Analysis of the "National Day of Hate" and the Dangers of Amplifying Low-Signal Extremist Content

PRESENTED BY

NCRI
NETWORK CONTAGION
RESEARCH INSTITUTE

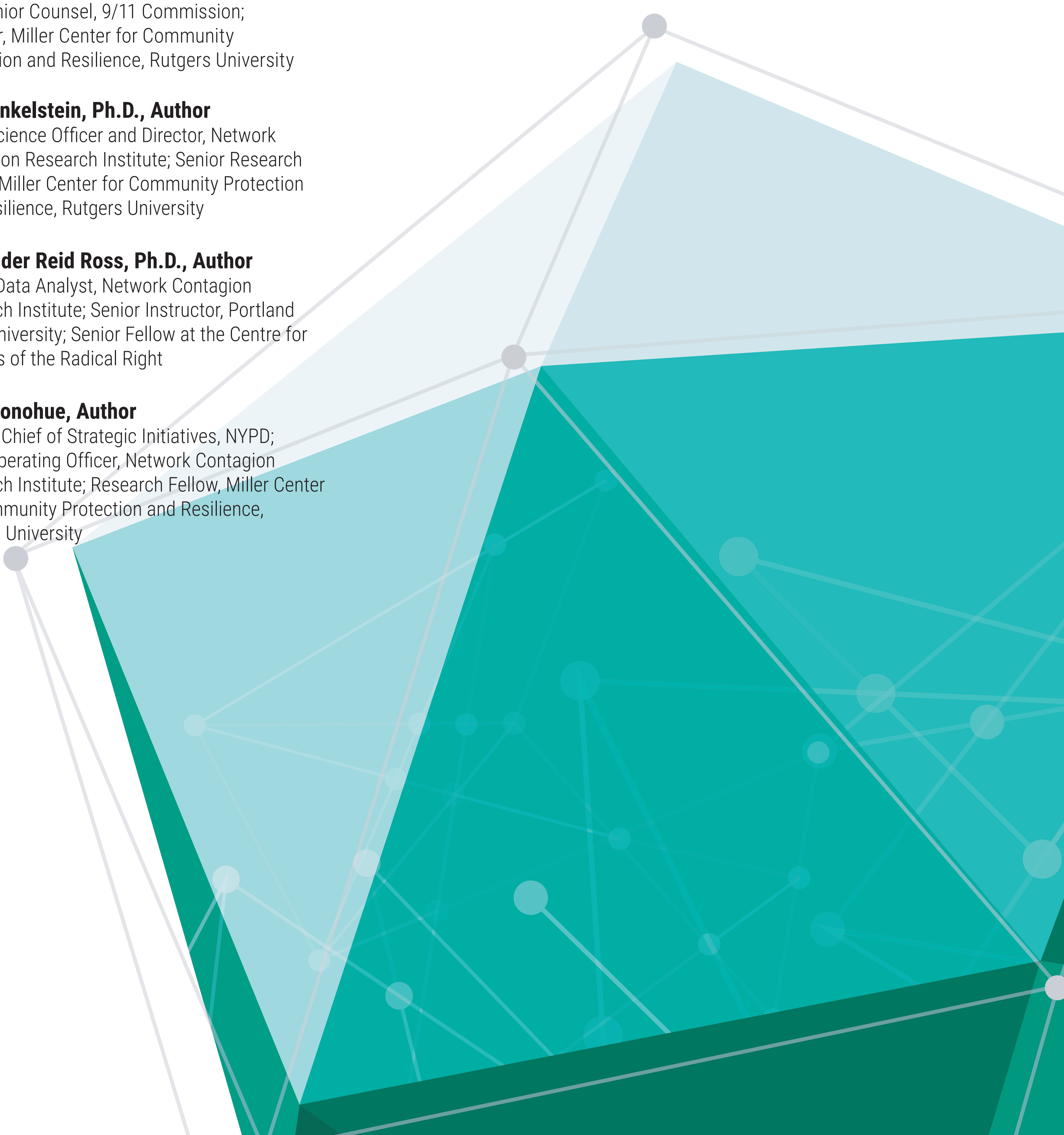
Alex Goldenberg, Author
Lead Intelligence Analyst, Network Contagion Research Institute; Research Fellow, Miller Center for Community Protection and Resilience, Rutgers University

John Farmer, Author
Former New Jersey State Attorney General and Senior Counsel, 9/11 Commission; Director, Miller Center for Community Protection and Resilience, Rutgers University

Joel Finkelstein, Ph.D., Author
Chief Science Officer and Director, Network Contagion Research Institute; Senior Research Fellow, Miller Center for Community Protection and Resilience, Rutgers University

Alexander Reid Ross, Ph.D., Author
Senior Data Analyst, Network Contagion Research Institute; Senior Instructor, Portland State University; Senior Fellow at the Centre for Analysis of the Radical Right

Jack Donohue, Author
Former Chief of Strategic Initiatives, NYPD; Chief Operating Officer, Network Contagion Research Institute; Research Fellow, Miller Center for Community Protection and Resilience, Rutgers University



2/28/2023

NCRI
NETWORK CONTAGION
RESEARCH INSTITUTE

Analysis of the “National Day of Hate" and the Dangers of Amplifying Low-Signal Extremist Content.

