BROOKINGS

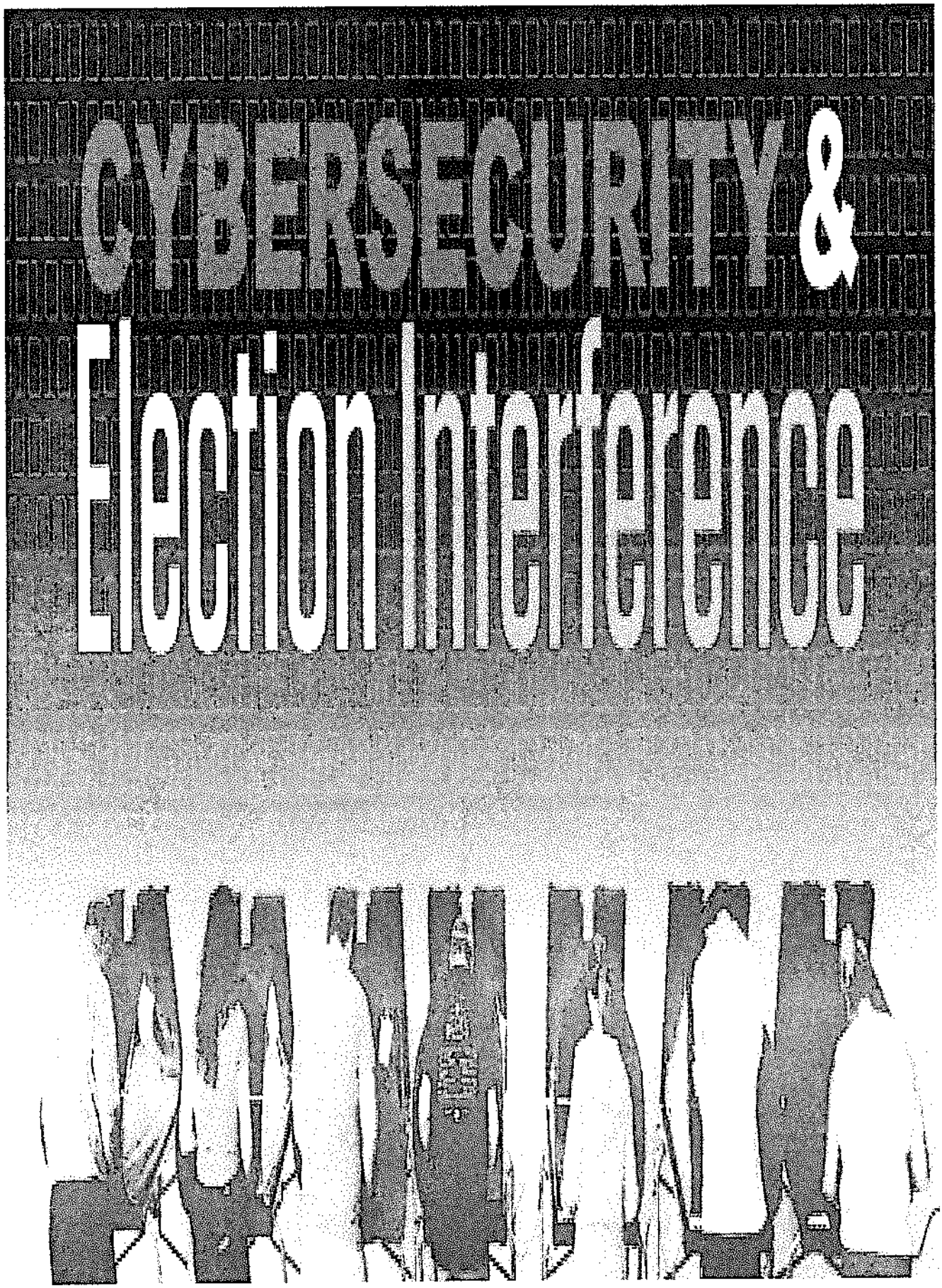
TechTank

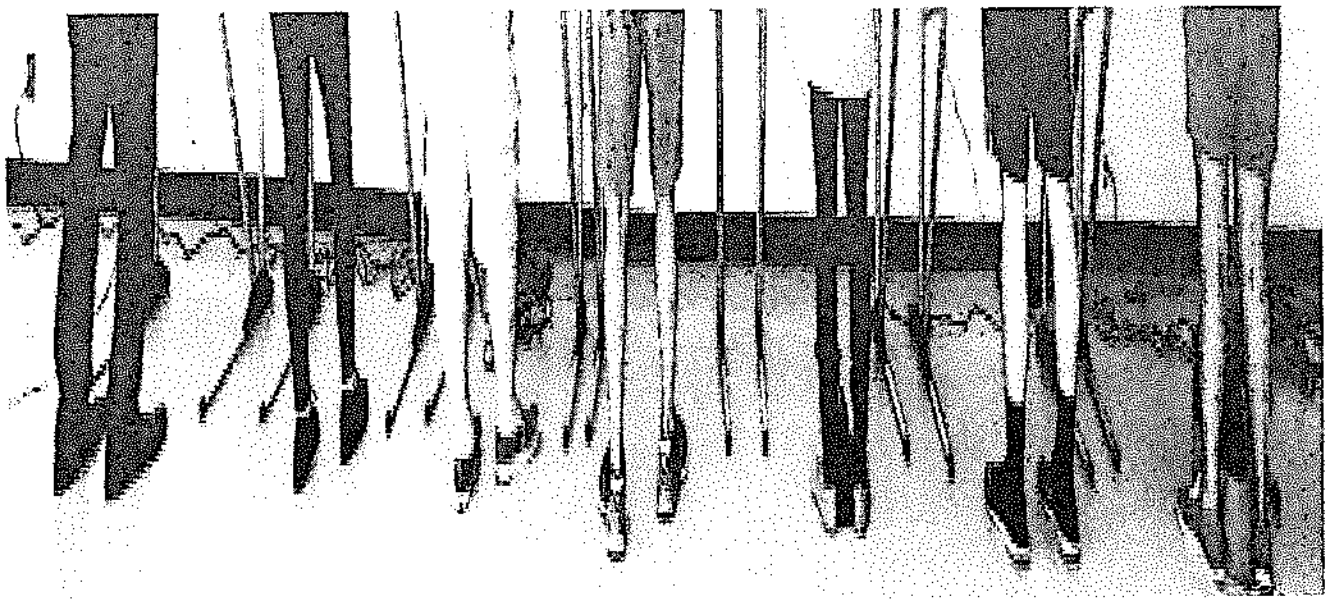
Digital threats to campaign 2020: Fake nudes, doctored images, and widespread disinformation

Darrell M. WestThursday, July 11, 2019

Editor's Note:

This post is part of "Cybersecurity and Election Interference," a Brookings series that explores digital threats to American democracy, cybersecurity risks in elections, and ways to mitigate possible problems.


CYBERSECURITY &
Election Interference



You are sitting at home watching online videos and a friend sends you a link showing a seemingly real image of Senator Kamala Harris removing her clothes. She had recently done well in a television debate and was garnering widespread praise for her takedown of Democratic frontrunner Joe Biden. You watch with amazement. Is this for real? Would a United States Senator allow herself to be filmed doing that? How many people will see this? How is it going to affect the campaign?

Of course, the picture is not authentic. It is a "deepfake," something that no longer lies within the realm of science fiction or political fantasy. An AI developer named "Alberto" created grave consternation recently when he devised a "DeepNude" app that could "digitally undress women". The software "used artificial intelligence to create the 'deepfake' images, presenting realistic approximations of what a woman – it was not designed to work on men – might look like without her clothes."[1] The depictions were so realistic that they appeared genuine to many viewers. The backlash which ensued from his application was so strong that he took down the offering within a few days of starting to sell it for $50. In an interview, he explained he was able to create the tool by training it on 10,000 pictures of naked women. However, other developers have replicated the software so the world is not safe from DeepNude knockoffs.[2]

This and other types of inventions show how far technology has come and what the political, ethical, and societal risks are as we head into Campaign 2020. Through current software, it is possible to develop and distribute content that is offensive and abusive. Editing tools are widely available to virtually anyone with access to a computer. Public skepticism about journalists means it likely will be difficult for news fact-checkers and gatekeepers to act as a counterweight to digital disinformation, doctored images, divisive rhetoric, and outright falsehoods. As took place in 2016, automated bots can distribute such materials widely and potentially affect the election outcome.

