For Whom and by Whom? Achieving Locally Sustainable Impact through Digital Security Capacity Building

Objectives and aims

The workshop will aim to discuss, and look to answer, the following high level digital security capacity building relevant questions:

- What does success look like? How do we define and measure success in digital capacity building?
- What challenges, opportunities, risks and benefits exist in the multistakeholder approach to digital capacity building?
- What are the context specific challenges from a post conflict/high risk digital capacity building perspective?

Approach

We will work towards answering the above questions by:

- Identifying "Digital Success" pathways and strategies of countries in the region. How has digital security capacity building aided, or impeded, success? Which digital security capacity building measures have worked, and which have not worked.
- Exploring how greater cooperation can be fostered for better digital security.
- Better understanding the benefits and risks of digital security capacity building.
- Assessing top-down, grassroots and hybrid approaches to digital security capacity building, considering the similarities and differences in each practice.
- Highlighting and promoting the necessity and advantages of local ownership vs externally imposed requirements, priorities and solutions.

Caveats:

As identified in the DSLA's previous workshop report, we recognise that for many academic fields there is an important distinction between 'cyber security' and 'digital security'. However, we also acknowledge that in practice, the term is often used interchangeably.

As our name suggests, we are keen to use the term 'digital security' because it helps to include a set of wider concerns that at times are often not associated with 'cyber security'. In this regard, it may be useful to see 'digital security' as a wider umbrella term that includes cyber security, but would also include issues of, for example, digital access, digital rights, and user experience amongst other important topics.

Throughout the workshop, we are likely to use the terms interchangeably, and want participants to use the term that they are more comfortable using. We are aware that the topic of discussion is often referred to as 'cyber security capacity building' in the literature, so it is important to engage with this terminology.

We recognise that holding the workshop in English may limit the contribution of some participants. Unfortunately, we currently do not have the necessary structure to hold spanish and english break out rooms. Some of our organisers are able to act as translators, but we also encourage other bilingual participants to act as facilitators by helping to translate ideas during the discussions when needed.

Structure of workshop:

The workshop will be structured around three topic areas. These topic areas are designed to bring together a variety of academic, practitioner, and industry perspectives on digital security capacity building. We hope to facilitate discussions that explore the areas of agreement and contention between these different fields.

The workshop will start off with a panel discussion with representatives from different fields, providing participants with an initial point for discussion.

Participants will then be split into groups. Group allocations will be made based on academic/work backgrounds. You will have the opportunity to indicate your topic preference. The organising team will try to place you in your 1st choice, but depending on numbers, you may be allocated in your 2nd choice.

Workshop Schedule:

<table>
<tr><td colspan="3">Introduction (10 min)</td></tr>
<tr><td colspan="3">Panel Discussion and Q&A (40min)</td></tr>
<tr><td colspan="3">Break (10 min)</td></tr>
<tr><td colspan="3">Break Out Rooms (30 min)</td></tr>
<tr><td>Topic 1 Discussion: Success in Digital Security Capacity Building</td><td>Topic 2 Discussion: Multi Stakeholder Digital Security Capacity Building</td><td>Topic 3 Discussion: Digital Security Capacity Building in Post Conflict/ High-Risk Scenarios</td></tr>
<tr><td colspan="3">Feedback Break out Rooms (10 min)</td></tr>
<tr><td colspan="3">Closing Remarks (10 min)</td></tr>
</table>

Workshop Topics:

1) Success in Digital Security Capacity Building
    a) What does it look like? How do we measure success?
    b) What are good examples in the region?
    c) Are there any shortcomings or unintended consequences of the current way success is being measured?
    d) What is the security designed to enable or to impede?
    e) What are the risks, as well as the benefits?
    f) What is the role of education in capacity building, and at what level? What are the risks/benefits of digital security capacity building involvement in education, and how do we balance between internally provisioned and externally imposed education programmes?

2) Multi Stakeholder Digital Security Capacity Building
    a) Who are the main actors in digital security capacity building?
    b) What challenges emerge for capacity building with the presence of multiple donor entities?
    c) How can we better facilitate complementary efforts in digital security capacity building?

   d) What is the role of maturity models? How do they impact identification and prioritisation of digital security capacity building requirements? What is the perception from a recipient perspective?
   e) Is digital legislation and policy/strategy formation a relevant and effective area for digital security capacity building?

3) Digital Security Capacity Building in Conflict, Post-Conflict or High-Risk Scenarios?
   a) How do we define and identify conflict/post conflict and high-risk scenarios?
   b) How do you build capacity building that takes into account fragile contexts?
   c) What is the role of grassroot capacity building efforts in these contexts?
   d) Building and maintaining support for capacity building in complex contexts.

Workshop Organisers & Contact Information

Jessica McClearn
Royal Holloway, University of London
jessica.mcclearn.2021@live.rhul.ac.uk

James Barr
Royal Holloway, University of London
james.barr.2020@live.rhul.ac.uk

Phil Sheriff
Royal Holloway, University of London
Phil.Sheriff.2022@live.rhul.ac.uk

Sofia Liemann Escobar
Royal Holloway, University of London
sofia.liemannescobar.2020@live.rhul.ac.uk