Bottom Line Up Front:

- The recent “National Day of Hate” event planned by an obscure Iowa-based white nationalist group received little attention (roughly 20 likes) within its own subcultural ecosystem on Telegram, yet received widespread amplification from mainstream media and organizations such as the ADL. There is little publicly available evidence to suggest larger white nationalist groups engaged with posts associated with the planned event or were planning to participate.
- The event did not lead to any high-profile antisemitic incidents, but “Day of Hate” was one of the top trending topics on social media causing fear within the Jewish community and heightened security posture across the country.
- Sounding an undue alarm about low-signal extremist content can potentially elevate security risks and embolden bad actors, as they see the attention generated by their actions as a sign of success and validation, and may be motivated to carry out further extremist activities.
- When amplifying low-signal extremist content, it remains crucial to consider the volume and credibility of threats, as well as the risk of further increasing the threat level through amplification by way of public alert.

Overview:

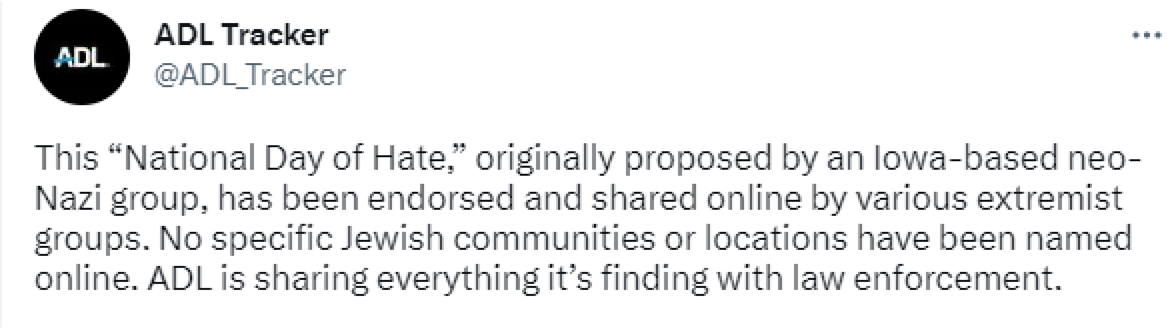
Last weekend, the U.S. Jewish community was placed on high alert in anticipation of a “National Day of Hate,” planned for February 25. An obscure Iowa based white nationalist group first announced the event on a Telegram chat channel in January, vowing to “shock the masses with banner drops, stickers, fliers, and graffiti.” Last year, the group gained the attention of local news agencies when it claimed responsibility for posting two antisemitic flyers in a park in northeast Iowa. Its two “National Day of Hate" posts garnered low engagement, receiving roughly 20 likes on their first post in January and 11 likes on a subsequent post referencing the event as of February 25. Their online flyers contained links to the group's Telegram channel, which initially maintained 7 subscribers and has since grown into the hundreds, remaining small relative to similar RWE Telegram groups.

Analysis:

Notwithstanding the low engagement, warnings of the “National Day of Hate” made national headlines, became one of the top trending topics on social media in the United States, frightened the Jewish community, and led to a heightened security posture across the country.

In this particular case, NCRI analysis suggests that the ‘National Day of Hate’ post on Telegram accumulated little attention in its own subcultural ecosystem and was not widely shared between extremist groups or on extremist forums until it received mainstream attention. Some reports suggested that more active white nationalist groups such as National Socialist Movement (NSM) and the Goyim Defense League (GDL) planned to take part in the event, which would elevate the threat level. However, the NCRI saw little evidence to suggest the involvement of NSM, GDL, or any other large white nationalist network. Our view is shared by other researchers on extremism.

The NCRI analyzed social media comments to assess the scale of chatter around the “National Day of Hate” online and to illuminate how the event garnered mainstream attention. Our analysis indicates that “National Day of Hate” was first referenced on Twitter by the ADL on February 9 and then cited in various law enforcement briefings that garnered media attention on February 21, which referenced the Telegram post and advised situational awareness ahead of the weekend.



ADL Tracker
@ADL_Tracker

This “National Day of Hate,” originally proposed by an Iowa-based neo-Nazi group, has been endorsed and shared online by various extremist groups. No specific Jewish communities or locations have been named online. ADL is sharing everything it’s finding with law enforcement.

