



# The Chain of Harm

---

Designing Evidence-Based,  
Locally Led Information Integrity Programming



# The Chain of Harm

Designing Evidence-Based,  
Locally Led Information Integrity Programming

---

Authors:

**Lisa Reppell**

Senior Global Social Media and Disinformation Specialist

**Brittany Hamzy**

Senior Information Integrity Officer

**Tarun Chaudhary**

Cybersecurity and Diplomacy Advisor



International Foundation  
for Electoral Systems

## **The Chain of Harm: Designing Evidence-Based, Locally Led Information Integrity Programming**

Copyright © 2024 International Foundation for Electoral Systems. All rights reserved.

Permission Statement: No part of this work may be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system without the written permission of IFES.

Requests for permission should include the following information:

- A description of the material for which permission to copy is desired.
- The purpose for which the copied material will be used and the manner in which it will be used.
- Your name, title, company or organization name, telephone number, fax number, e-mail address and mailing address.

Please send all requests for permission to:

International Foundation for Electoral Systems

2011 Crystal Drive, Floor 10 Arlington, VA 22202

Email: [media@ifes.org](mailto:media@ifes.org)

Phone: 202.350.6701

Fax: 202.350.6700



# About IFES

---

IFES advances democracy for a better future. We collaborate with civil society, public institutions and the private sector to build resilient democracies that deliver for everyone. As a global leader in the promotion and protection of democracy, our technical assistance and applied research develops trusted electoral bodies capable of conducting credible elections; effective and accountable governing institutions; civic and political processes in which all people can safely and equally participate; and innovative ways in which technology and data can positively serve elections and democracy. Since 1987, IFES has worked in more than 145 countries, from developing to mature democracies. IFES is a global, nonpartisan organization based in Arlington, Virginia, USA, and registered as a non-profit organization [501(c)(3)] under the United States tax code.

# Acknowledgements:

---

The authors would like to thank Cathy Buerger, Tonei Glavinic, Matt Emery, Rakesh Sharma, Regina Waugh, Meredith Applegate, Erica Shein, Vasu Mohan, Xeneb Shah, Federico Roitman, and Nicole Leaver for their invaluable contributions to the conceptualization, review and refinement of the Chain of Harm methodology and publications.

The authors would also like to thank Salam Al Waeli, Danielle Anthony, Devitree Haimnarine, Jeanne Mitchell, Rosemarie Ramitt, Ganesh Singh, IFES Iraq colleagues, as well as partners from the iSTAR network, Guyana Council of Organizations for Persons with Disabilities, and Youth Challenge Guyana for their expertise, dedication and ingenuity in the piloting and refinement of the Chain of Harm Co-design Workshop and their leadership of the subsequent programming implementations.

# Table of Contents

---

Overview .....	1
Using the Chain of Harm for Program Design .....	2
What is the Chain of Harm? .....	2
FIGURE 1: Endemic Narratives .....	2
FIGURE 2: Disinformation-Amplified Endemic Narratives .....	3
Identity and the Chain of Harm .....	4
Each Stage of the Chain of Harm as an Intervention Point .....	4
FIGURE 3: Programming to Strengthen the Media Mapped to the Chain of Harm ...	5
Using the Chain of Harm to Avoid Program Design Mistakes .....	5
The Chain of Harm Co-Design Workshop: A Replicable Process for Locally Led and Evidence-Based Program Design .....	7
Future Applications of the Chain of Harm .....	9
The Chain of Harm Evaluation Workshop: Culturally Responsive Evaluation .....	9
FIGURE 4: Program Outcomes Mapped to the Chain of Harm .....	10
The Chain of Harm Threat Modeling Workshop .....	11
FIGURE 5: Cybersecurity Attacks .....	12
FIGURE 6: Gender-Specific Cybersecurity Risks Mapped to the Chain of Harm .....	13
Conclusion .....	14

## Overview

Since IFES published [\*Disinformation Campaigns and Hate Speech: Exploring the Relationship and Programming Interventions\*](#) in 2019, challenges to public trust, public health and social cohesion presented by inaccurate, inciteful, and deliberately deceptive information have continued to demand innovative responses. The Chain of Harm, introduced in that 2019 publication, is a framework that breaks down the challenges of disinformation, misinformation, and dangerous speech (DMDS) into five interrelated stages (*actor, message, mode of dissemination, interpreter, and risk*). Each stage describes a discrete intervention point to disrupt the ultimate manifestation of harm. This five-stage approach supports the design of multi-layered programming that more effectively promotes healthy information environments around moments of critical social and civic importance, with particular emphasis on designing programming that is responsive to the different experiences of diverse populations.

The Chain of Harm has proven both useful and replicable for the broader community of development practitioners, particularly those who aim to create evidence-based and locally led programming. This publication provides guidance in three areas:

- **Using the Chain of Harm to design more nuanced information integrity programming**

This publication reintroduces the Chain of Harm, depicting the interplay of deliberate disinformation campaigns with endemic conspiracy, misinformation, and dangerous speech across the five stages. The updated framework provides a means for practitioners and researchers to identify multi-layered intervention strategies and focus scarce resources on the most impactful interventions.

