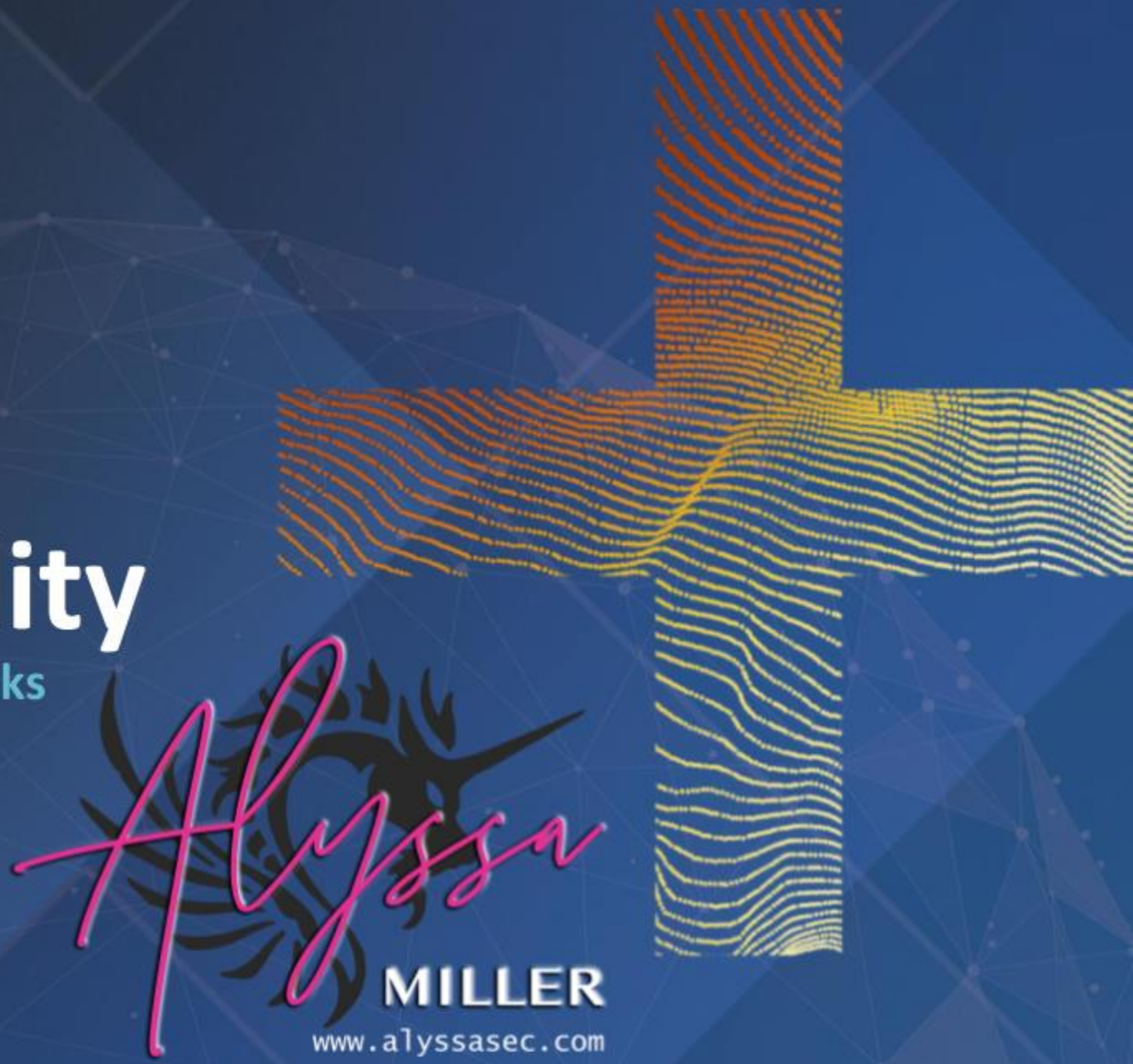
GSX+
GLOBAL SECURITY EXCHANGE PLUS

21–25 SEPTEMBER 2020
GSX.ORG | #GSXPLUS

Losing our Reality

Deepfakes Changing the Face of Attacks



Alyssa MILLER
www.alyssasec.com

Hacker/Researcher

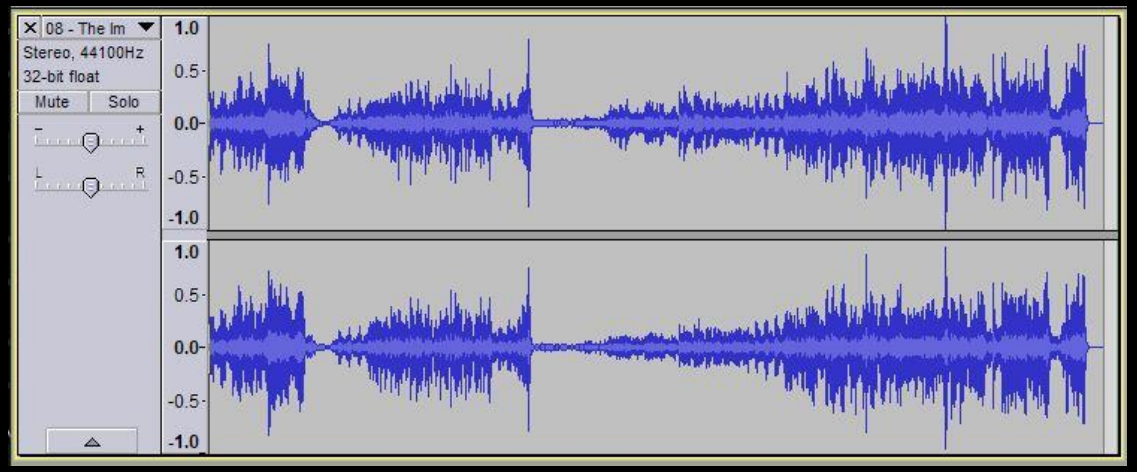
Security Advocate