First reference of “National Day of Hate” on Twitter on February 9th

On February 23, the ADL referenced the event again, telling followers that a “nationwide extremist “Day of Hate” campaign planned for this Saturday is meant to be intimidating and divide us,” and that the “Jewish community may be the target of vile antisemitic hate,” suggesting extremist activity was imminent. The ADL encouraged followers to amplify a counter messaging hashtag to the “National Day of Hate,” which became a top trending topic in the United States, mentioned over 100k times during the weekend. An email was also sent out to the ADL's mailing list with the subject line reading "TAKE ACTION against a "National Day of Hate."

On Friday, February 24, high-profile lawmakers referenced the "National Day of Hate" in solidarity with the Jewish community. The small Iowa-based extremist group on Telegram enthusiastically highlighted high-profile references and the trending hashtag on the United States Twitter-trends leaderboard, claiming their event was already a success before it started. According to Cassie Miller, Senior Researcher at the Southern Poverty Law Center, "the panic made these groups look terrifying and well organized—something they desperately want, even though it doesn't reflect reality."

A time series analysis of tweets on both Twitter (blue) and 4chan (black) [Figure 1], one of the most prominent extremist subcultural forums, confirms that mainstream amplification of the event began on Twitter, and was followed later by chatter on 4chan. These efforts would see "Day of Hate" among the top trending terms on Twitter, mentioned in over 104,000 Tweets including retweets over the weekend and garnering tens of millions of impressions. Accounts on 4chan repeatedly made mention of the ADL as the key alert-source for the day itself, often referencing the event as a "Jewish false flag." Several accounts suggested learning and next steps from the "Day of Hate."

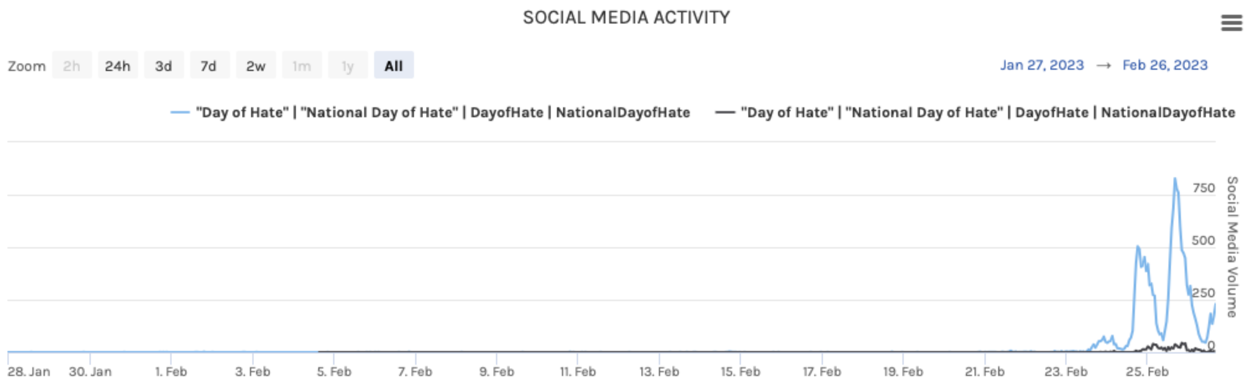


Figure 1.

Despite widespread fear, the "National Day of Hate'' passed without any high profile antisemitic incidents. However, on February 26, the small Iowa-based RWE group called the event a complete success and a learning experience on how to exploit the media to promote their hateful ideology. In their view, they set out to "shock the masses," and amplification helped them succeed.

Conclusion

Low-signal extremist content of this nature is commonplace on Telegram and other extremist subcultural forums. Therefore, alerting the public of such content, even with the intention of warning, always carries trade-offs and risks:

- To sound an undue or outsized alarm amplifies extremist causes with unnecessary attention, potentially elevating risks of acceleration.

- Disproportionate outcry about imminent threats absent substantive evidence of reach and extent can also lead to the spread of distrust and conspiracy theories—as in this case, claims among white supremacists of a “Jewish false flag” proliferated on 4chan’s /pol/ board, allowing them to put forward their general narrative of purported innocence.

- Sounding the alarm about an inflated threat that does not come to pass can give way to the specious evaluation that one has “prevented” the incident, cutting off critical thinking and increasing the “echo-chamber” effect.

Best practices in data-informed decision making regarding the collection of open source intelligence involve cautiously weighing the existing volume and credibility of threats with the risk of accelerating the threatening activity through amplification by way of public alert. That does not mean downplaying risks when they appear but remaining prudent as to how, when, and where alerts are used.