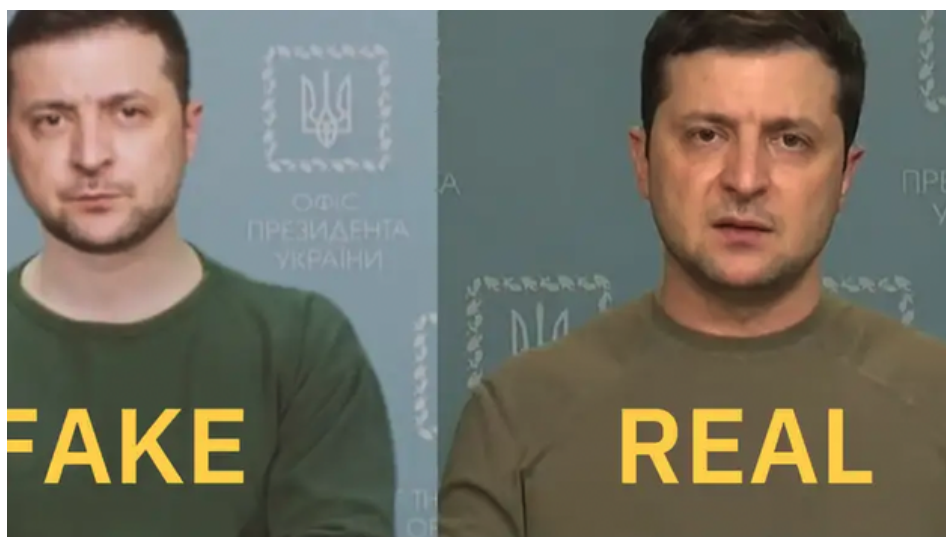


Lương Thái Sỹ - Deepfake, trò đùa cực kỳ nguy hiểm

27/3/2022



Vào tuần thứ ba cuộc xâm lược của Nga ở Ukraine, Tổng thống Ukraine Volodymyr Zelensky bất ngờ xuất hiện trong một video, mặc áo sơ mi màu xanh lá cây sẫm quen thuộc, nói chậm rãi, khi ông đứng sau bục tổng thống màu trắng có quốc huy. Ngoại trừ đầu, cơ thể Zelensky hầu như không cử động khi nói. Giọng thì méo mó và gần như khô khốc khi ông khuyên người dân Ukraine hãy đầu hàng Nga.

“Tôi yêu cầu các bạn hạ vũ khí và trở về với gia đình. Cuộc chiến này không đáng để hy sinh. Tôi đề nghị các bạn hãy tiếp tục sống, và tôi cũng sẽ làm như thế” – Zelensky nói tiếng Ukraine. Nhưng ngay lúc đó, người nghe nhanh chóng xác định đây là một màn đánh lừa, mạo danh tổng thống. Và màn tuyên truyền bị lật mặt nạ ngay lập tức.

Cách đây năm năm, hầu như không có ai nghe nói đến deepfake, một từ mới dùng để chỉ những tệp video và tệp âm thanh trông rất thuyết phục nhưng... “xạo láo” và được tạo ra có mục đích, với sự trợ giúp của trí khôn nhân tạo (AI). Bây giờ, chúng được sử

dụng để tác động lên một cuộc chiến chưa biết bao giờ mới kết thúc. Ngoài video Zelensky giả mạo, được lan truyền vào tuần trước, còn có một video deepfake khác cũng được phát tán rộng rãi, trong đó Tổng thống Nga Vladimir Putin tuyên bố “hòa bình”, kết thúc cuộc chiến Ukraine!

Trong nhiều năm qua các chuyên gia về thông tin sai lệch và tính xác thực của các nội dung được lan truyền trên mạng đã lo lắng về khả năng phổ biến những điều dối trá và gây hoang mang bằng kỹ thuật “phù phép” tinh vi. Nhờ sự phát triển vũ bão của AI nên những video lừa đảo ngày càng giống thực hơn. Nhìn chung, deepfake đã được cải thiện rất nhiều trong một khoảng thời gian tương đối ngắn. Chẳng hạn, video cảnh nam diễn viên Tom Cruise tung đồng xu và video cover các bài hát của Ban nhạc Dave Matthews vào năm ngoái, cho thấy deepfake đã “giống thực một cách thuyết phục” như thế nào.

Cả video của Zelensky hay Putin đều không đạt được hiệu quả cao như video Tom Cruise trên TikTok (chúng có độ phân giải thấp, một chiến thuật phổ biến để che giấu những lỗi). Nhưng các chuyên gia không hề đánh giá thấp sự nguy hiểm của chúng. Đó là bởi tốc độ phát tán quá nhanh của các thông tin sai lệch sử dụng công nghệ cao ở qui mô toàn cầu khi nhiều người không có khả năng hoặc không kịp nhận biết đâu là thật đâu là giả. Deepfake ngày càng được sử dụng nhiều trên mạng cũng có nghĩa là việc phát hiện ra chúng sẽ khó khăn hơn nhiều.

