To: Suzanne Spaulding[g@csis.org]
Cc: Suzanne Spaulding[@gmail.com]; Vijaya Gadde]; Vijaya Gadde| ;
Tate-Nadeau, Alicia[@illinois.gov]
From: Kate Starbird
Sent: Tue 5/17/2022 4:55:50 PM
Subject: Re: Question about MD vs. MDM
Received: Tue 5/17/2022 4:55:50 PM

I like how you've navigated with the language you added… which acknowledges MDM is part of the broader, but that we're focused on false/misleading content here and may need to address mal-information separately. Do we want to say that explicitly? Or just leave it as it stands, more subtly?

Kate

On May 17, 2022, at 9:50 AM, Suzanne Spaulding < @csis.org> wrote:

I vote for the latter. That said, I still think we may not be ready to make recommendations in this interim report that specifically address the challenge of malinformation. We can just say that, maybe?

From: Kate Starbird <@uw.edu>
Sent: Tuesday, May 17, 2022 12:48 PM
To: Suzanne Spaulding <@gmail.com>
Cc: Suzanne Spaulding < @csis.org>; Vijaya Gadde < >; Vijaya Gadde < @twitter.com>; Tate-Nadeau, Alicia < @illinois.gov>
Subject: Re: Question about MD vs. MDM

Hi Suzanne,

I agree that malinformation is perhaps the hardest challenge in this space — and one of the most effective tactics. Hacked/stolen/deceptively obtained materials that are strategically leaked into the public sphere are technically malinformation — but unfortunately current public discourse (in part a result of information operations) seems to accept malinformation as "speech" and within democratic norms. By invoking malinformation, we may open up a potential vector of bad faith criticism to undermine the work. By not invoking it, we leave out a critical dimension of information operations.

So, do we bend into a pretzel to counter bad faith efforts to undermine CISA's mission? Or do we put down roots and own the ground that says this tactic is part of the suite of techniques used to undermine democracy?

Kate

On May 16, 2022, at 6:02 PM, Suzanne Spaulding < @gmail.com> wrote:

Kate,
thanks for continuing to think about this issue. As I've read more about malinformation, I think you're right that it could fit the kinds of risks we are concerned about. The challenge may be that because it is not false, per se (though presented in a misleading, manipulative way to cause harm), it is much trickier from a policy perspective. I

think we could compromise by noting that it is part of CISA's current scope but that our recommendations, at least at this stage, are focused primarily on countering false information. Would that work? I'll try suggesting line-in line-out changes to the text.
best,
Suzanne

On Fri, May 13, 2022 at 6:00 PM Kate Starbird < @uw.edu> wrote:

Hi folks,

I want to follow up on Suzanne's comments on the recommendations report regarding focusing on "mis- and disinformation" vs. the "MDM" framework that Geoff and others have invoked in our conversations. Suzanne seems to be suggesting that we remove the malinformation, as it doesn't appear in our subcommittee name. And as I was working to do that in the document, I started waffling a bit.

Mis- and disinformation do seem more defensible — and less likely to run into some of the potential complaints that may see malinformation around elections as part of typical politics.

BUT, it seems like CISA and the government more broadly do use "MDM" as their acronym in this space, which means reducing it to MD may send a stronger message than we mean to send in the reduction of terms. Also, my sense is that malinformation provides an umbrella for some of the targeted harassment (in addition to hacking/leaking) that I think we do want to include in our recommendations.

Any thoughts on whether we should go with "mis- and disinformation" or "MDM" across the document? Or maybe use MDM but only define and stress the definitions for mis- and disinformation. ??

Kate