- **Creating locally led, evidence-based programming through the Chain of Harm Co-design Workshop**

This publication outlines how the Chain of Harm can be used to create evidence-based, locally led information integrity programming that centers the perspectives of local communities, with a focus on traditionally marginalized or underrepresented populations. Companion Method Notes provide step-by-step implementation guidance for democracy and governance, humanitarian, or public health practitioners who wish to adapt and deploy the Chain of Harm Co-design Workshop for their own work.

- **Future applications: Culturally responsive evaluation and inclusive threat modeling**

The Chain of Harm is also valuable as a culturally responsive evaluation tool that helps ensure the inclusion of local voices and perspectives in evaluations of information integrity programs. Additionally, the Chain of Harm can be used as the foundation for a participatory threat modeling workshop that generates insights about the diverse experiences of underrepresented populations with respect to digital safety and cybersecurity risks. These insights can be used to design and implement more responsive interventions and risk mitigation strategies.

While the focus of this paper – and of IFES's work – is the democracy, rights, and governance sector, the Chain of Harm can also be useful for practitioners in confronting the challenges that misinformation, dangerous speech, conspiracy, and deliberate disinformation campaigns present for other sectors, such as public health, peacekeeping, or humanitarian aid.

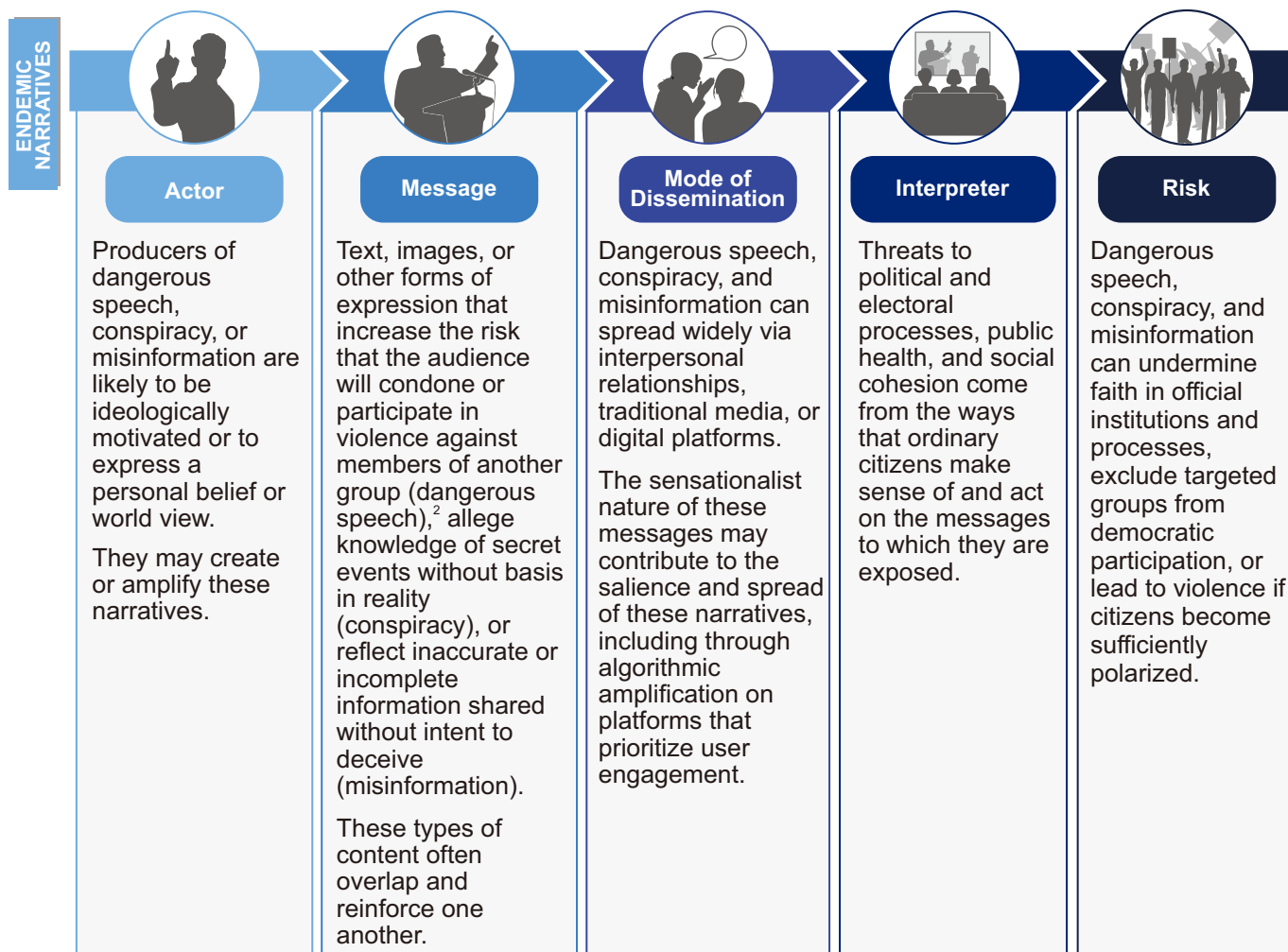
# Using the Chain of Harm for Program Design

## What is the Chain of Harm?

The Chain of Harm is an analytical tool that depicts the interplay between existing, endemic narratives – such as dangerous speech, conspiracy, or misinformation – and directed, intentional disinformation campaigns that seek to amplify and exploit these fissures to serve a goal. The Chain of Harm divides these challenges into component parts, each presenting a discrete intervention point for programming to target.