Digital disinformation

Brookings Senior Fellow Elaine Kamarck recently noted that electoral dirty tricks are not new.[3] She outlines a long history of disruptive tactics and deliberate disinformation being used to take down political opponents. Her litany of examples is quite striking: a letter in 1972 accusing Senator Edmund Muskie of using a derogatory word for French Canadians, robocalls in 2000 claiming Senator John McCain had fathered an illegitimate black child, 2004 ads claiming Senator John Kerry didn't deserve the medals he earned during the Vietnam War, and the 2016 "Pizzagate" story saying leading Democrats were engaged in a child sex ring.

But in as we move into the 2020 campaign, there are new disinformation risks. Social media platforms enable offensive materials to be widely distributed. The country is quite polarized and there is a widespread tendency to view political opponents as enemies to be destroyed leading to a willingness to believe the worst about your opponents. Traditional journalists and fact-checkers don't have the ability to police the digital frontier. And social media platforms have shown a reluctance to police themselves too aggressively. After it was discovered that a slowed down video of Speaker Nancy Pelosi made her look bumbling, possibly drunk, and out of touch, Facebook refused to take down the video, merely

labeling it as fake and something viewers should judge for themselves.[4] All of these features creates a ready-made environment for the online distribution of toxic information.

Combined with a digital world where people get considerable information over the internet, there is the potential for widespread abuse of photo editing tools, online videos, social media, and digital platforms. With a historic number of female and minority candidates for president, one has to be alert to the very real possibility of deep fake videos presenting unflattering or abusive images of women and minority aspirants in an effort to discredit them. It is easy to manipulate still images or video footage to put someone in a compromising situation or engaging in despicable acts, even if the individual was not actually present for the activity. One can manufacture footage showing a candidate saying something highly objectionable even if that person did not utter the words.

Sowing discontent

One of the classic ways to sow discontent and reduce support for an opponent is to associate him or her with unpopular issues, causes, or people. Republicans already are waving the socialist flag in an effort to tie a number of Democratic proposals to far-left ideology. And Democrats are accusing President Donald Trump of authoritarianism, militarism, and fascism as they confront his presidency and seek to paint him as dangerous and extremist.

With digital technology, it is easy to blend images of particular candidates espousing liberal positions with pictures of leaders in Cuba or Venezuela, and claim their views are outside the American mainstream. Likewise, President Trump's penchant to praise authoritarian leaders in other countries such as North Korea, the Philippines, and Russia opens him to digital strategies tying him to outlandish acts, real or imagined.

In a divided country, it is easy to spread inaccurate information that inflames people and creates political discontent. In 2016, for example, Democrat Hillary Clinton was accused of having major health issues after she fainted following a campaign appearance. Some African Americans were provided information through electronic means about Democratic leaders doing nothing to help them. At various points in recent years, white, rural voters erroneously were told liberal Democrats planned to take their guns away. Deceptive or misleading information through online tools or fake videos could further divide a country that already is seriously polarized.

Suppressing the vote

It is possible to win elections not just through political persuasion but by convincing important blocs of voters that their preferred candidate is a dishonest career politician out for him or herself and it therefore is a waste of time for them to vote. If you can get enough people in swing states not to vote or waste their ballot on a third party candidate, it is possible to triumph politically.

In this type of situation, one can imagine digital suppression activities targeted on key voting blocs. Opponents can play to common stereotypes and convey appeals based on people's hopes or fears. They can develop false information that leads individuals to be cynical and not to vote. In a close election, those strategies could tilt the contest one direction or another.

