DCAF Geneva Centre for Security Sector Governance

DCAF - Geneva Centre for Security Sector Governance

Regional Conference on Cybersecurity Capacity Building in the Western Balkans

Podgorica, Montenegro

9 and 10 May 2022

REPORT

By Dr. Mika Kerttunen

Introduction

DCAF – Geneva Centre for Security Sector Governance's **Regional Conference on Cybersecurity Capacity Building in the Western Balkans** was held in in Podgorica, Montenegro, on 9 and 10 May 2022. The Conference was organized as part of DCAF's regional project 'Good Governance in Cybersecurity in the Western Balkans', funded by the United Kingdom Government Foreign, Commonwealth and Development Office (FCDO), and in cooperation with the Ministry of Public Administration of the Government of Montenegro.

The conference centred on cybersecurity capacity building, cyber education, the development of cybersecurity courses and programmes, and how to improve cyber resilience and readiness. The presentations, panels and workshops covered a range of issues related to training, such as best practices in cybersecurity education and advice for policy makers, what training is most needed in the public sector, experiences in developing cybersecurity courses at the higher education level as well as designing and running cybersecurity exercises and hackathons for students. The Conference program and other detailed information is available at: https://www.dcaf.ch/regional-conference-cybersecurity-capacity-building.

9 MAY Plenary Discussions

The panel discussions and presentations brought out some cross-cutting themes. Two central questions were raised repeatedly: What expertise do the Western Balkan economies need? How can the identified needs be met given the general lack of competent workforce?

Formal and informal education

Two education frameworks were noted: formal, or academic education, which is still the most common, and informal, or professional education, which is newer but increasingly recognized as very important. It was noted that all these frameworks and approaches have their advantages and that they are not exclusive. Participants discussed that:

- Both formal and informal education are needed in cybersecurity.
- Whether to focus more on formal or informal approaches, depends on:
    - the current state of national cybersecurity,
    - the work force skills and competences,
    - the available educational programs, and
    - the anticipated market and technological development.

Top down and bottom-up education

The participants also identified two approaches to cybersecurity learning processes: A "top-down" approach, where a larger public or private education institution sets up and organises education programmes or activities, imposing the teaching programme, and a "bottom-up" approach, where cybersecurity experts take the initiative to teach their peers through informal exchanges or more structured self-organised training sessions, shaping the content and topics needed for the trainings. They concluded that:

- Both top-down and bottom-up education are needed in cybersecurity.
- Advantages of "Top-down" education:
    - can better foster the long-term and whole-of-nation needs,
    - can facilitate inter-agency as well as public-private cooperation,
    - can help raising cybersecurity awareness in the general public and private sector,
    - can steer public attention and cross-ministerial funding to cybersecurity education, at different levels of schooling.
- Advantages of "Bottom-up" education:
    - is more agile in targeting specific and sectorial issues,
    - is able to spread baseline competences among staff, especially in the public sector but also enterprises.
- Foreign, including regional, experiences and lessons learned are valuable in the improvement of cybersecurity level. International and regional experiences shared at the conference allowed participants to identify good practices that may stimulate national and organizational thinking. Still, nationally identified needs and ambitions should determine the initiation and implementation of educational programs and projects specific to each economy.

How to strategically plan cybersecurity education

Several times, speakers and participants emphasised the importance of planning national cybersecurity capacity building strategically. For example, countries should consider including a section on cybersecurity education and capacity building in national cybersecurity strategies. In this context, discussions focused on the following:

- A thorough needs assessment is necessary before cybersecurity education is planned. How educational needs are defined and determined also condition the choices and emphasis of the curricula.
- It is important to have a balance between technical studies and competencies, and those of 'non-technical' nature. It was widely recognized that while technical disciplines (e.g. information technology, computer science, or digital forensics) constitute the core of cybersecurity, there is no one, clear profession of cybersecurity: skills such as law,

international law, law enforcement, behavioural science, economics, marketing, and political science and security studies, are equally needed.