First, the Chain of Harm depicts how problematic endemic narratives – meaning false, misleading, or incendiary narratives that are inherently present in public discourse – manifest as harms, absent a directed disinformation campaign.<sup>1</sup>

**FIGURE 1: Endemic Narratives**



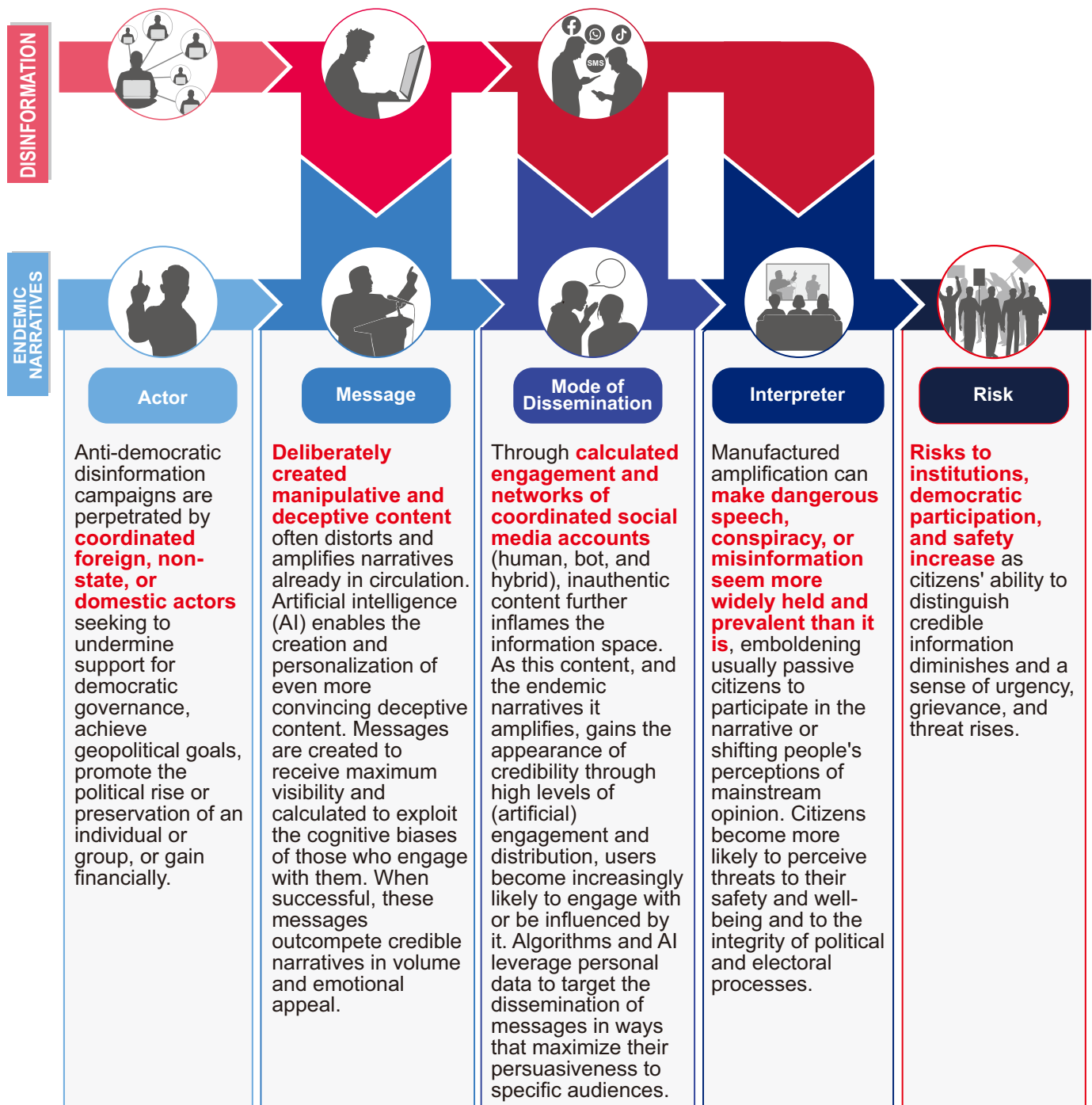
<sup>1</sup> The Chain of Harm adapts ideas from Wardle, C. (2017). "Information Disorder: Toward an interdisciplinary framework for research and policy making," which conceptualizes the *elements* of information disorder as agent, message, and interpreter and the *phases* as creation, production, and distribution.

<sup>2</sup> Dangerous Speech Project: [What is Dangerous Speech](#)



In a directed disinformation campaign, coordinated *actors* inject fabricated and manipulated content into the pool of dangerous speech, conspiracy, and misinformation already in circulation, altering the *actor*, *message*, and *mode of dissemination*. The effect of such a disinformation campaign is depicted as a second layer (in red in the graphic below). The text below the graphic describes how these disinformation efforts amplify the risk and magnitude of violence and democratic erosion.

**FIGURE 2: Disinformation-Amplified Endemic Narratives**



## Identity and the Chain of Harm

The Chain of Harm can illuminate the experiences of diverse populations with information integrity challenges – particularly those that are traditionally marginalized or under represented. In particular, the Chain of Harm depicts how disinformation campaigns amplify identity-based dangerous speech as a common tactic.