Interfering with the count

There are a wide variety of ways that the vote count itself could be compromised. Many people wonder why we can't vote online and the answer is simple. Small errors, intentional or otherwise, in the software code could, for example, delete every seventh Democratic or Republican vote. Or entire precincts could disappear in the transmission of results from precinct to county or county to state. In fact,

the possibility of digital mischief in counting the vote is so noteworthy that many states have disconnected voting machines from the internet and are going back to paper backup ballots to be used in the case of a recount.

These risks are problematic because America has an electoral system that largely is administered at the state and local levels. Most of the local agencies lack much in the way of cybersecurity expertise and are not well-equipped to prevent hacking or safeguard software. The kind of expertise needed for effective oversight and supervision simply is lacking in many jurisdictions. This expertise gap creates the potential for meddling in highly targeted geographic ways. Miscreants can focus on a few counties in crucial swing states and seek to throw the election.

Tampering with voter registration data

There already is evidence that foreign agents have hacked state voter registration databases. According to the FBI, Russians successfully infiltrated registration data in at least two Florida counties during the 2016 presidential election.[5] Since that is the information source which election officials use to determine who is eligible to vote, it is an ominous vulnerability. Foreign agents who get into registration databases could alter information, disqualify voters, or otherwise create electoral havoc. It is a disruption that could prevent specific people from voting and threaten the election itself.

Undermining the legitimacy of the election

Even if one's preferred candidate loses, it is possible with weaponized digital tools to weaken the ultimate winner by casting doubt on his or her legitimacy. The United States has convoluted election rules and it is possible to create doubts through a number of different scenarios that analysts say are possible in 2020. For example, commentator Jeff Greenfield describes three ominous options: a state

legislature rejects the popular vote and casts its Electoral College votes the way it wants (as opposed to in line with voter preferences), the U.S. House of Representatives refuses to accept votes from particular states, or the absence of an Electoral College majority tosses the race into the House, where each state delegation has one vote. With Republicans holding a majority of state delegations, there is a good chance under this scenario the House would choose the GOP candidate as the next president.[6]

With any of these results, it is easy to see a number of Americans not accepting the ultimate electoral result as legitimate and seeing the verdict as unfair or unjust. They could conclude the winning party used nefarious means to produce a victory. They could see the results as completely tainted and therefore not accept the authority of the resulting administration.

Conclusion

The DeepNude app mentioned at the beginning of this piece clearly violates most people's expectations of responsible technology utilization. It goes way beyond what nearly everyone would consider reasonable and ethical, but is perfectly legal under most current jurisprudence. Even though it is highly objectionable, the fact that it relies upon digitally-generated images puts it beyond the scope of most existing legal, policy, or regulatory restrictions.

Given this situation, America needs to reconsider its generally libertarian stance towards technology regulation and enact guardrails against malicious and non-consensual uses of editing software. One of the first states to recognize this problem was Virginia. In 2019, it enacted a statute outlawing the distribution of nude "falsely created videographic or still image[s]" of actual people without that person's consent.[7] The hope was clear penalties would discourage nefarious or

exploitative behavior of the sort discussed here. Before 2020 voting takes place, other jurisdictions should consider similar legislation in order to impose penalties on those producing or transmitting abusive digital images.

---

[1]Taylor Telford, "'The World Is Not Yet Ready for DeepNude': Creator Kills App That Uses AI to Fake Naked Images of Women," *Washington Post*, June 28, 2019.

[2]Joseph Cox, "GitHub Removed Open Source Versions of DeepNude," *Motherboard*, July 9, 2019.

[3]Elaine Kamarck, "A Short History of Dirty Tricks in Political Campaigns Before Social Media," Brookings Institution policy report, July 8, 2019.

[4]Cecilia Kang, "Nancy Pelosi Criticizes Facebook for Handling of Altered Videos," *New York Times*, May 29, 2019.

[5]Gary Fineout, "Russians Accessed Voter Records in 2 Florida Counties, FBI Confirms," *Politico*, May 14, 2019.

[6]Jeff Greenfield, "How the 2020 Election Could Go Off the Rails," *Politico*, May 15, 2019.

[7]Kate Cox, "Deepfake Revenge Porn Distribution Now a Crime in Virginia," *Ars Technica*, July 1, 2019.