Solidarity Playbook: Case studies on cybersecurity

Research Consultant - Terms of Reference

22 June 2022

1 Overview

The International Civil Society Centre (ICSCentre) is looking for a research consultant to support its Solidarity Action Network (SANE) with capturing three to five case studies looking at how (international) civil society organisations – (I)CSOs – have dealt with cyberattacks and digital risks. This will be an extension of the Solidarity Playbook – a collection of case studies and best practices on strategies, resilience, and solidarity mechanisms – with a topical focus on cybersecurity. The aim is to make experience, strategies and lessons learned available for other civil society actors who have faced or might face similar attacks and challenges in the future. The cases will address (I)CSO professionals across departments (non-technical audience) as cybersecurity needs to be everyone's responsibility.

2 Background information

The Solidarity Action Network (SANE), hosted by the International Civil Society Centre (ICSCentre), focuses on strengthening resilience of and solidarity among civil society actors when faced with civic space restrictions or changing operating conditions. It connects international and national civil society organisations – (I)CSOs – across all sub-sectors and brings them into discussions on civic space challenges and opportunities.

The Solidarity Playbook is an integral part of SANE with a focus on collecting case studies and best practices to help other (I)CSOs respond to undue scrutiny and challenges, and to enable learning on how to act in solidarity with civil society actors, particularly local partners.

The Solidarity Playbook particularly captures:

- **Strategies and resilience mechanisms of ICSOs** developed to respond to civic space restrictions and changing operating conditions for civil society (e.g. legal restrictions, bureaucratic clampdowns, financial constraints, disinformation attacks or digital risks).
- **Coalition responses to civic space restrictions** that demonstrate how civil society actors can respond to threats and challenges with a unified voice.

Building on positive feedback of the Playbook's first (2019) and second edition (2020-2021), we are extending the collection by adding three to five case studies with a particular focus on addressing cyberattacks. The cases will show concrete experience, responses, and resilience

mechanisms developed by (I)CSOs. The examples will likely deal with phishing attacks, domain spoofing, ransomware attacks and denial-of-service (DDoS) attacks. A technical advice and recommendations will be provided by the CyberPeace Institute, with whom we have recently published "Navigating cybersecurity: Guidance for (I)CSO professionals". The case studies will be jointly identified by the ICSCentre and the CyberPeace Institute.

The new case studies will have a similar length (2,000 – 2,500 words each + executive summary) and follow a similar structure of already published Solidarity Playbook case studies. The chapters will likely encompass: 1) what happened; 2) how organisations responded; 3) outcomes; 4) organisational learnings, including experienced challenges and main lessons learned.

The published cases will be made available to ICSO and CSO professionals across departments and will also target non-technical audience as we believe cybersecurity needs to be everyone's responsibility.

3 Scope of work and key tasks

1. Review and adjust the existing framework of the Solidarity Playbook case studies to accommodate the topical focus on cybersecurity.
2. Conduct desk review and analysis of any written documentation (either publicly available or made available by contributing organisations).
3. Conduct interviews with case study partners.
4. Produce drafts of three to five case studies in a written form, including executive summary.
5. Refine the case studies based on feedback received from the case study partners, the ICSCentre and the CyberPeace Institute.
6. Submit final case studies.

4 Timeline

- 15 – 19 August 2022: Kick-off (virtual) meeting and start of work
- 29 – 31 August 2022: Adjusted framework is presented and discussed with the ICSCentre
- 1 September – 6 November 2022: Interviews with case study partners are conducted and case studies are written
- By 7 November 2022: First drafts of case studies are submitted
- By 30 November 2022: Final case studies are submitted

We expect the overall consultancy to encompass max. 10 working days if five cases are selected (the expected workload is 1,5 – 2 days per each case).

5 Experience and skills/competencies

- At least a bachelor's degree in a relevant field (political science, social sciences, international relations or similar)
- At least 5 years proven experience conducting research and analysis (political or social science), preferably on civil society space (more specifically civil society's freedom to act independently, unrestricted and effectively)
- Excellent English writing skills, with affinity to editing, layout and attention to detail
- Experience working on issues related to cybersecurity and digital risks is a huge asset
- Experience working with civil society actors (ICSOs, CSOs) and expert knowledge of the civil society sector
- Ability to explain complex issues to non-technical audience
- Ability to self-manage and meet project deadlines

6 Application

To apply, please send:

1. **Cover letter (no more than 3 pages)**, including:
    - A brief **description of your experience and expertise** in the field that illustrates your overall qualifications and capabilities for this scope of work, including **two examples of your previous comparable work**
    - Your **consultancy rate** (amount in EUR/day) and amount of working days
2. Your **CV**
3. **Two references** that can be contacted should you be shortlisted

to Eva Gondorová (egondorova@icscentre.org) by **25 July 2022 COB**.

If you have any questions, please reach out to Miriam Niehaus (mniehaus@icscentre.org).

Shortlisted applicants will be invited to a virtual interview in the first half of August.