Marginalized communities experience DMDS on multiple fronts. Opportunistic actors evoke identity to stoke fear or resentment, heightening dangerous sentiments about marginalized groups that circulate among majority and minority populations. At the same time, marginalized groups are targeted with messages intended to suppress their political participation or heighten a sense of

insecurity, further excluding communities that already face barriers to civic and political engagement. These campaigns amplify existing, deep-seated sources of tension, discord, and hatred in ways that erode human rights, undermine public trust in democratic institutions, and increase the possibility of electoral violence and political instability.

Given the frequent reliance of disinformation campaigns on leveraging identity-based social divisions to serve their goals, the experiences of marginalized and underrepresented groups must be central to any programming approach that seeks to mitigate the erosion of information integrity.

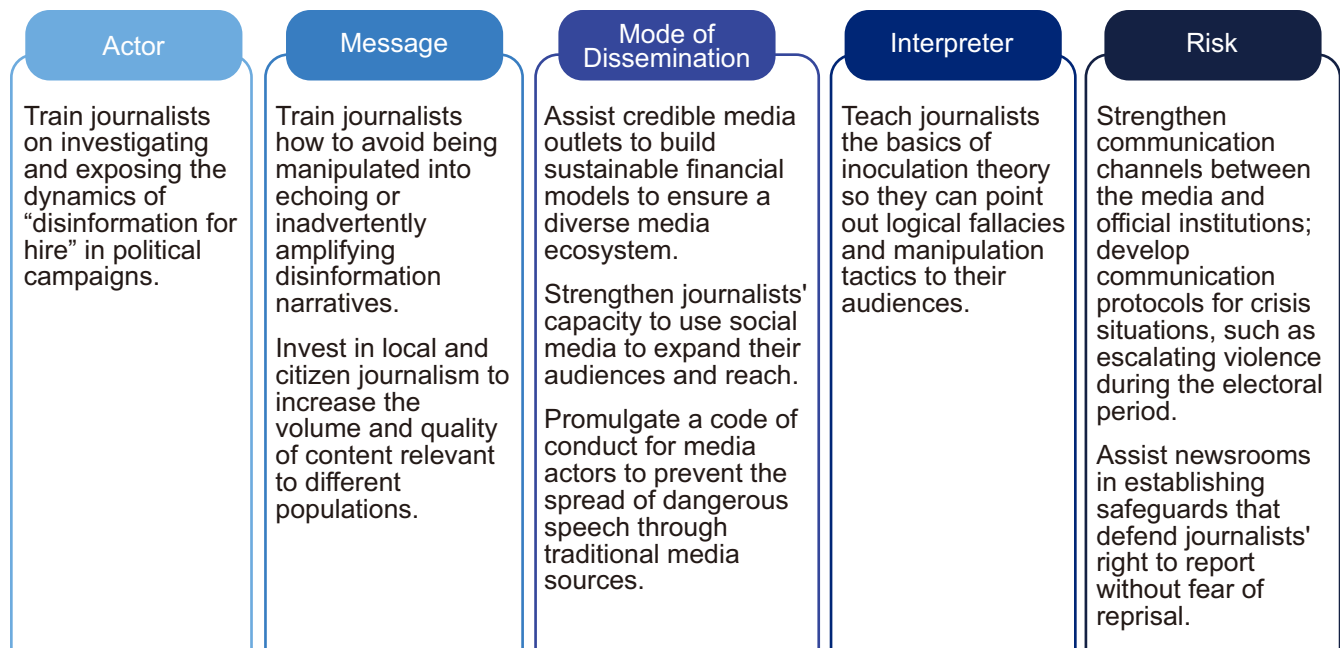
## Each Stage of the Chain of Harm as an Intervention Point

Using the Chain of Harm to visualize the relationship between endemic narratives and directed disinformation campaigns illuminates intervention points that information integrity programming can address. It can also be a useful brainstorming tool to expand on an initial program idea.

The ultimate goal of information integrity programming is to stop the creators of endemic and deliberately deceptive narratives (the actors) from causing violence or undermining faith and participation in democratic processes and institutions (the risk). To that end, effective interventions can disrupt the Chain of Harm at any point (actor, message, mode of dissemination, interpreter, or risk). For example, if programming could create extremely savvy interpreters who were impervious to disinformation and conspiracy, no other intervention along the chain would be needed. This is patently unrealistic, of course, so effective approaches need to disrupt at multiple intervention points. Crucially, the problem does not need to be neutralized equally at every phase along the chain to mitigate the ultimate risk. Thus, the Chain of Harm can help prioritize program decisions to focus on the most impactful and realistic intervention points.

The Chain of Harm can be applied to develop a multi-layered programming approach that supports a higher-level objective. For example, the chart below illustrates how information integrity programming to strengthening the media can be designed to address each stage of the Chain of Harm.

**FIGURE 3: Programming to Strengthen the Media Mapped to the Chain of Harm**



Considering how a program can make an impact at each of the five stages can challenge program designers to think more expansively about the approaches they wish to take. The Chain of Harm Co-design Workshop, discussed further below, provides a step-by-step process for using the Chain of Harm in this way to develop locally led, evidence-based programming.

## Using the Chain of Harm to Avoid Program Design Mistakes

Articulating how an intervention disrupts the Chain of Harm can help practitioners avoid common program design fallacies, including conceiving of information integrity programming too narrowly.