Author & Blogger

Co-Host: Uncommon Journey

snyk

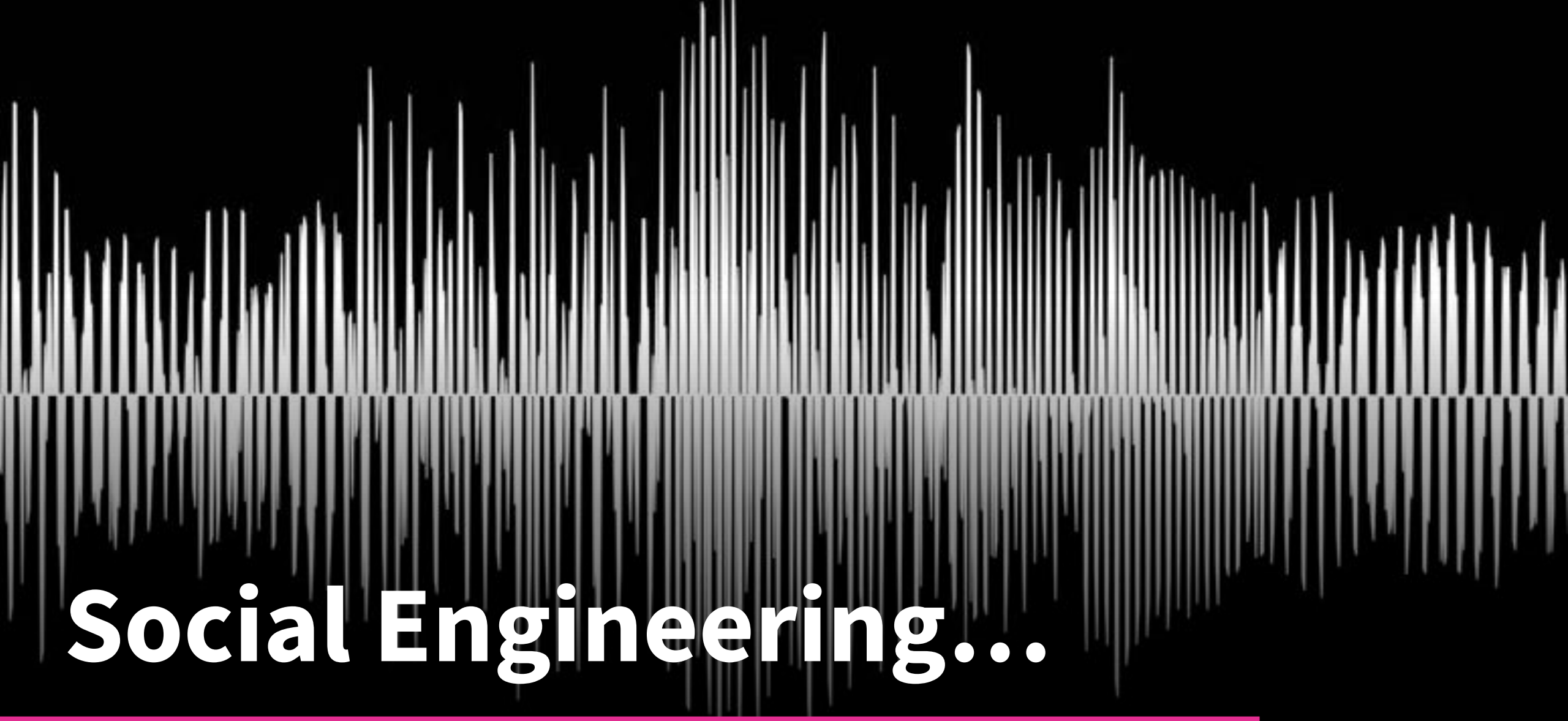
Deep Fakes...


08 - The Im
Stereo, 44100Hz
32-bit float
Mute
Solo
1.0
0.5
0.0
-0.5
-1.0


GOLDEN

Deepfake Beginnings…

Politics...



Social Engineering...

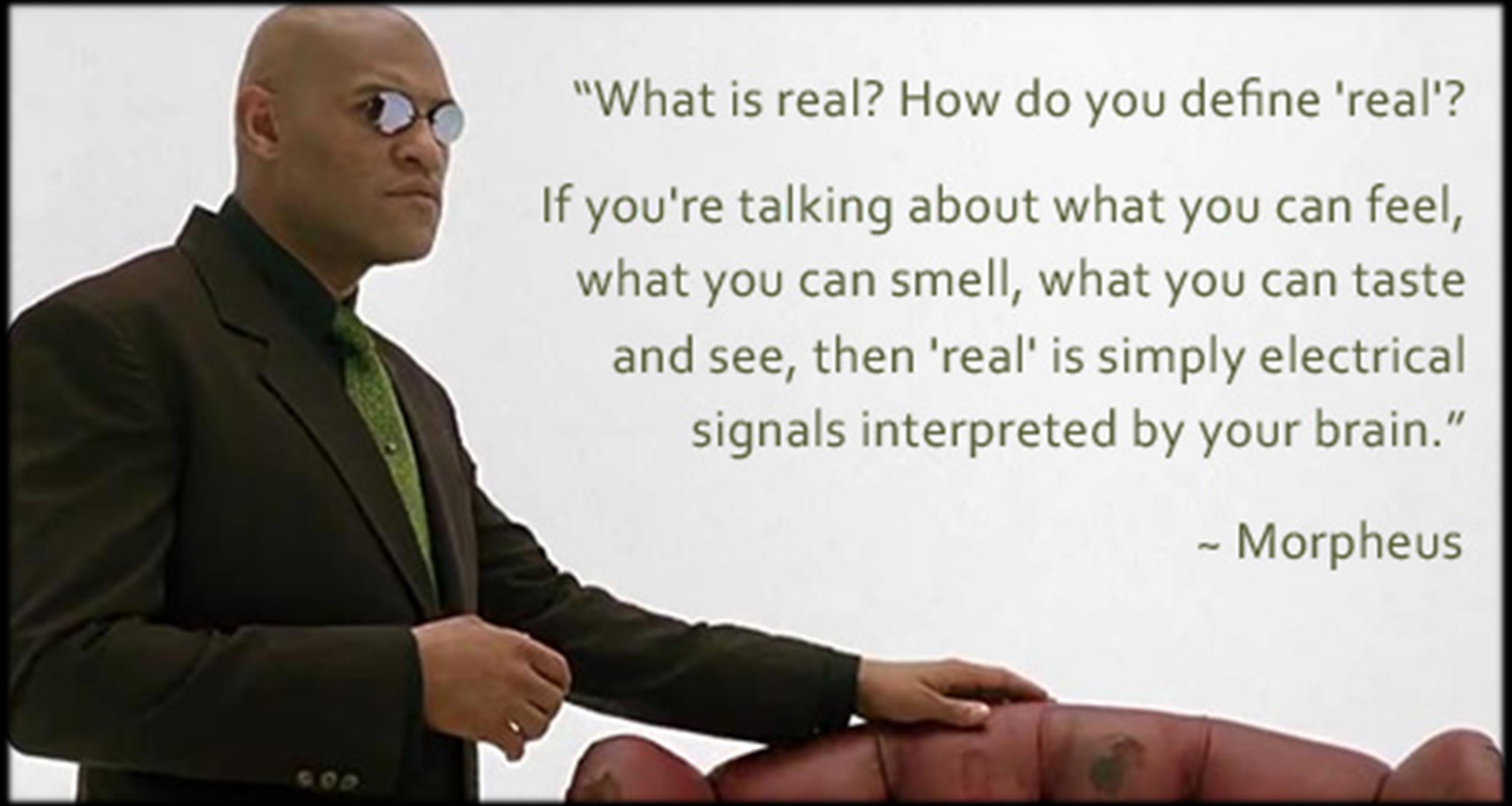
Revenge Porn...


