



Exploiting Tragedy:

The Rise of Computer-Generative Enabled Hoaxes and Malicious Information in the Wake of Mass Shootings

Recent hoaxes surrounding mass shootings suggest that easily accessible online tools can be leveraged for malicious purposes, deepening the crisis of polarization in US society, increasing the risk of violence, and impacting public safety operations. Technology is evolving rapidly, including AI chatbots and image generation tools that may create future hoax manifestos and computer-generated calls that falsely report mass shootings in progress, thereby spreading terror and confusion. As technology continues to advance, bad actors are likely to discover new ways to harness these developments to commit malicious actions more efficiently.

Nashville Manifesto Hoax:

On March 27, 2023, a former student entered The Covenant School, a kindergarten through sixth grade religious school, in the Green Hills neighborhood of Nashville, and opened fire with AR-type weapons, killing six (three nine year olds and three adults) before being killed by law enforcement. Aside from the brutality of the act against children, teachers, and staff in a grade school, the act shocked the public for its departure from the usual formula of a white, young male, issuing instead from a young trans male. The unexpected nature of the shooter's identity, coupled with the discovery that Audrey Hale, who used male pronouns on social media, had left a manifesto in their home before initiating the attack, fueled a prolonged period of speculation and excitement on the part of conspiracy theorists on internet message boards like 4chan's /pol/ board.

A post featuring a purported manifesto initially emerged on 4chan on a thread that went viral hours after the incident, showcasing a manifesto. At first glance the document appeared to be handwritten, but closer inspection revealed it to be computer generated, using a font designed to simulate female handwriting. The NCRI identified several posts of this fake manifesto on other online platforms, including kiwifarms, a notorious platform known for targeted harassment campaigns, and Twitter. The fabricated manifesto soon began circulating on Twitter, making its way to prominent right-wing Twitter accounts like that of Ian Miles Cheong, who maintains over 500k followers, and accumulating hundreds of thousands of views.



The fake manifesto, which the NCRI is intentionally not amplifying in this report (but will share with researchers upon request) capitalized on public concerns surrounding trans people and attempted to associate the term "ACAB" (All Cops Are Bastards) with the shooter's actions. Overall, the hoax document aims to depict the Covenant School shooter as sharing the same opinions as many trans people with the aim of further marginalizing and alienating the community.

This incident serves as a case study on how mass shootings can be exploited by bad actors to inflame social conflicts. Hoaxes¹ and conspiracies² almost always arise following high-profile mass casualty attacks³; however, the potential to enable and amplify malicious content following an attack will continue to be exacerbated by computer generative technology and AI. While a quick and close examination could conclude that this particular manifesto was inauthentic, rapidly evolving AI tools can generate text that is virtually indistinguishable from authentic handwriting. Furthermore advanced image generation tools akin to Midjourney are becoming increasingly sophisticated and can, in theory, rapidly generate realistic images of handwritten notes in different environments. In all likelihood, bad actors will leverage these easily accessible tools to create believable documents, images, and messages following mass shootings, or other high profile incidents, in an effort to implicate innocent individuals or groups to intentionally provoke animosity and incite further violence.

Pittsburgh Computer-Generated Hoax:

Days after the attack at a Christian day school in Nashville, several schools in Pittsburgh, including Central Catholic and Oakland Catholic were targeted by what authorities described as "computer-generated swatting calls." The calls falsely claimed that there was an active shooter

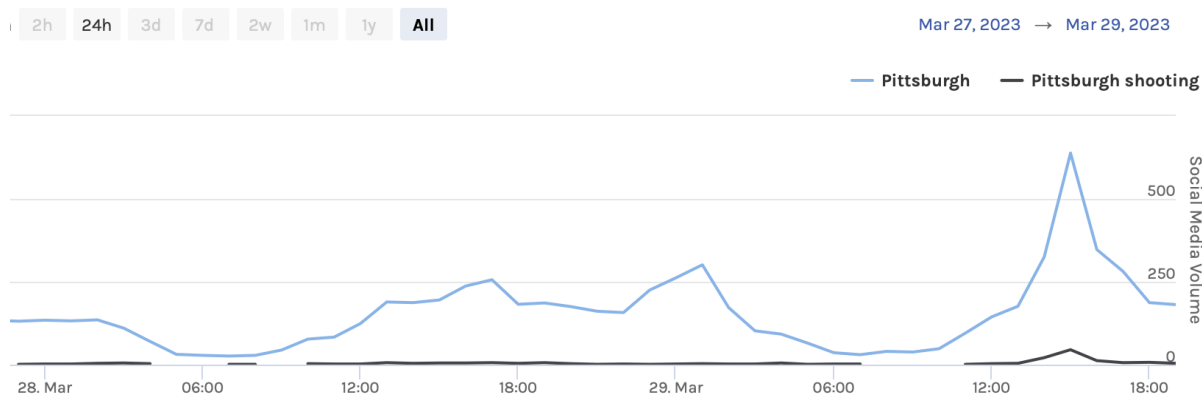
¹https://www.washingtonpost.com/business/economy/we-studied-thousands-of-anonymous-posts-about-the-parkland-attack---and-found-a-conspiracy-in-the-making/2018/02/27/04a856be-1b20-11e8-b2d9-08e748f892c0_story.html

² https://en.wikipedia.org/wiki/Sandy_Hook_Elementary_School_shooting_conspiracy_theories

³ <https://www.cfr.org/blog/seven-resources-debunking-911-conspiracy-theories>

incident with multiple injuries, prompting a quick response from law enforcement who promptly cleared all schools involved. Evidently, parents rushed to the schools to ensure their children were safe.

Moments after reports of a potential active shooter, Twitter seized on the alert, reporting that police were being dispatched to the schools for a critical incident. Many of these posts accrued hundreds of thousands of views, and were posted predominantly by concerned netizens in the area.



Time-series analysis on Twitter for "Pittsburgh" and "Pittsburgh shooting" shows a sharp spike in mentions in tandem with local reporting on a 'critical incident' at multiple schools in Pittsburgh.



While the specific technology used by the suspect remains unknown, human voice generators are becoming increasingly sophisticated due to rapid advancements in AI and machine learning. Years ago, it was quite obvious when someone was using a voice generator. However, cheap systems accessible to all can convert text into spoken language that can replicate tone, pitch, and inflection. The ease with which bad actors can create convincing audio content is concerning, and NCRI assesses this tactic to be leveraged frequently in the future.

Conclusion:

The Nashville and Pittsburgh incidents underline the importance of addressing the dangers posed by bad actors leveraging rapidly evolving computer-generative technologies to amplify hoaxes and disinformation following mass shootings. As AI and other advanced technologies

become increasingly accessible, the potential misuse grows, posing a significant threat to law enforcement, the media, and society at large. Furthermore, the psychology of these hoaxes on affected communities cannot be underestimated. It is crucial for stakeholders to keep a close eye on the evolution of computer/AI generative technology, anticipate how bad actors will exploit them, develop processes to identify computer/AI generated content, ensure digital provenance of tips and evidence and develop best practices for immediate response to viral hoaxes.



For more information contact: director@ncri.io