The Chain of Harm demonstrates that interventions that might not seem like counter-disinformation programming at first glance are essential ingredients to mitigate risk. For example, values-based voter education campaigns designed to compete with emotionally salient anti-democratic messaging (targeting the message) or civic engagement initiatives that prioritize building inter-communal bonds (targeting the interpreter) may not seem technologically forward enough to match preconceived ideas about what counter-disinformation programming should look like. Nonetheless, such campaigns are key to building resilience in the face of disinformation, conspiracy and dangerous speech.

Another common limitation of traditional program design that the Chain of Harm can help address is a tendency to design programs that describe the information environment but do not connect that knowledge to action and impact. For example, programming that creates technologically sophisticated methods to monitor the online information environment does not, on its own, interrupt the Chain of Harm. Without a clear end use, knowledge of the nature and origin of salient online narratives does not deter actors, alter the message landscape, interrupt the mode of dissemination, or reach interpreters in a way that influences belief or behavior – leaving the ultimate risk unchanged. If donors and implementers want an online monitoring approach to have impact, it must connect convincingly with, for example, a means to sanction or deter perpetrators, craft more effective counter-messages, or inform an impactful mode of dissemination for those counter-narratives. In terms of resource allocation, a program that invests most of its resources in detecting narratives and treats the application of that knowledge as a secondary purpose is less likely to be impactful.

# The Chain of Harm Co-Design Workshop: A Replicable Process for Locally Led and Evidence-Based Program Design

The Chain of Harm Co-design Workshop is a replicable process for locally led and evidence-based program design and implementation. The purpose of the workshop is to improve the responsiveness of information integrity interventions to the ways that misleading and deceptive information affects different communities. In particular, the workshop is designed to center the perspectives of traditionally marginalized and underrepresented communities.

The Co-design Workshop uses the Chain of Harm to provide a structure for understanding how DMDS affects different populations at each of the five stages of the chain, and how these insights can inform programming to strengthen the democratic information space and protect the rights of marginalized people.

The Chain of Harm can reveal meaningful insights that might otherwise be missed. For example, programming that addresses the differential impacts of DMDS often analyzes the messages that target marginalized groups. However, marginalized populations are also consumers (or *interpreters*) of these messages; the *modes of dissemination* by which messages reach different groups vary; and the specific risks and harms for various communities are different. In some instances, marginalized groups might also be the actors creating or spreading DMDS.

The Chain of Harm Co-design Workshop enables practitioners, donors, and academics to operationalize this thinking to base decisions about implementation on an understanding of how each of the five stages of the chain impact different communities. This includes people who identify with multiple social identities, such as women with disabilities or young people who are members of ethnic minorities.

The Co-design Workshop is a facilitated two-day event that brings together representatives of local partner organizations or institutions, local and international experts, and implementers. The workshop guides participants through a process that enables them to articulate or expand an information integrity programming approach to reach previously underserved or disserved populations.

Prior to the workshop, implementors and partners engage in an adaptable data gathering process to gain insights into how different populations receive and make sense of the information they consume. Local partners receive training and resources to conduct focus groups with representatives of different populations in the target country. If programmatic resources allow, implementers may choose to commission a national or regional survey or engage an organization or expert to conduct an analysis of the social media environment in the target country.


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

IFES developed, piloted, and refined the methodology behind the Chain of Harm Co-design Workshop in Iraq and Guyana in coordination with local partners, leaders of underrepresented communities, and inclusive program design experts.

to refine the programming approach. Focus group and survey data are shared with workshop participants, and the local partners that led the focus groups also lead the discussion. Participants are guided through exercises to identify actionable and interesting insights from the data, particularly those that reveal differences among different populations at each stage of the Chain of Harm. To close out the first day, facilitators then guide participants through a series of ideation activities to tap into the collective knowledge and creativity in the room to begin connecting insights from the evidence into intervention ideas that can fill programming gaps or strengthen current programming.

On the second day, workshop participants have opportunities to refine and advocate for the implementation of the ideas they believe are most valuable before the group votes on the ideas they would like to implement in practice. They vote based on different criteria – including which interventions are most likely to reach currently underserved populations, which activities fill a clear gap in programming, and which ideas excite them the most. After the group selects and sorts final ideas based on available resources and feasibility, participants discuss the top ideas and elaborate them in workplans, including associated monitoring and evaluation considerations.

The workshops should be conducted with the intent and resources to fund and support the ideas that come out of it, with local participants leading the implementation of the ideas they co-created and ongoing support from an implementing partner.



To learn how to use the Chain of Harm Co-design Workshop in your own work, IFES compiled a [comprehensive user guide for organizing and facilitating your own workshop](#).

For example, local partners in Iraq identified a need to increase understanding among women, religious minorities, and people with disabilities of how to protect themselves from being manipulated online. To respond to this need, the partners designed and delivered skill-building workshops with civically engaged individuals representing the groups – creating informed messengers who could share what they learned with their communities, families, and classrooms. In Guyana, IFES youth partners who volunteered at voter education booths in public markets described the difficulty of knowing what to do or say when they were approached by confrontational individuals echoing conspiracy narratives about the elections. This led to a conflict mitigation and communication workshop for youth volunteers that included role-playing on building connections and de-escalating potential conflict. These ideas, and other initiatives that were implemented based on the Co-design Workshop, came out of the ideation sessions. Local partners advocated for them based on their knowledge and experience as well as the survey and focus group data. In both countries, local partners demonstrated creative problem-solving and ownership throughout the implementation of their programming.

