


# 'Deepfakes' a national security threat

 [washingtonexaminer.com/policy/defense-national-security/deepfakes-a-national-security-threat](https://www.washingtonexaminer.com/policy/defense-national-security/deepfakes-a-national-security-threat)

by Jamie McIntyre | February 08, 2019 12:00 AM [Print this article](#)

8 février 2019



A new potent weapon of psychological warfare has the potential to overthrow governments, influence elections, and turn the tide of battle, and it can be wielded by a lone hacker anywhere in the cyberverspace.

Welcome to the world of “deepfakes,” hyper-realistic forgeries that defy easy detection and can fool even the most savvy skeptic of fake news.

A quick web search for “deepfakes” will turn up videos in which former President Barack Obama appears to be saying “Killmonger was right” (a reference to the Black Panther villain), a young Harrison Ford replaces actor Alden Ehrenreich in the trailer for “Solo: A Star Wars Story,” or an animated image of gun control activist Emma Gonzalez rips up the Constitution.



Would Trump's national emergency really be an "emergency"?

Watch Full Screen to Skip Ads

All are fakes, but in the case of Gonzalez — one of the students who survived the mass shooting at Marjory Stoneman Douglas High School in Parkland, Fla., last year — the intent was to stoke outrage, and it worked.

"They changed imagery to make it look like they were tearing up the U.S. Constitution, when they were actually tearing up a bullseye from a shooting range," said Peter Singer, co-author of the book *LikeWar*, which explores the weaponization of social media.

"Then that false imagery was driven viral by a mix of NRA, pro-gun rights activists, alt-right trolls, and Russian bots," said Singer, who is also a former Pentagon official. "The result is more people saw and believed the false imagery. It became their 'truth,' and you can see obviously how this could be used against the U.S. military."

This month's Senate Intelligence Committee hearing on worldwide threats cited deepfakes as a growing concern.

"I don't need to remind anyone in the room, when this country's democracy was attacked in 2016, it wasn't with a bomb or a missile or a plane. It was with social media accounts that any 13-year-old can establish for free," said committee Chairman Sen. Richard Burr, R-N.C.

For years, experts have been warning of the threat of cyberwarfare, in which hostile powers hack into the utility grid or the banking system to wreak havoc with the basic services Americans rely on in their daily lives.

But deepfakes represent a different and in some ways more insidious form of hacking, an attack on our brains, using our emotional biases to change the way we think and what we believe in order to further a political or military objective.

"Over the last roughly 15 years, we started to come to grips with the idea of cyberwar, the hacking of networks," said Singer. "Now we have its twin, 'like war,' the hacking of people on the networks by driving ideas viral through a mix of likes, shares, and lies."

Deepfake technology often uses artificial intelligence to do things like transfer one person's facial expressions and lip movements to another person's face.

"It's getting better and better, where you can have a politician making a speech, being at a site, and totally change the reality, the words coming out of their mouths," said Sen. Angus King, I-Maine, on CNN after the Senate hearing.

"As a politician, this is terrifying that a video could surface showing you doing something that isn't you. But then you're on the defensive saying, 'Oh, no, I didn't kick that dog walking down Fifth Avenue.'"

Not only can deepfakes fool people into believing false narratives, they can also fool people into disbelieving the truth.

"Donald Trump has already changed the way he talks about the 'Access Hollywood' sex assault tape, where for two years he admitted it was him and said, 'Yeah, well, that was locker room talk,' and all that. He's now changed his story and started to say, 'Well, it was faked,'" said Singer.

We are entering what Burr described as a new age of “weaponized disinformation” occurring in the context of a world producing more data than mankind has ever seen.

The technology is becoming so cheap and accessible that the confusion about what’s real is only going to get worse.

“The barrier to entry for deep fakes technology is so low now, lots of entities short of nation-state actors are going to be able to produce this material and, again, destabilize not just American public trust but markets very rapidly,” said Sen. Ben Sasse, R-Neb.

As deepfakes become more sophisticated, it will take new algorithms developed by artificial technology to detect the tiny anomalies that separate a real video or photo from a fake.

But King believes that, ultimately, every American will need to develop a finely tuned personal BS-detector.

“The best defense is for people to be skeptical, to dig in and find out the facts.”