



DEEP FAKE

Перспективы и последствия



Что такое deep fake?

Технология дип-фейк позволяет легко и с высокой достоверностью заменять лица людей на видео-записях. Таким образом, можно фальсифицировать практически любое видео с тем или иным человеком



Современные возможности технологии

- С развитием нейросетей стала доступна непрофессионалам, с минимальными аппаратными требованиями и временными затратами.
- Для тренировки нейросетей нужно большое количество свободно доступных изображений человека, поэтому в первую очередь под удар попадают актеры и политики
- Еще одна область применения, которая во много и двигает эту технологию – порнография
- Технология активно применяется в Китае, а также в США



Ближайшие перспективы

- По прогнозу одного из ведущих специалистов в области дипфейков Хао Ли, поддельные видео станут неотличимыми от реальности в течение 6-12 месяцев, то есть, скорее всего, в самый разгар предвыборной кампании в США.
- «Весьма скоро дело дойдет до того, что мы больше не сможем выявить подделки, поэтому нам придется искать другие решения», — подчеркивает Хао Ли.
- Возможно эти дипфейки повлияют на ход кампании в США, как это произошло с таргетированной рекламой и троллями в Facebook в прошлом электоральном цикле

Какие опасности несет в себе технология?

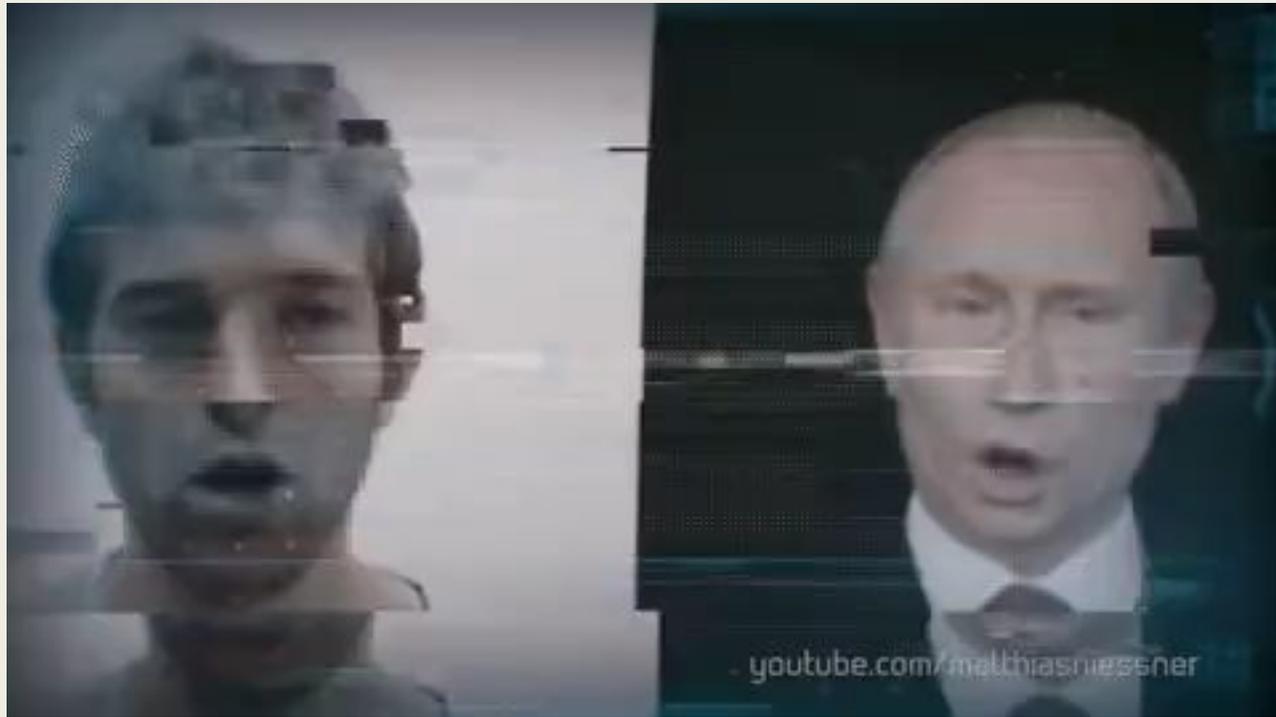
- Невозможно настроить автоматическое определение подделок

Возрастает роль модератора. Только человек способен (и то не всегда) распознать подделку

- Распознавание дипфейков срабатывает слишком поздно

Крайне сложно убрать из Сети то, что туда однажды попало. Можно убрать видео с площадки, но невозможно из мессенджеров

- Дипфейки могут вывести политическую пропаганду и контрпропаганду на невиданный ранее уровень



Предпринимаемые меры

- Недавно штат Калифорния запретил предвыборные дипфейки, но запрет касается только роликов с политиками и длится в период 60 дней перед выборами.
- Стало известно, что в Китае фактически запретят использование дипфейков. Управление по вопросам киберпространства КНР требует при производстве и распространении подобных материалов в явном виде указывать использование соответствующих технологий, а невыполнение этих требований будет считаться уголовным преступлением. Вступает в силу в 2020 году.

Как технология повлияет?

- Влияние технологии на область контрпропаганды:
 - Крамольные заявления кандидата
 - Неприличные, возмутительные действия кандидата
 - Незаконные действия (взятки, передача секретной информации и т.п.)

- Любая попытка человека, попавшего под удар технологии, упрется в его возможности по донесению «правды». По сути, окончательная «правда» окажется в руках того, кто контролирует большие каналы передачи информации.

- Настоящий кандидат «Иванов» - не тот, у кого паспорт на это имя, а тот у кого больше подписчиков.

Главное следствие развития технологии

- Полное исключение видео-контента из области доверия.
Первые десятки дипфейков могут произвести эффект разорвавшийся бомбы. Однако в дальнейшем, аудитория может оказаться полностью дезориентирована и отказаться верить в какие-либо видео доказательства.
- Для контента будет найден новый способ авторизации
- Если способ не будет найден – должна будет измениться сама информационная реальность, учитывающая невозможность отличить реальное событие от виртуального