NQUIRER
INSIDE HIS $144 BILLION SPLIT
ZOS' DIVORCE!
CHEATING
HOTOS
HAT
NDED
S MARRIAGE
HIS MISTRESS OF 8 MONTHS REVEALED
OWNER OF The Washington Post
ext sex & wild romps on his PRIVATE JET!
How he STOLE ANOTHER MOGUL'S WIFE!
PAGES OF EXCLUSIVE PHOTOS – WHAT REALLY HAPPENED

Extortion…

“Outsider” Trading…

Market Manipulation...


"What is real? How do you define 'real'?
If you're talking about what you can feel, what you can smell, what you can taste and see, then 'real' is simply electrical signals interpreted by your brain."
~ Morpheus

GANs...

Target Media

Generator

Training Set

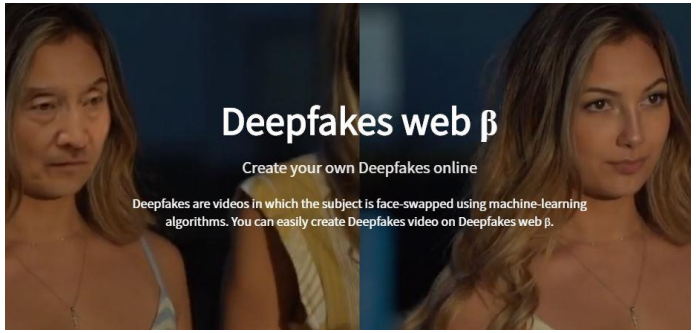
Feedback (Loss)

Discriminator

DeepFake

Consumer Deepfakes…

faceswap



DeepNude

Talking Heads…

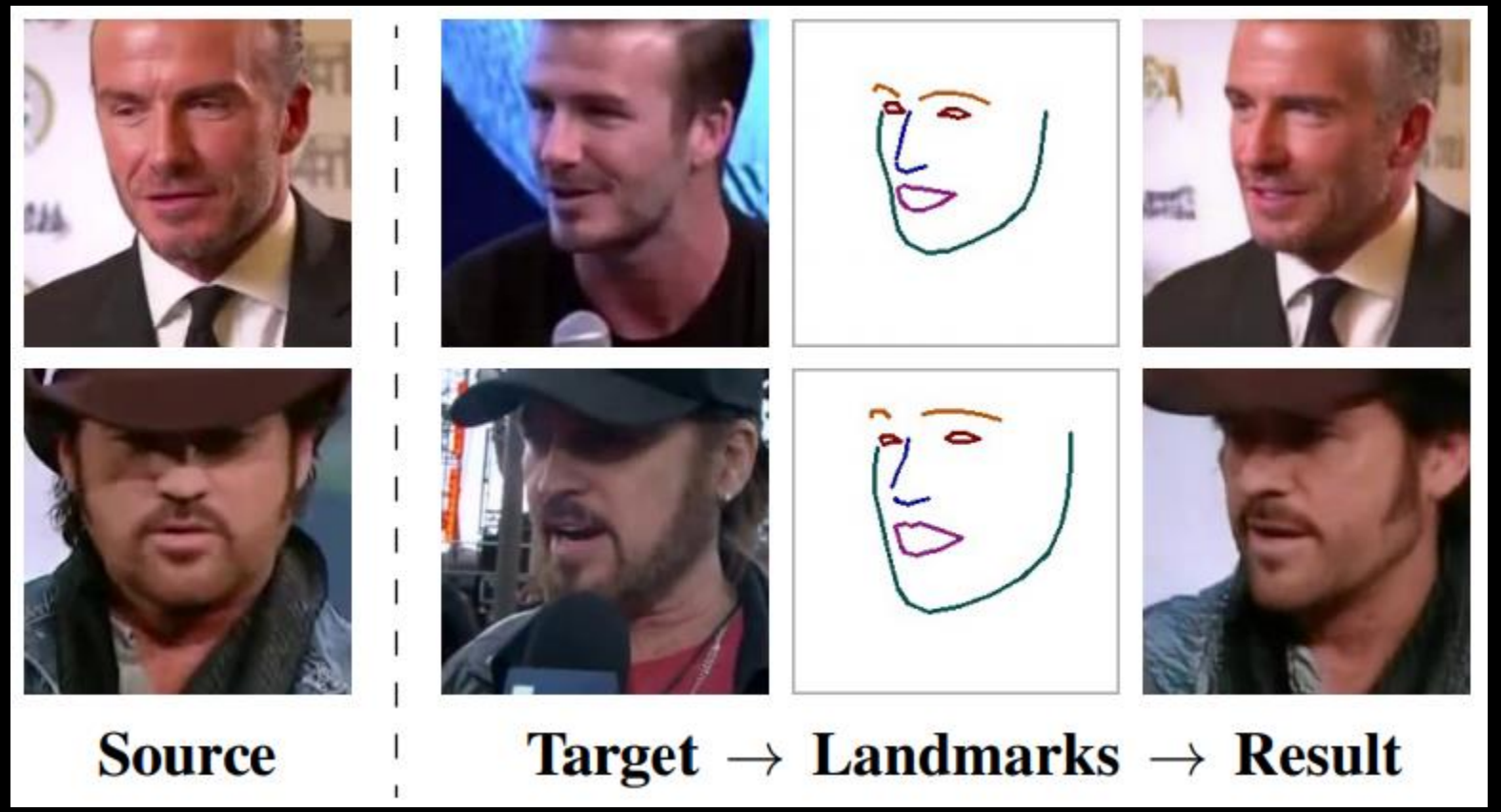


Image taken from: https://arxiv.org/pdf/1905.08233.pdf

Meta-Learning...