Three important questions for designing cybersecurity education were identified:

- Where are we, as countries, organisations, and individual experts, in terms of our cybersecurity expertise?
- What kind of cybersecurity expertise do we need (and why)?
- What kind of education do we need to achieve this level of cybersecurity expertise in our country / organisation / at individual level?

Higher education as well as professional and vocational education

There are several different, relevant ways for the development of cybersecurity education: higher education, professional and vocational trainings. The conference participants agreed that rather than opposing the two approaches, it would be important to see and seize the advantages of both approaches. These include:

- Advantages of academic courses:
    - to provide the best solutions in response to certain needs,
    - to educate and train students into cybersecurity professionals and experts.
- Advantages of professional and vocational education (internships and on-the-job trainings):
    - can tackle skills and competencies needs, as they offer more practical, rapid, and rather sustainable ways to complement previous knowledge of the staff and target specific needs and shortfalls,
    - can help find (and possibly keep) new talent,
    - can help the institution that organises the internships to expand the professional network (former interns will remain connections regardless of where they will later work).

10 MAY Workshops

The second day of the Conference contained two parallel workshops: Workshop 1 on how to organize national cyber drill, and Workshop 2 on the development of educational programmes and hackathons for pupils at high school level.

Workshop 1 – How to organise national cyber drill

Based on the joint presentation of two national experts and one academic commentator, the Workshop 1 participants discussed the educational and organizational parameters of organizing a national or organizational cybersecurity exercise.

It was widely emphasised that the identified needs should determine the outline of a cybersecurity exercise. There is no one format, fashion, content or conduct which would automatically and without contingent consideration fit. Drills and exercises can, for example, be organized to improve or test individual, organizational or inter-organizational skills or procedures; similarly, the target audiences will vary by organization, profession, nationality, and maturity. For some drills, a short, written scenario is all that is needed to launch critical thinking and interaction, for others, a simulated environment of responders, operators, decision-makers as well as red teams and judges would make a difference. Above all, drills should help the country or organisation prepare for crisis, and give indications on the steps to follow in any cases and situations. Education is rewarding as such, but occasionally token, and tangible rewards make the day.

A number of guidebooks and manuals by national institutions or international organisations on how to organise cybersecurity exercises exist already.[1] They do not offer easy copy-paste solutions, but discuss general parameters for organizing large scale drills and exercises. The Workshop participants recognized the practical and educational benefits of regional and wider international cooperation in organizing cybersecurity drills and exercises. For once, it was recognized that one does not necessarily need a big budget to carry out a useful cybersecurity exercise.

Workshop 2 – Development of educational programmes and hackathons for pupils at high school level

In this workshop, participants exchanged experiences in fostering new cybersecurity talent through hackathons. An alliance of Serbian universities and high schools, with the support from the private sector and government institutions as well as the national CERT, has successfully organised hackathons for Serbian high school pupils. The speaker outlined the importance of good preparation of activities and the coordination of organisers and the many volunteers who help train the hackathon teams. Regional or European-wide cooperation with other hackathon initiatives was also considered useful. A representative from the Albanian National Authority for Electronic Certification and Cybersecurity shared information on the many different initiatives the Authority has organised for pupils, from awareness raising to hackathons.

[1] National Exercise - Good Practice Guide — ENISA (europa.eu)
SP 800-84, Test, Training and Exercise Programs for IT Plans & Capabilities | CSRC (nist.gov)
Organiser un exercice de gestion de crise cyber | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

Conclusion

The Conference underlined how education in its various forms can strengthen national and organizational cybersecurity. Successful and sustainable cybersecurity education recognizes local needs, making education not only relevant by tailored and targeted content but also by its individual and societal impact. Domestic, regional and wider international cooperation, e.g. in the forms of multistakeholder and multidisciplinary engagement, public-private partnership and joint or co-run educational institutions, programs and training and exercise events will enhance the desired outcomes.