Cuộc chiến Ukraine khi được chuyển tải lên mạng có đầy rẫy thông tin sai lệch. “Chỉ cần một “mảnh bòn” tin giả cũng có thể làm vẩn đục cả vùng nước thông tin tình hình chiến sự – Wael Abd-Almageed, phó giáo sư nghiên cứu tại Đại học Nam California kiêm Giám đốc sáng lập Phòng thí nghiệm Phân tích đa phương tiện và Trí tuệ thị giác

của trường nhận định – Một khi ranh giới thực-giả bị xói mòn, ngay cả sự thật cũng sẽ bị nghi ngờ, thậm chí... không tồn tại. Bị lừa vài lần, bất cứ những gì bạn nhìn thấy cũng bị nghi là giả và bạn không thể tin vào chúng nữa. Mọi thứ xuất hiện trên mạng đều trở thành giả dối. Nhiều người đã mất niềm tin.

Quay trở lại năm 2019, thời điểm bắt đầu xuất hiện mối lo ngại về những lệch lạc có thể ảnh hưởng nghiêm trọng đến kết quả cuộc bầu cử tổng thống Mỹ năm 2020. Dan Coats, Giám đốc Tình báo Quốc gia Mỹ lúc đó cảnh báo về khả năng này. Dù điều đó không xảy ra nhưng số người tin vào các thuyết âm mưu không hề nhỏ. Siwei Lyu, Giám đốc Phòng thí nghiệm Computer vision and Machine learning tại Đại học Albany, cho biết, lúc đó, deepfake chưa đạt đến trình độ cao. Không dễ dàng tạo ra một deepfake tốt, một video giả mạo ‘bạc thầy’ đánh lừa được số đông với giọng nói giống thực, ngôn ngữ cơ thể như thực (video Zelensky bị phát hiện vì cơ thể cứng đờ không chuyển động).

Giờ đây, việc tạo ra các bản deepfake tốt đã dễ dàng hơn nhiều và cũng nguy hiểm hơn khi chúng được sử dụng trong một cuộc chiến tranh để kích động những cái đầu nóng và gây hiểu lầm. Cách deepfake đang dùng để tác động đến người xem trong chiến tranh là đặc biệt nguy hiểm, vì nó dẫn đến phản ứng tiếp theo dựa vào những thông tin giả, dù là tiếng hay hình. Người xem nhầm lẫn sẽ dẫn đến hậu quả khó lường. Trong những video giả như Tom Cruise, deepfake không có nhiều tác động ngoài việc thu hút sự quan tâm và chú ý. Nhưng trong những tình huống nguy cấp, chiến tranh hay thảm họa, khi mọi người không có thời gian để suy nghĩ thấu đáo và phải phản ứng trong một khoảng thời gian rất ngắn, thông tin giả thực sự trở thành vấn đề lớn.

Thực tế cho thấy, việc đưa ra những thông tin sai lệch đã làm phức tạp thêm cuộc chiến Ukraine. Cuộc xâm lược của Nga lôi kéo theo một lượng cực lớn thông tin theo thời gian thực trên cả truyền thông chính thống lẫn các nền tảng xã hội như Twitter, Facebook, Instagram và TikTok. Phần lớn là tin thật, nhưng một số là giả hoặc đưa theo cách để gây hiểu lầm. Bản chất trực quan của những thông tin được chia sẻ cùng với mật độ, tần xuất và cách chúng tấn công mạnh vào cảm xúc sẽ khiến chúng ta dễ mất cảnh giác. Đây chính là lúc tin giả hoàn thành sứ mệnh của nó và trở thành... tin thật nhờ có quá nhiều người tin. Nina Schick, tác giả của cuốn Deepfakes: The Coming Infocalypse xem hai video Zelensky và Putin là dấu hiệu cho thấy vấn nạn tin giả trên mạng lớn hơn nhiều so với mường tượng của chúng ta.

Khi deepfake trở nên tinh vi và hoàn hảo hơn, các nhà nghiên cứu và các công ty cố gắng nâng cấp các công cụ phát hiện để sớm loại bỏ chúng. Abd-Almageed và Lyu sử dụng thuật toán để phát hiện deepfake. Giải pháp của Lyu, được đặt tên là DeepFake-o-meter, cho phép bất kỳ ai cũng có thể tải video nghi ngờ lên để kiểm tra tính xác thực, dù có thể mất vài giờ mới có kết quả (vài giờ là quá đủ để gây hậu quả nghiêm trọng cho một sự kiện đang nóng).

Một số công ty, chẳng hạn như nhà cung cấp phần mềm an ninh mạng Zemana, đang nghiên cứu phát triển phần mềm phát hiện deepfake. Dĩ nhiên, tính năng phát hiện tự động phải cập nhật thường xuyên cho theo kịp với trình độ giả mạo và đánh lừa thị giác, thính giác của các “bậc thầy” deepfake. Ví dụ, năm 2018, Lyu đã tìm ra cách phát hiện video deepfake nhờ quan sát bất thường cử động mắt của nhân vật trong video. Nhưng chưa đầy một tháng sau, kẻ lừa đảo nào đó đã làm được video chớp mắt giống

như thật! Tại Mỹ, đã có một số luật để giải quyết vấn nạn deepfake, chẳng hạn luật của tiểu bang California được thông qua vào năm 2019 cấm phân phối video và âm thanh giả mạo của các ứng viên chính trị trong vòng 60 ngày trước ngày bầu cử.

<https://saigonnhonews.com>