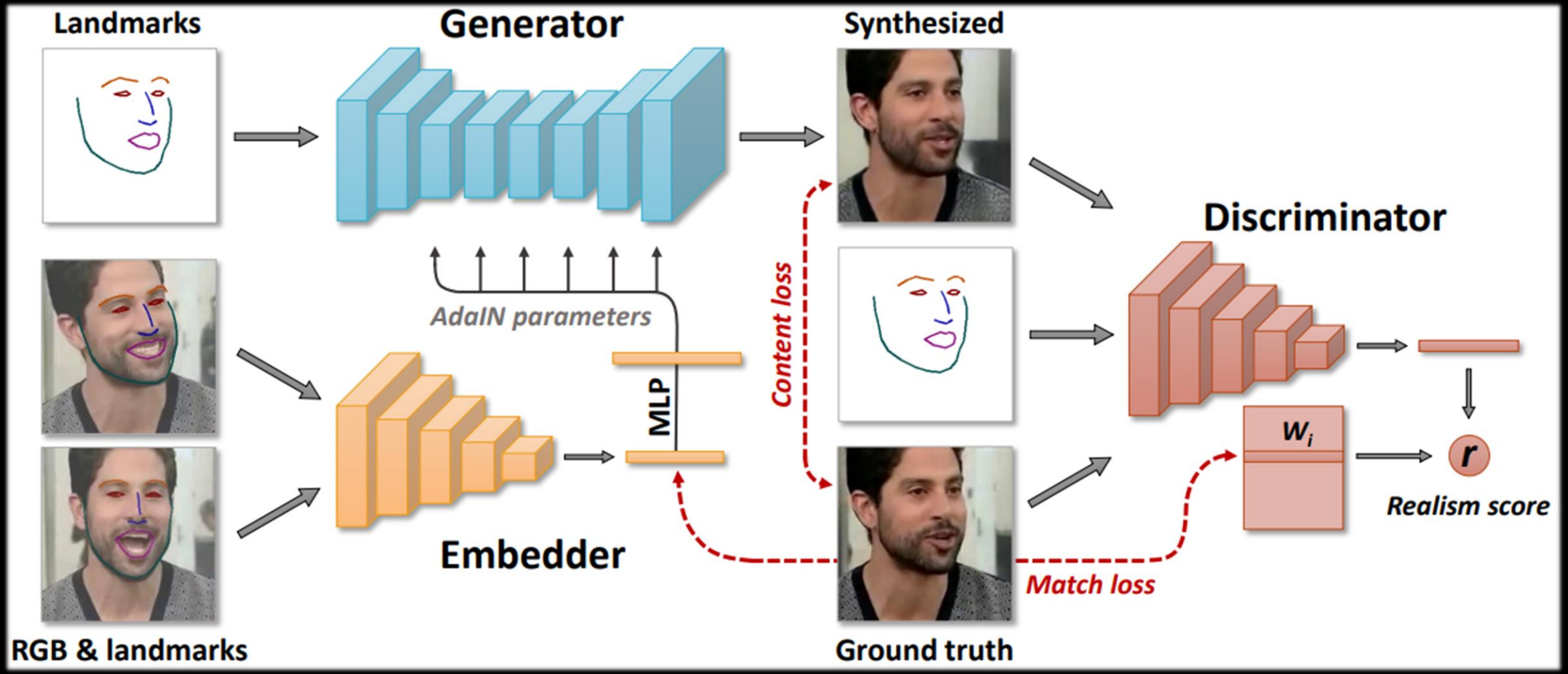
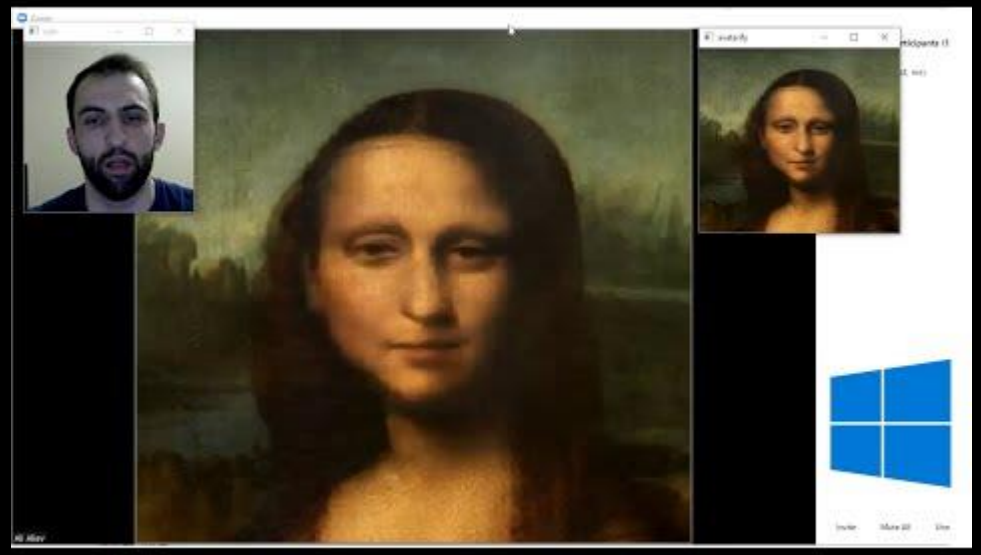
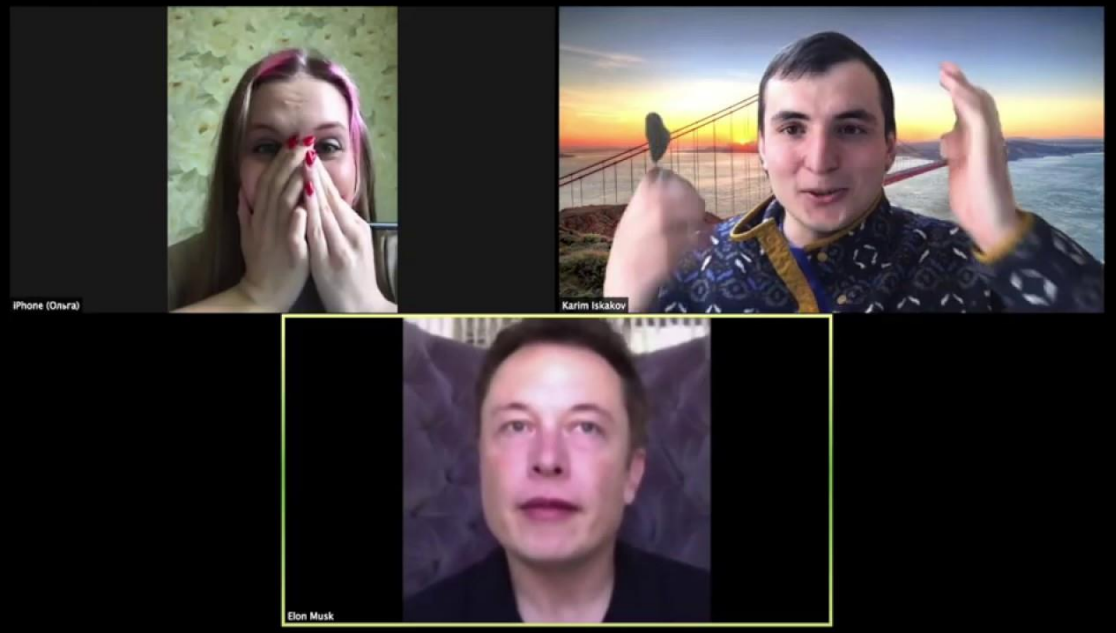


