CYBER SECURITY
Inter-American Committee against Terrorism
Secretariat for Multidimensional Security

OAS | More rights for more people

Session title:
Towards an inclusive cybersecurity capacity building approach

Date:
21st December 2017

Time:
11:50 to 13:20

Workshop Organiser:
Belisario Contreras, Cybersecurity Program Manager, Inter-American Committee against Terrorism (CICTE), Secretariat for Multidimensional Security**,** Organization of American States (OAS)

Chairperson/Moderator:
Belisario Contreras

Rapporteur/Note Taker:
Daniela Schnidrig, Global Partners Digital

List of Speakers and their institutional affiliations:

- Kaja Ciglic, Microsoft
- Lea Kaspar, Global Partners Digital
- Liesyl Franz, U.S. Department of State
- Carolin Weisser, University of Oxford, Global Cyber Security Capacity Centre
- Chris Painter, Global Commission on the Stability of Cyberspace
- Felix Antonio Barrio Juarez, Spanish National Cybersecurity Institute

Key Issues raised (1 sentence per issue):

- Benefits of adopting a multistakeholder approach to cybersecurity capacity building.
- Challenges that may come up when adopting a multistakeholder approach to cybersecurity capacity building.
- Good practices to overcome challenges to adopting multistakeholder approaches to cybersecurity capacity building.

If there are Presentations during the workshop session, please provide a 1-paragraph summary for each Presentation

N/A

Please describe the Discussions that took place during the workshop session: (3 paragraphs)

Some of the benefits of adopting a multistakeholder approach to cybersecurity capacity building that discussants identified are the following:

- Inclusive approaches and working with other stakeholders are not only important to learn good security best practices, but also to exchange lessons learned and improve internal processes.
- For all nations to benefit from cyberspace, the internet has to be open, interoperable, secure and reliable. Dealing with cybersecurity issues cannot be done by one actor or in one specific way. It's necessary to adopt an inclusive approach and to work with several stakeholders.
- Inclusive approaches to cybersecurity policymaking benefit from expertise and lead to better outcomes.

Some of the challenges that might come up when adopting a multistakeholder approach to cybersecurity capacity building identified by discussants are the following:

- Different definitions and understandings of cybersecurity. Issues under cybersecurity can sometimes get conflated (for example content regulation, cybercrime and network security)
- Lack of awareness with regard to cybersecurity and cyber capacity building.
- Multistakeholder approaches are very developed in internet governance. However, when extrapolating this to the cyber field, the level or the normative principles that underpin Internet governance are not necessarily the same that underpin some of the cybersecurity discussions. The nature of the actors involved might also bring specific challenges when it comes to implementing the approach.
- Lack of practical guidance to implementing inclusive approaches.

Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways: (3 paragraphs)

Some key lessons identified by discussants are:

- It's crucial to link different capacity building efforts to ensure that they are leveraged. The Global Forum on Cyber Expertise (GFCE), and other initiatives aim to do this.
- Approaches to cybersecurity capacity building need to be holistic and multidisciplinary

- Sharing best practices is crucial. Global exchange of opinions allow for exchanges with different countries.
- Capacity building is not one course, or training - it's a comprehensive process, which can last for years. The ever-evolving landscape of the internet is a challenge for which there's not a static solution – it is therefore key to keep reassessing and learning.
- Example of good practice - NIST cybersecurity framework, which was a bottom up process. It was convened by one institution but fuelled by other stakeholders.

Gender Reporting

- Estimate the overall number of the participants present at the session: cca 50 participants.

- Estimate the overall number of women present at the session: cca 25.

- To what extent did the session discuss gender equality and/or women's empowerment?

The session touched upon challenges in inclusive cybersecurity capacity building, including the lack of women in the cybersecurity field.

- If the session addressed issues related to gender equality and/or women's empowerment, please provide a brief summary of the discussion:

With regard to the gender divide and the lack of women in the cybersecurity workforce, it was recognised during the session that it is a problem across the tech sector in general. This issue is very complex and not a problem to be solved quickly but with a holistic, sustainable approach. It was also recognised that it's key to start with education very early on. Representatives of the OAS/CICTE Cybersecurity Program and of the Spanish National Cybersecurity Institute brought to attention the initiate on Gender and Cybersecurity co-sponsored by the Government of Spain and by the General Secretariat of the OAS in the framework of the GFCE. A first workshop on "Gender and Cybersecurity: Creating a more inclusive digital world" was organized by the OAS/CICTE Cybersecurity Program and Spanish National Cybersecurity Institute in June 2017 in Leon, Spain.