International Foundation for Electoral Systems

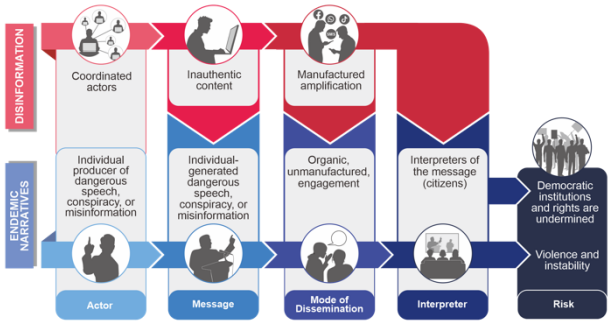
The Chain of Harm

Designing Evidence-based, Locally Led Information Integrity Programming

The Chain of Harm is a tested, replicable approach for practitioners to design evidence-based and locally-led information integrity programming that centers traditionally marginalized perspectives.

Overview

The Chain of Harm is a useful framework for practitioners in the democracy, rights and governance space, as well as those funding, designing or implementing information integrity programming in other sectors, as it breaks down the challenges of disinformation, misinformation, and dangerous speech into five inter-related intervention points (actor, message, mode of dissemination, interpreter, and risk).



Operationalizing the Chain of Harm

Operationalizing the Chain of Harm involves using the five-stage framework to drive a participatory, facilitated program design process with local partners. The goal is to improve the responsiveness of information integrity programming to the differential experiences of local communities while emphasizing the perspectives of traditionally marginalized and underrepresented groups.

Operationalizing the Chain of Harm follows an iterative structure:

1. Primary research through surveys and focus groups to understand information ecosystems and the spread and impact of DMDS, focusing on the experiences traditionally marginalized communities.
2. Local program implementers are engaged to leverage research, evaluate existing programming, and plan new interventions that respond directly to documented community needs through the Chain of Harm Co-design Workshop.
3. Interventions are implemented and led locally, and program leaders monitor progress to determine impact, especially for marginalized communities.

Chain of Harm Co-design Workshop

Piloted in Iraq and Guyana, the Co-design Workshop brings together local partners, experts, and implementers, guiding them through a process that enables them to articulate and/or expand upon an information integrity programming approach to reach previously underserved or disserved populations.

During the workshop, current or planned information integrity programming is divided into component activities and mapped along the Chain of Harm to reveal visually where there are gaps and opportunities to refine the programming approach. Focus group and survey data are shared with workshop participants before they identify actionable and interesting insights from it. Participants then go through a series of ideation activities to tap into their collective knowledge and creativity to begin connecting insights from the evidence into intervention ideas that can fill programming gaps or strengthen current programming.

To learn how to use the Chain of Harm Co-design Workshop in your own work, IFES compiled a comprehensive user guide

Future Uses

Chain of Harm Evaluation Workshop

In line with culturally responsive evaluation (CRE) approaches, the Chain of Harm can be the foundation for a participatory workshop that centers local voices and perspectives in program evaluation activities. By the end of the Evaluation Workshop process, evaluators, programmatic implementers, and local community members will have a stronger shared understanding of the impact of the information integrity programming on the information environment.

Chain of Harm Threat Modeling Workshop

The Chain of Harm can be used as a framework for participatory digital safety and cybersecurity threat modeling, with an emphasis on understanding and adapting to the different experiences of populations that are underserved by mainstream digital safety and security practices. The generated insights can be used to update existing risk models and to supplement and extend cybersecurity industry frameworks that catalogue the tactics, techniques, and procedures that known threat actors use.

HQ | 2011 Crystal Drive | Arlington, VA 22202 | USA T +1.202.350.6700 www.IFES.org