Image taken from: https://arxiv.org/pdf/1905.08233.pdf

Avatarify...





https://github.com/alievk/avatarify


REAL
FAKE

That Doesn’t Fit…

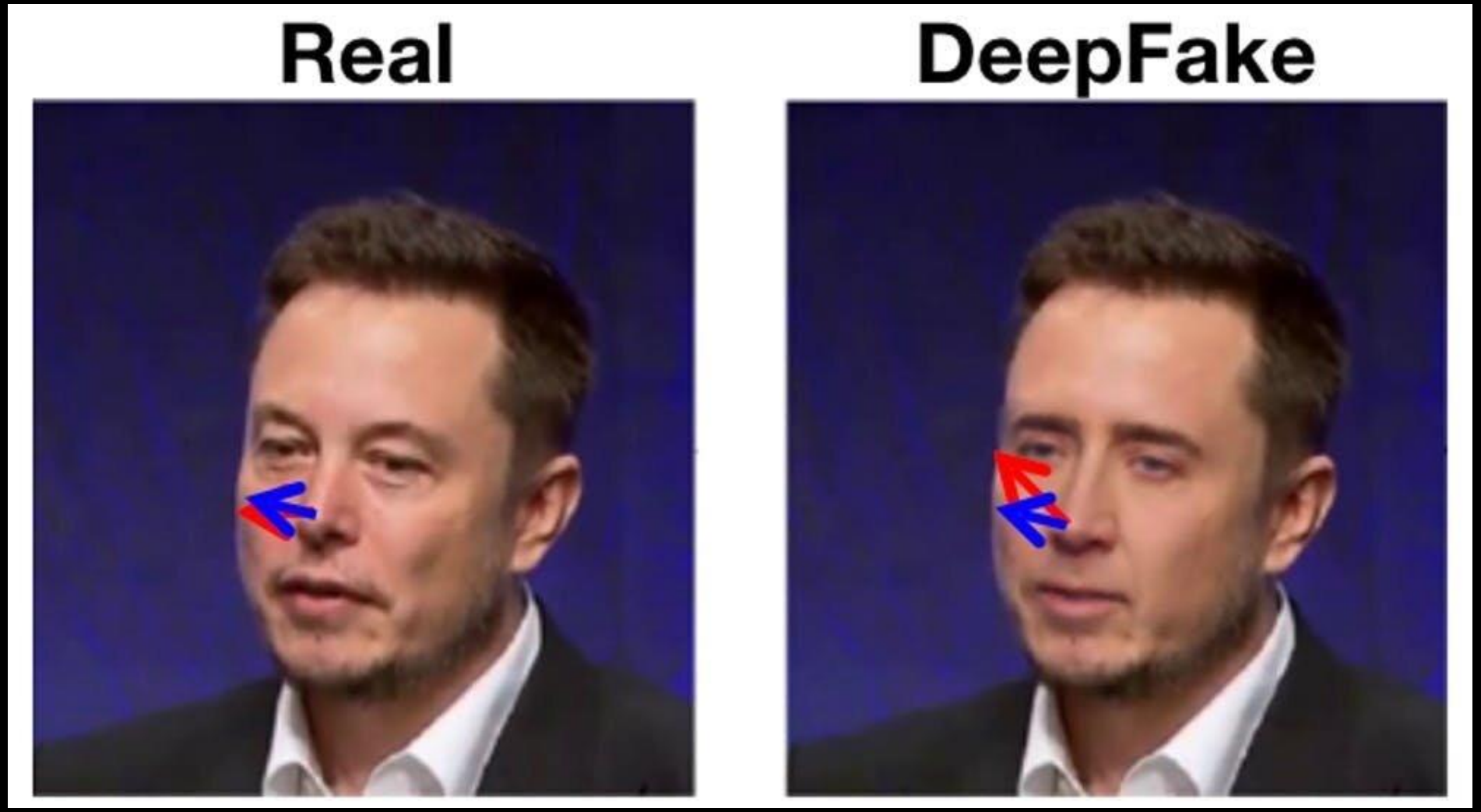


