06

CAPACITY BUILDING

VLADIMIR RADUNOVIĆ, DIPLO FOUNDATION;
TAYLOR ROBERTS, GLOBAL CYBER SECURITY CAPACITY CENTRE, UNIVERSITY OF OXFORD

INTRODUCTION

Cybersecurity capacity building has become an area of common interest for several governments across the world. However, there is little common understanding as to what capacity in cybersecurity consists of. This training will provide participants with a fundamental understanding and overview of the landscape of cybersecurity capacity building.

THE WHAT – WHAT IS THE TOPIC ABOUT?

The webinar and training will focus on cybersecurity capacity building with a focus on freedom, security and growth. Cybersecurity capacity should not be limited to technical capacity, but expanded to include policy and strategy, society and culture, education and training, legislation and regulation, as well as standardisation and market development. Capacity building goes far beyond single training - it needs to be approached comprehensively and with a blended-learning format that should ensure learning and understanding, allow time for reflections and building own positions, then coaching people into getting involved with policy processes and being comfortable to engage and contribute within them.

THE WHY – WHY IS THIS TOPIC IMPORTANT?

Capacity development has been a central theme within development for several decades. In order to ensure that people around the world can reap the benefits of the Internet and information communication technologies (ICT's), capacity building in cyberspace has now become a pillar of many government's foreign policy approach, and has emerged as a potential area of cooperation not only between governments, but also between public, private and civil society sectors.

Given the breadth of cyber capacity building fora, there are several areas of potential benefit as well. Building policy for development in cyberspace will enhance the overall strategic coordination and implementation of efforts. Raising awareness of cybersecurity and other initiatives will increase social participation in key debates, ensuring societal values are taken in consideration when developing policy and legislation, while at the same time raising the overall

security and economic level of the country. Formal education and training in ICT and cybersecurity will enable social growth through a more technically skilled workforce. Building frameworks for legislation and regulation on issues concerning cyberspace will help to ensure freedoms, security and economic growth. Finally, implementing technical standards will enable the adoption of best practices during technical infrastructure development.

THE WHO, WHERE AND WHEN – WHO ARE THE MAIN PLAYERS, WHERE AND WHEN IS THE TOPIC BEING ADDRESSED?

Capacity building is necessarily a multi-stakeholder endeavor, as cyber capacity spans the public, private and civil society sectors. Here is a non-exhaustive list of actors that may be involved:

- ministries
- information technologies
- defense
- interior
- foreign affairs
- education
- health
- economy
- commerce
- transportation
- justice and attorney general's office
- academia
- Internet governance representatives
- Internet Society chapters
- criminal justice community
- intelligence community
- legislators
- national security representatives
- CERT/CSIRT teams
- major commercial sectors and SME's
- finance sector
- telecommunications companies.

An approach which involves different stakeholders and professional cultures enables knowledge-sharing across these institutional silos, and improves inter-professional communication and understanding. It also enables a more holistic understanding of cyber-security, discussed from various angles: technology, law, economy, societal perspective, international relations and diplomacy.

Regardless of whether a new capacity building program is being developed, or if an institution is looking for partners to implement an existing one, there are several dimensions to look at, depending on the target audience:

- For Whom: The capacity building program needs to be adjusted according to specific target audiences. Thus the main starting question is who is the target audience (e.g. technical community, law enforcement, governmental institutions, corporate sector, youth activists)? Besides, what is the target level of the targeted audiences (high level, coordination and management level, operational level)?

- What: What is the thematic focus (e.g. overall cybersecurity, cybercrime, international peace and security, Internet safety and child protection, digital rights, policy and strategic planning, Internet governance)? What is the desired perspective (e.g. policy, technology, legal, diplomatic)?

- Where and when: Traditional approaches include in-situ workshops, panels, simulations, case studies etc. The Internet has also enabled online courses, webinars and similar 'remote' events enabling remote participation at lower costs and extending the outreach from national to regional or global level participation. Timing is equally important and the combination of online and in-situ activities throughout the year(s).

THE HOW – HOW IS THIS TOPIC BEING ADDRESSED?

There are several organisations with various areas of expertise that seek to enhance cyber capacity building. Some organisations, such as the Forum for Incident Response and Security Teams (FIRST) and the International Telecommunications Union (ITU) have invested resources in Computer Incident Response Team (CIRT) development. Other organisations, such as the European Union Agency for Network and Information Security (ENISA) and Organisation of American States (OAS) have adopted a regional approach to capacity building, working with particular countries across a range of capacity building areas, such as national cybersecurity strategies and crisis management. Given the breadth of cybersecurity issues, the Global Cyber Security Capacity Centre at the University of Oxford has developed a capability maturity model (CMM) that helps a nation comprehensively assess their cybersecurity capacity in order to guide more strategic investment. In addition to these organisational approaches to capacity building, individual countries have begun to develop programmes that seek to deliver capacity in various areas.

In order to connect these numerous initiatives together, GCCS 2015 will launch the Global Forum on Cyber Expertise, which seeks to stimulate new funding streams and the sharing of expertise and experiences. By matching supply and demand, countries that lack knowledge in certain cyber areas can benefit from the knowledge and expertise that will be provided by countries and companies with more experience in cyber matters.

CONCLUSION

Capacity building has become a very frequent term in cybersecurity-related discussions around the globe. At the same time, developing an effective and efficient capacity building program is not easy - it requires sustainable funding, skills, continuity and comprehensive methodology and didactics. In developing new programmes or engaging with the existing programmes, it is important to look into specific elements that can ensure the desired impact. There is number of existing capacity building programmes around the world, which should be better mapped and utilised.