, and the Strategy for the Development of Artificial Intelligence, which was adopted several months later, addressed the security aspects accordingly.

Conclusion

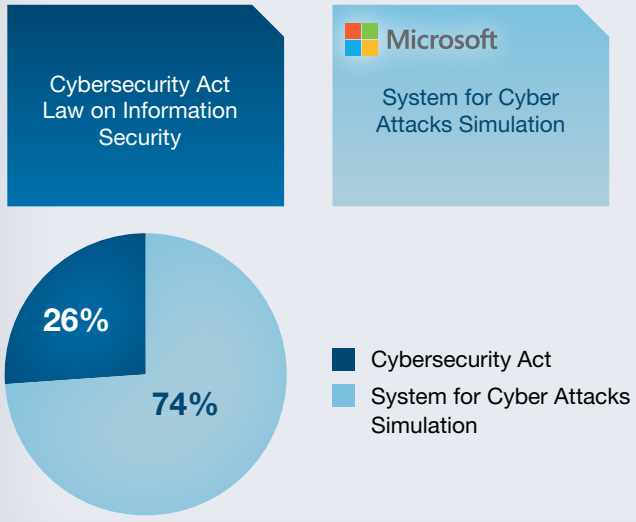
Serbia is the only country in Southeast Europe that has adopted the standardization approach in designing training and establishing a Strategy for the Development of Artificial Intelligence, offering a unique opportunity for other countries to learn from Serbia's experience and results.

The training for local governments provided by SRB-CERT resulted in increased trust, enhanced cyber awareness and improved knowledge, leading to an increased number of incidents reported by local governments. This process also made it possible to identify improvements for



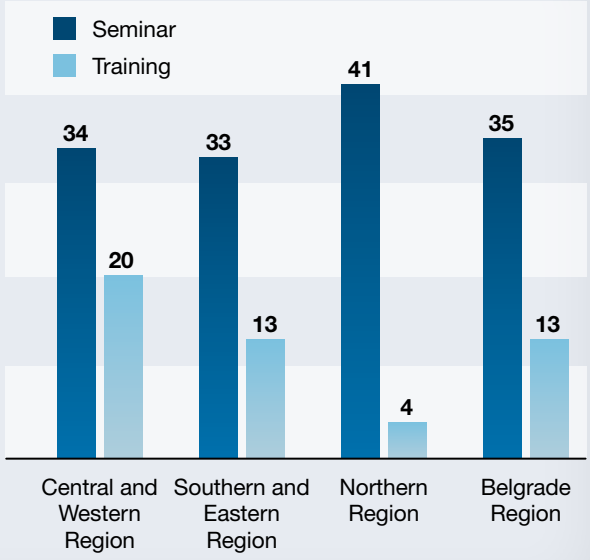
The Djerdap I hydroelectric power station near Kladovo, Serbia, is the largest dam on the Danube River. Protecting critical infrastructure from cyber threats is a growing challenge. AFP/GETTY IMAGES

Seminars | Technical Trainings



Source: Adapted from the National Training Laboratories, Bethel, Maine

Participants Per Region



Source: SRB-CERT

subsequent training. The knowledge, skills and abilities of the SRB-CERT members have been significantly improved, and it has been confirmed that the Cybersecurity Act model developed by SRB-CERT can be applied and easily adjusted to any of the participant organizations. Although the results of the training standardization cannot be detected in this short period, it is expected that more accurate information about work roles and training requirements will be available in a future phase. The focus of future training will be on the development of advanced education for local governments and, by following the same methodology, on a basic level of instruction for other operators of critical infrastructure.

The first steps in making AI-related security training have already been taken. Further research is needed to fully define the syllabus, the target audience and learning methods. A recent study by the Future of Humanity Institute at Oxford University in the United Kingdom showed that scientific research on AI offense-defense balance is different from research on computer security because there is a much greater probability of revealing methods that adversaries would not discover by themselves but are capable of exploiting for attacks. It is, therefore, recommended to discuss offensive aspects together with defensive solutions and to avoid providing information about attacks that contain not-so-easily-patched social components, whereas special precaution should be taken in situations when source codes are shared. □