Image: Phys.org

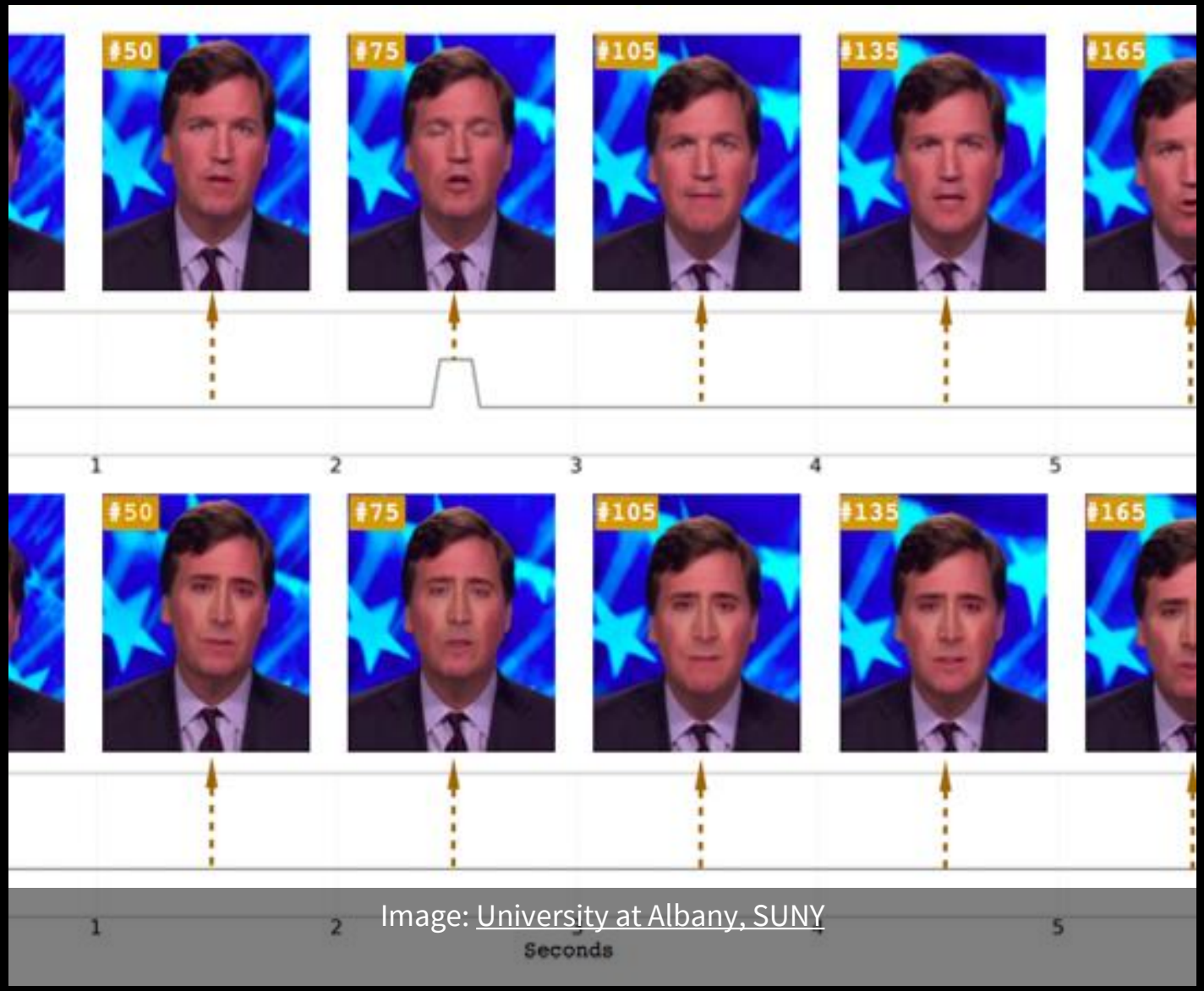


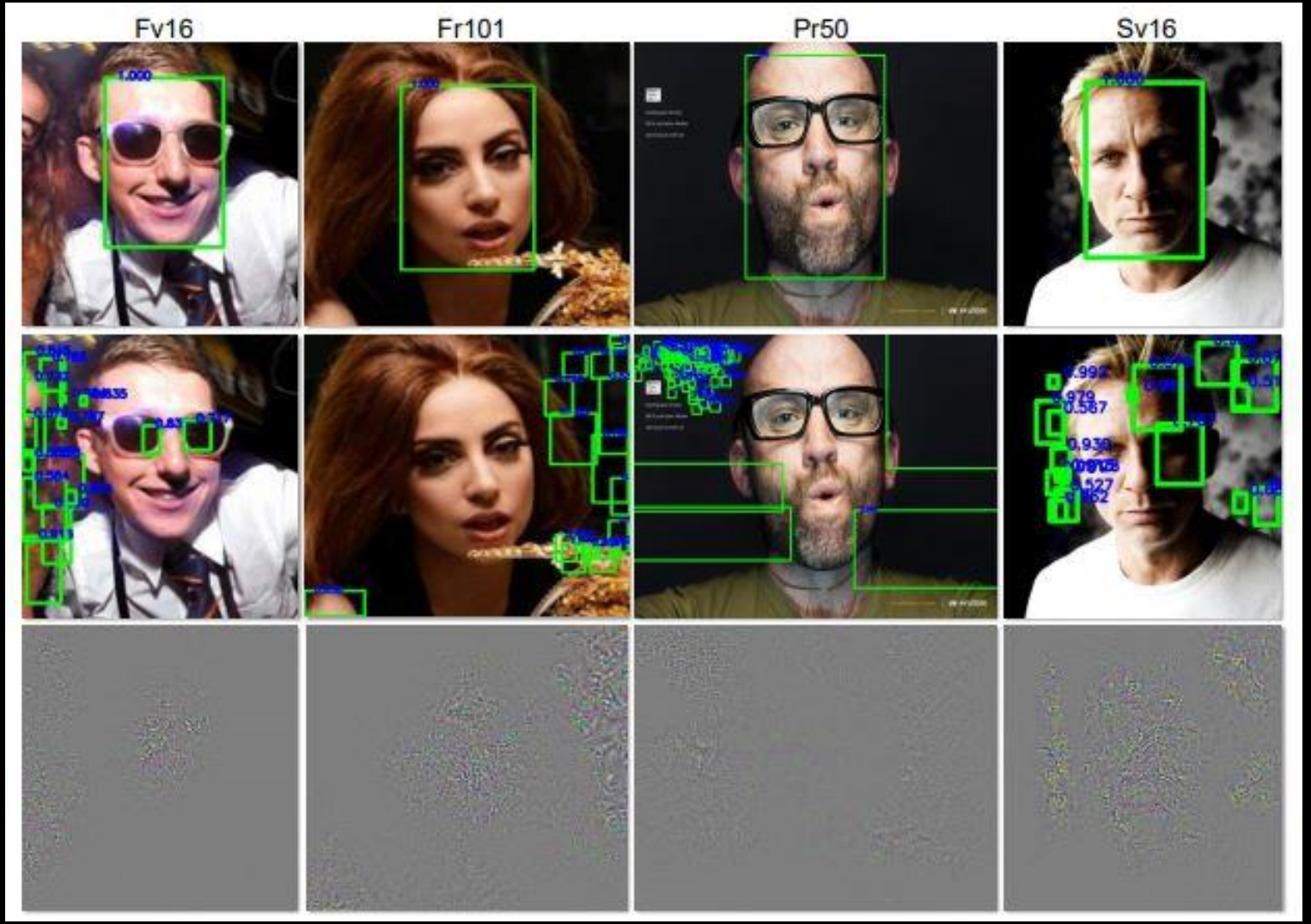
Image: University at Albany, SUNY

In The Blink of an Eye...