# Future Applications of the Chain of Harm

## The Chain of Harm Evaluation Workshop: Culturally Responsive Evaluation

In addition to its value as a program design tool, the Chain of Harm is useful for program evaluation. 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.

CRE assesses programs, interventions, or initiatives by considering the cultural contexts, values, and perspectives of the individuals or communities involved, recognizing that “demographic, sociopolitical, and contextual dimensions, locations, perspectives, and characteristics of culture matter fundamentally in evaluation.”<sup>3</sup> CRE emphasizes the impacts of programming on traditionally marginalized groups; acknowledges the power dynamics; and incorporates all stakeholder voices into the evaluation process to ensure relevance, fairness, and effectiveness.

Traditional program evaluations are typically performed from a donor's perspective, parsing the outcomes and impact that will be most meaningful to their future efforts. However, members of local communities where programming takes place often do not hold the same views as the donor community and therefore do not place the same value on the same outcomes. Additionally, target communities often are not recipients of final evaluation language; nor is this language generally accessible to them. The Chain of Harm Evaluation Workshop remedies the disconnect between implementer, donor, and local partners by centering the evaluative process in the experiences of community members. Doing so increases the likelihood that the data collected and the outcomes identified represent local priorities and, ideally, are used to inform future programming decisions to align with those priorities.

The Chain of Harm Evaluation Workshop follows an evidence-based, participatory format similar to that of the Co-design Workshop. In the case of the Evaluation Workshop, the data sources that are shared and discussed comprise assessment data collected throughout the program – for example, surveys, pre- and post-test results, participant focus groups, and other indicators. The Evaluation Workshop gathers local program implementers, program beneficiaries, evaluators, and donors to identify outcomes from the evaluation data that are most meaningful to them. Participants map these outcomes onto the Chain of Harm to derive a holistic perspective on where the program had impact. Facilitators then guide participants to consider each stage of the Chain of Harm with the goal of illuminating any unintended or subsidiary outcomes. Finally, participants work together to vote on and rank the importance of each outcome, with consideration for how those outcomes might differ for marginalized populations. Participants leave the workshop with a clear understanding of the most impactful outcomes of their work, where future opportunities for programming exist, and a plan for communicating these insights to other community members.

---

<sup>3</sup> Hopson, R. K. (2009). “Reclaiming Knowledge at the Margins: Culturally Responsive Evaluation in the Current Evaluation Moment.” Pages 429–446 in Ryan, K., and Cousins, J.B. (eds.). *The SAGE International Handbook of Educational Evaluation*.

Below is an example of how hypothetical outcomes from a school-based counter-speech and media literacy program could be mapped to the Chain of Harm. The illustrative outcomes are intended to demonstrate how the process can reveal insights into the experiences of different populations with the programming, or subsidiary outcomes that might otherwise be missed.

**FIGURE 4: Program Outcomes Mapped to the Chain of Harm**

Actor	Message	Mode of Dissemination	Interpreter	Risk
<p>15 percent of students report deciding not to share or post at least one misleading or inciteful post online as a result of the training.</p> <p>Several participants who are girls report being bullied less by classmates on social media in the past 30 days.</p>	<p>Teachers who attended the evaluation workshop report that interactions in their classrooms have been more respectful and supportive.</p> <p>10 percent of students and 20 percent of teachers who participated in the program say they are more likely to re-share civic content that they see in their social feeds.</p>	<p>Several students report sharing what they learned with family members with low literacy.</p> <p>Teachers incorporated core media literacy points into lesson plans in other classes that they taught.</p> <p>20 percent of students report that they stopped following or engaging with a creator or influencer who posted conspiracy or sensationalist content.</p>	<p>In a post-test, 70 percent of students reported increased confidence that they can identify misleading content.</p> <p>Two participants in the program were inspired to start a civic initiative.</p>	<p>10 percent of respondents report increased willingness to report bullying or threats of violence that they see on social media to a teacher.</p>
Gaps Left Unaddressed				
<p>Participants from a religious minority group report no decrease in the online bullying they face from classmates.</p>	<p>Students expressed interest in how to create more effective counter-messages, suggesting future programming opportunities.</p>	<p>The training was offered at a time that prevented student athletes from participating.</p>	<p>Students with disabilities reported a lower increase in confidence, suggesting the programming could be more accessible to this audience.</p>	<p>Participants' interest in engaging in civic or electoral processes remains unchanged, suggesting an opportunity to include additional civic education content in future programs.</p>



The Chain of Harm Evaluation Workshop mitigates several issues with traditional ways to evaluate information integrity programming beyond the stakeholder disconnect identified above. The workshop provides an opportunity for evaluators to obtain multiple participant perspectives at once, reducing the need for extensive individual post-program interviewing, coding, and analysis. Additionally, the process of mapping data and outcomes along the Chain of Harm makes it easier to see whether outcomes match the original need that the program tried to address or whether unexpected outcomes occurred. It also enables evaluators to see whether data is insufficient to substantiate or prove impact, revealing areas where more follow-on data collection is necessary.