Warping Reality…

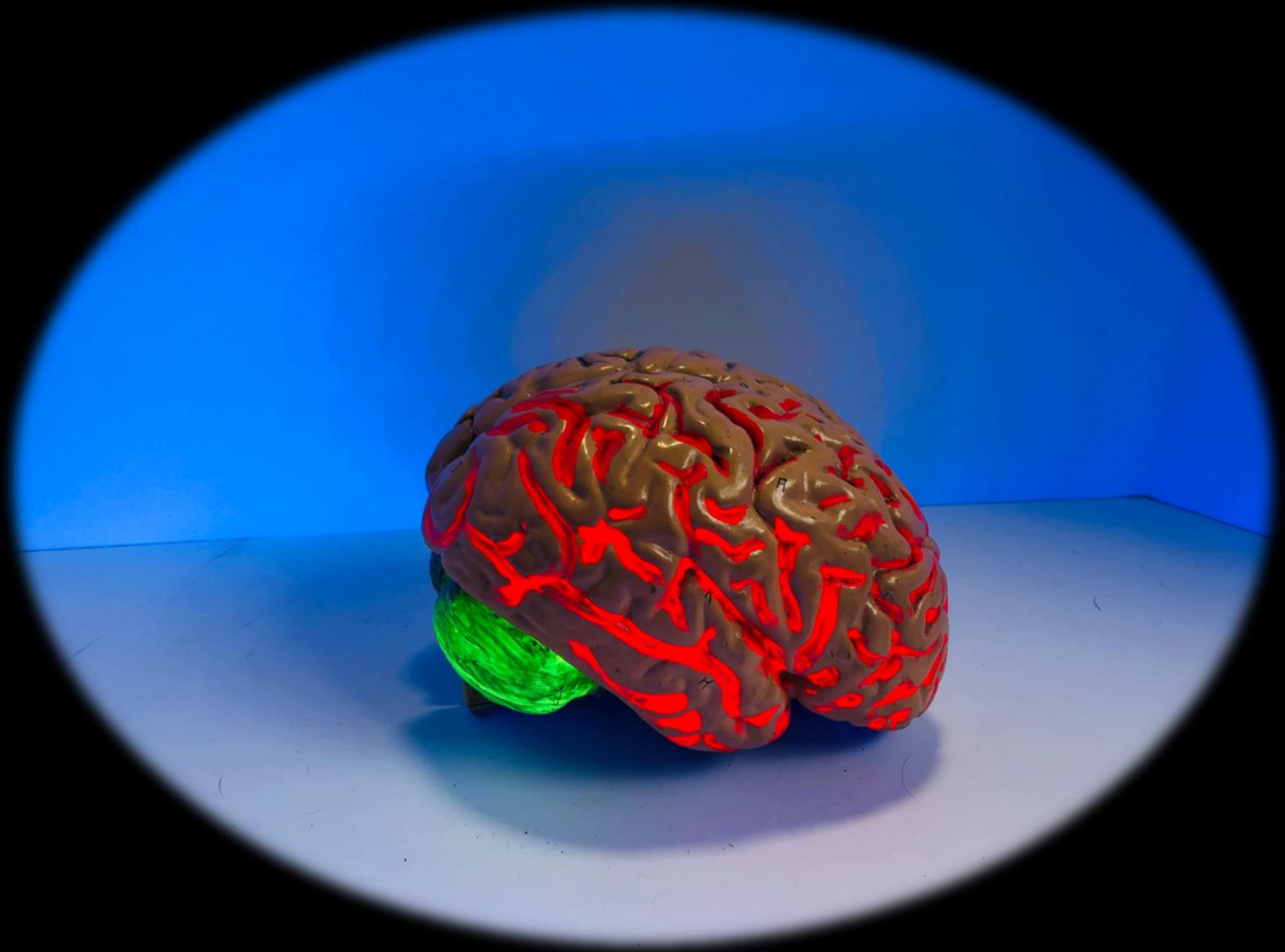
Modeling Behaviors…

An Ounce of Prevention…

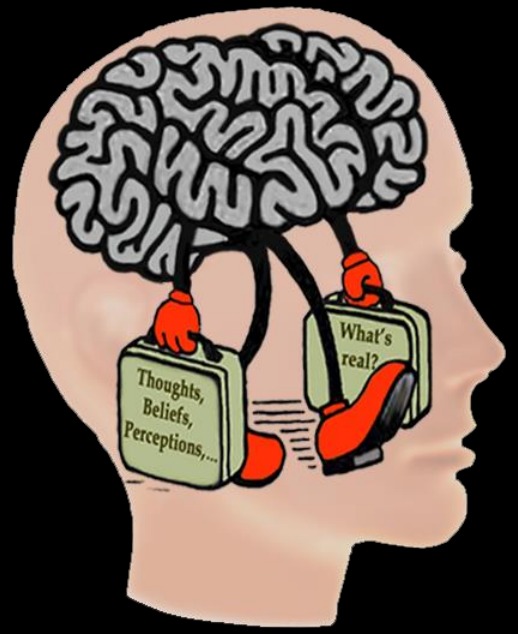


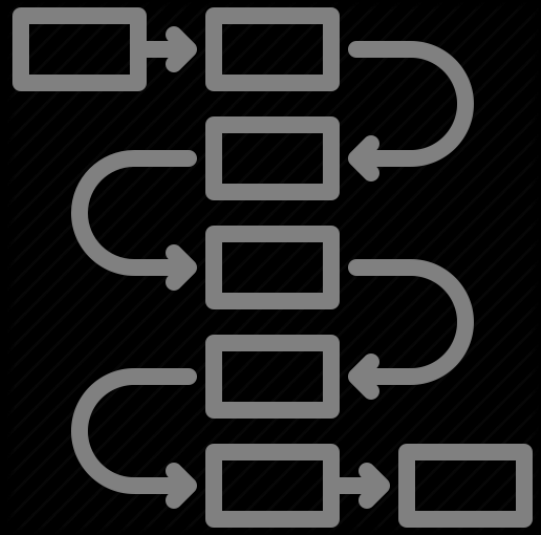
But how concerning is this threat?

Misinformation is a Human Problem

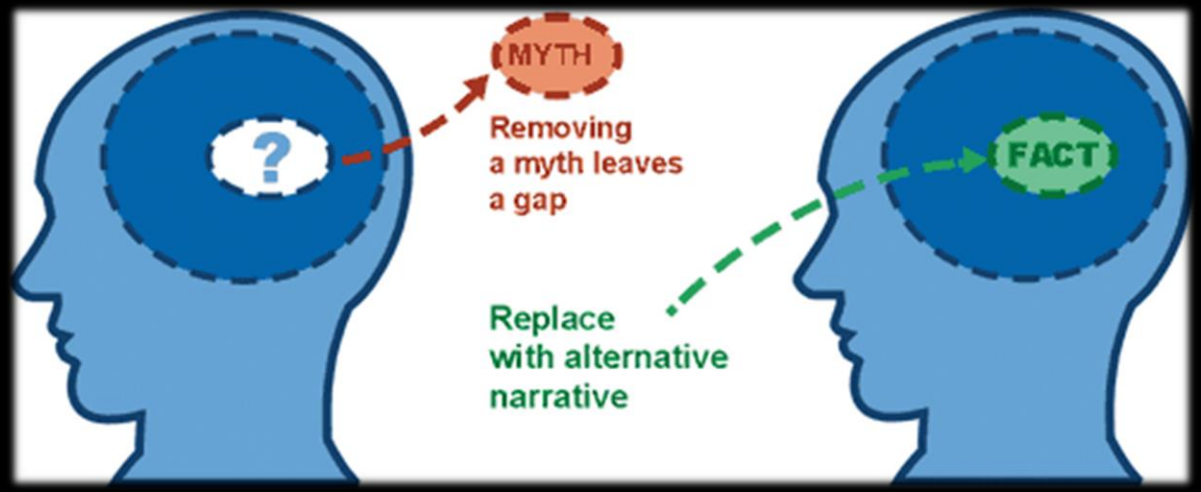


It’s So Sticky…





Debunking Misinformation...



Positive Intentions…

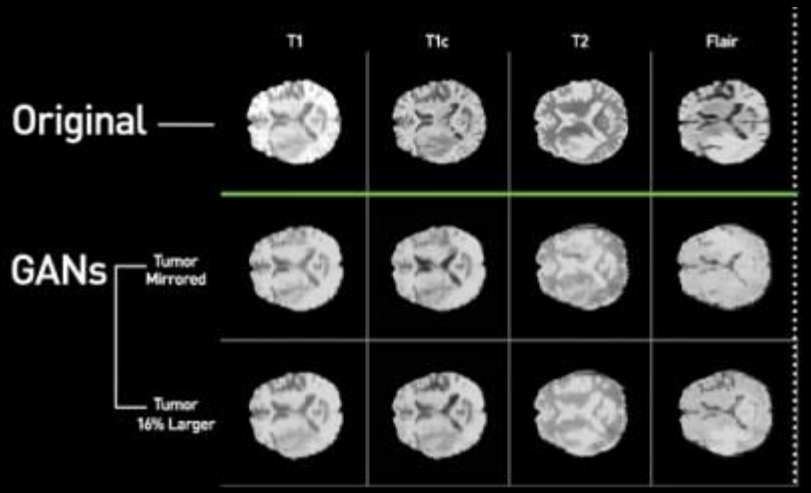


Image: Courtesy Shin et al.

"What it basically means is: to change the perception of reality of every [person] to such an extent that despite of the abundance of information no one is able to come to sensible conclusions in the interest of defending themselves, their families, their community, and their country.“

-Yuri Bezmenov (former KGB)

#ProjectDeepfake…

Example on YouTube
https://www.youtube.com/watch?v=iUOoApdY0lM

Follow on LinkedIn
https://www.linkedin.com/feed/hashtag/projectdeepfake/

Follow on Twitter
https://twitter.com/search?q=%23ProjectDeepfake

These Slides
https://github.com/r4v1np1nk/ProjectDeepFake/blob/master/LosingOurReality-AlyssaMiller-BSidesKnoxville.pdf

References…

Misinformation and its Correction
https://www.researchgate.net/publication/277816966_Misinformation_and_its_Correction

Detecting Deepfakes by Looking Closely…
https://phys.org/news/2019-06-deepfakes-reveals.html

In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking
https://arxiv.org/pdf/1806.02877.pdf

Exposing DeepFake Videos By Detecting Face Warping Artifacts
https://arxiv.org/pdf/1811.00656.pdf

Protecting World Leaders Against Deep Fakes
http://openaccess.thecvf.com/content_CVPRW_2019/papers/Media%20Forensics/Agarwal_Protecting_World_Leaders_Against_Deep_Fakes_CVPRW_2019_paper.pdf

Hiding Faces in Plain Sight: Disrupting AI Face Synthesis with Adversarial Perturbations
https://arxiv.org/pdf/1906.09288.pdf

Few-Shot Adversarial Learning of Realistic Neural Talking Head Models
https://arxiv.org/pdf/1905.08233.pdf

@AlyssaM_Infosec

/in/alyssam-infosec

https://alyssasec.com

Thank You

Alyssa

MILLER