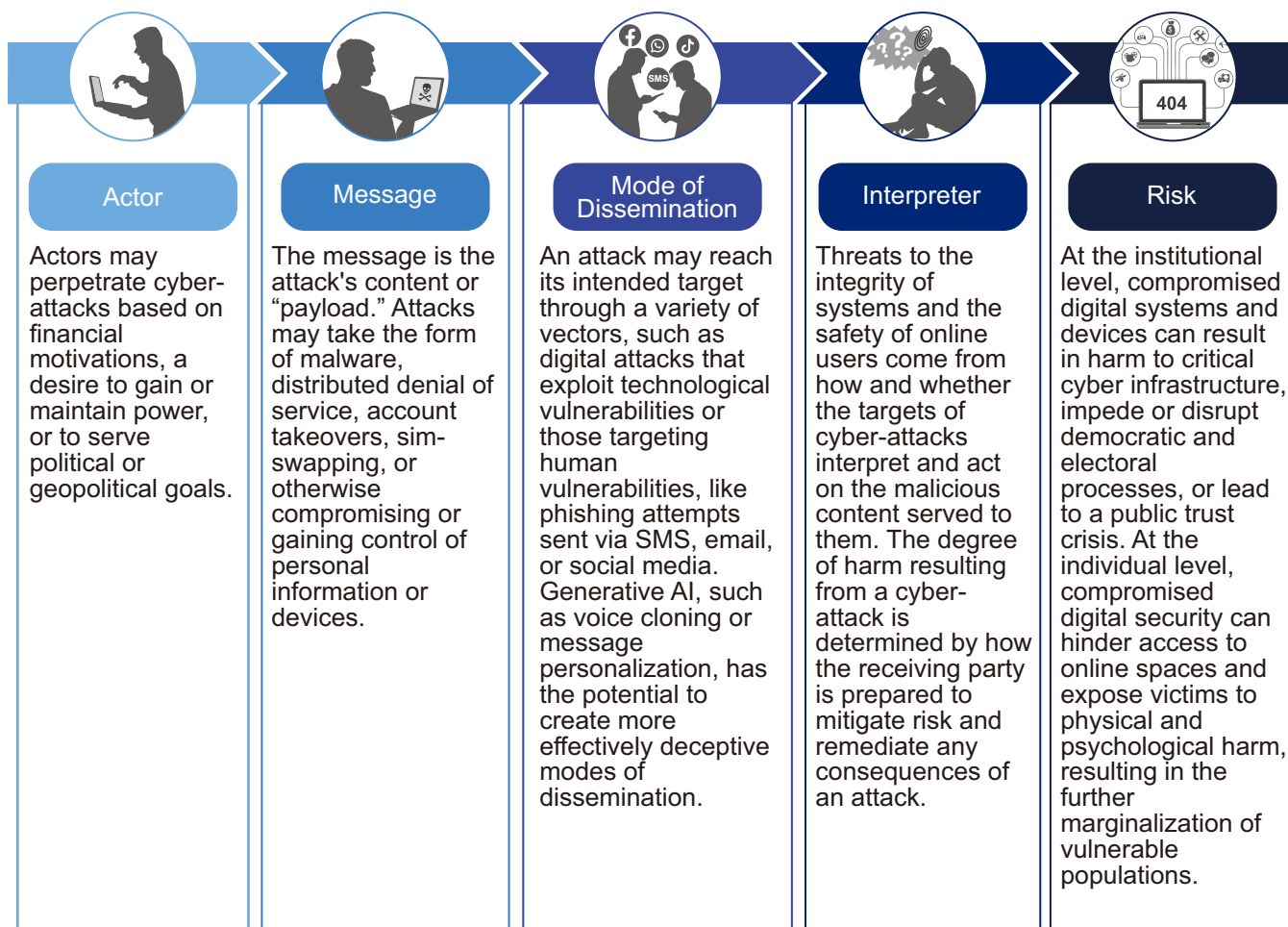
At the end of the Program Evaluation Workshop, evaluators, programmatic implementers, and local community members will have a stronger shared understanding of the impact of the information integrity programming on the information environment. This mutual understanding may lead to an improved, ongoing working relationship to address these issues.

## **The Chain of Harm Threat Modeling Workshop**

With slight adaptation, 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. By mapping cyber-attacks across the Chain of Harm, multiple points of intervention that address various dimensions of digital, physical and psychological safety can be identified.

The figure below illustrates how the five stages of the Chain of Harm can be applied to understand how cybersecurity attacks lead to harm.

**FIGURE 5: Cybersecurity Attacks**



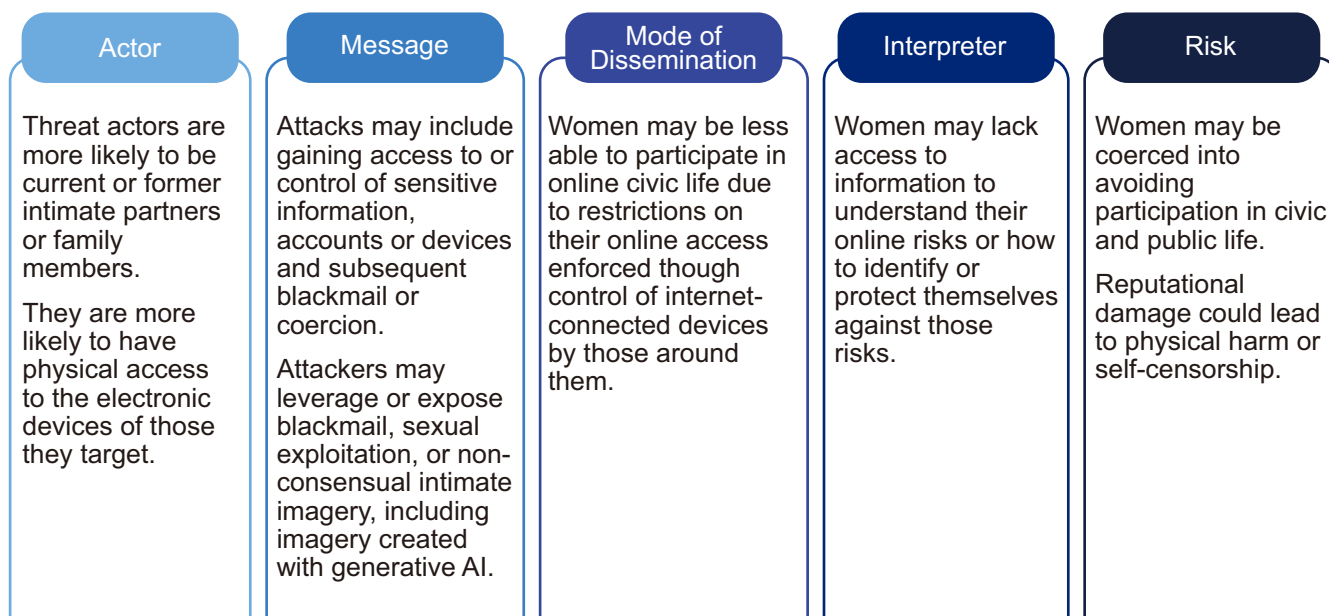
In the context of cybersecurity, threat modeling is a proactive and iterative strategy to identify, understand, and inform the management of risks. When used correctly, it can enable product designers, cybersecurity practitioners, and technology users to anticipate and plan for issues that may compromise the confidentiality, integrity, and availability of electronic systems and devices. In plain language, threat modeling provides a process to understand what is at risk, what can go wrong, and how those anticipated risks can be prevented when it comes to the security of technological systems.

The answers to these questions can vary for different audiences, and cybersecurity professionals and existing threat modeling procedures are not well equipped to understand the different experiences of underrepresented populations. Cybersecurity threat modeling, as normally practiced, does not adequately address social, psychological, and physical harms to traditionally marginalized populations, such as women, older persons, and people with disabilities. Cybersecurity practitioners are overwhelmingly men from majority groups with specialized technical knowledge. This leaves most of the global population underserved by current digital safety and cybersecurity practices that are seen and informed through an overly narrow lens and without the intentional incorporation of inclusive perspectives.

For example, exploring the digital safety and cybersecurity risks of women who engage in civic activities or public figures using the Chain of Harm might reveal gender-specific insights that in turn might suggest a different set of solutions or risk mitigation.

The chart below provides samples of the types of insights that might be revealed in this way.

**FIGURE 6: Gender-Specific Cybersecurity Risks Mapped to the Chain of Harm**



A participatory Chain of Harm Threat Modeling Workshop adapts the format of the Chain of Harm Co-design Workshop. The Threat Modeling Workshop shares a similar goal of centering the perspectives of traditionally marginalized and underrepresented populations to identify unexplored and responsive interventions. A multi-day Chain of Harm Threat Modeling Workshop brings together technical experts, international practitioners, and local partners, with an emphasis on participants who are representatives of marginalized and underrepresented populations.

The workshop captures the sources, threats, and harms that underserved populations experience as they engage online. Using a participatory process similar to that of the Co-design Workshop, participants draw on quantitative and qualitative data to map threats to cybersecurity along the Chain of Harm, with an emphasis on distinguishing how threats may differ for different populations at each stage of the Chain. Workshop participants then brainstorm potential counter-measures and cybersecurity tools that can be deployed at each stage of the Chain of Harm to neutralize the identified threats. At each step, facilitators center the question of how counter-measures can be more responsive, or how to focus resources more effectively, on the most significant vulnerabilities and most impactful intervention points.

The workshop culminates with the selection of the most impactful and viable programming interventions through group consensus, along with the development of preliminary implementation plans. Participants are then supported to further refine and implement these programming ideas. 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. In the example above, civically engaged women represent a population that may have unique cybersecurity concerns. The manner in which threat actors attack women through digital vectors can be documented and classified in much the same way that cybersecurity professionals can attribute cyber-attacks emanating from specific entities based on the combination of tools and techniques that the attackers employ.

## Conclusion

The bedrock of the Chain of Harm framework is the idea that access to accurate information is fundamental to democratic participation. Given the sharp increase in political polarization and democratic backsliding, there is a demonstrable need to strengthen coordination within and across communities that are responding to – and on the receiving end of – disinformation, misinformation, and dangerous speech.

The Chain of Harm is an intuitive and useful tool for practitioners that want to design and implement more inclusive, nuanced, and evidence-based programming. As the democracy, rights, and governance community (and other sectors) grapple with the reality that the challenges contributing to the erosion of trust and pollution of information environments are complex and multi-faceted, we must look outside the established programming playbook to support the development of healthy democratic societies.



HQ | 2011 Crystal Drive | Arlington, VA 22202 | USA

[www.IFES.org](http://www.IFES.org)