**Deep fakes and Infocalypse – The things you need to understand urgently**

There’s a YouTube video of President Obama sitting on a mahogany chair in the Oval Office. He’s staring straight into the camera. His proclamation is solemn. “How we move forward in the Age of Information is going to be the difference between whether we survive or become some fucked-up dystopia.” Except that Obama never actually said that. So what’s going on? Well, this video is a shockingly sophisticated deepfake. Its creators used artificial intelligence to manipulate reality to produce an entirely believable – and completely unreal – new world. Sadly, the warning that fake Obama is delivering may be too little, too late. We are already living in what the author calls the “Infocalypse,” an ecosystem of “dangerous and untrustworthy information.” Deepfakes will only exacerbate the problem. It is essential that we protect ourselves against the perils that deepfakes and the Infocalypse pose – before it’s too late.

In the nineteenth century, humans invented photography. For the first time, we could capture a true, seemingly incontrovertible slice of reality. But very soon, it became clear that “reality” could be not only captured, but also manipulated. At first, altering photos was a painstaking process. Over time, though, it became simpler. Now, anyone can do it – just download a free app. As a result, we’ve become used to the idea that photos can be altered and know to look out for any retouching or editing. But aren’t audio and video different? Surely they can’t be convincingly faked, right? In fact, new developments in artificial intelligence confirm quite the opposite.

The key message here is: Photo, video, and audio manipulation have become easy thanks to AI.

AI - or artificial intelligence - is software that processes information through deep learning. It enables AI to make decisions autonomously, based on what it’s “learned” after crunching large amounts of data. The term “deepfake” is derived from this “deep learning,” plus – for obvious reasons – the word “fake.” The first deepfakes showed how AI can swap a person’s face into an existing video. They were posted on the website Reddit by an anonymous user. Before long, they were attracting some worrying attention. In late 2017, a journalist named Samantha Cole published an article called “AI-Assisted Fake Porn is Here, and We’re All Fucked.” Her story warned of a Reddit forum full of deepfake porn. Its founder used AI to swap the faces of Hollywood celebrities onto the bodies of porn stars. Deepfake porn is non-consensual, deeply embarrassing, and demeaning. And it doesn’t matter how rich you are – there’s nothing you can do to wipe it off the internet. Even Scarlett Johansson, the highest-paid actress in Hollywood, couldn’t protect her own name from it. The fake porn forum on Reddit was eventually taken down. But its creator shared the code that he’d used to make the deepfakes. Now, there’s a whole suite of free tools and software out there, open to anyone who wants to produce their own deepfakes. Sounds horrifying, doesn’t it? But this is all just the tip of the iceberg. Deepfake technology is continuing to improve. Soon, it may become literally impossible to tell when an image, video, or audio clip is fake. This technology is already leading us down a dark path of mis- and disinformation.

People tend to use the terms “misinformation” and “disinformation” interchangeably. But there is an important difference. Misinformation is something that’s simply wrong, whereas disinformation is purposely intended to mislead people. Various countries engage in disinformation campaigns. But the undisputed master of this type of warfare is Russia. One of the most damaging Soviet disinformation campaigns occurred in the 1980s, at the height of the AIDS epidemic. It was known as “Operation Infektion,” and it started with an article published in an obscure, Soviet-sponsored Indian newspaper called the Patriot. The article accused the US military of releasing the AIDS virus as a bioweapon. The Americans, the Patriot alleged, wanted to kill Black and gay men.

The key message here is: Russia is the master of Deepfakines and the I format infocalypse on warfare.

There was a tiny grain of truth in the Russians’ disinformation – the US did formerly have a biological weapons program. But it was already in decline during the 1960s, and by the 1970s, the Pentagon was focused more on defending against bioweapons than on creating them. That truth didn’t stop the AIDS claim from going viral. After becoming particularly widespread in Asia and Africa, it tore through newspapers all over the world, carried across 80 different countries by the press. The story tarnished America’s global reputation, but it also divided the country from within. The Soviets attempted to exploit racial tensions, so they specifically targeted the African American community. Given US history, many people found it easy to believe that their government really did want to murder them. The next major Kremlin disinformation campaign came in 2016. Its purpose was to divide the country and turn voters against Hillary Clinton. Its code name? “Project Lakhta.” The operation involved Russians posing as Americans on social media. These fake US citizens created communities based around political identities. The communities were carefully managed. They served a purpose – to polarize Americans and make them helpless against Russia’s attacking strategy. All signs say this approach worked. Russian interference in American politics is now a partisan issue, with one side overly paranoid about the threat, and the other denying that it even exists. Eventually, deepfakes could make the Russian tactics even more potent, divisive, and dangerous. It took the Soviet Union years to promote “Operation Infektion” in newspapers. But, in the digital age, deepfakes can spread highly believable disinformation in no time at all.

Democracies around the world are experiencing a crisis of trust. A 2018 global survey revealed shocking figures: 64 percent of people who lived in democracies felt their government “rarely” or “never” acted in the interest of the public. But there’s another surprise from the same study. In non-democratic countries, that number was much lower – only 41 percent. This crisis of trust has a figurehead: US President Donald Trump. The key message here is: The Infocalypse is threatening Western democracies, most notably that of the US. Trump lies continuously. That’s an objective fact, not a partisan statement. According to a database set up by the Washington Post, Trump made over 18,000 false and misleading claims in just three years – from January 2017 to January 2020. That’s an average of 15 lies a day But Trump doesn’t only contaminate the public discourse with lies. He goes a step further. The President dilutes the whole idea of truth. He’s a master of the so-called “liar’s dividend.” This is a tactic where somebody dismisses anything they don’t like as “fake,” even if it’s true. Just think about how Trump brushes off all criticism as “fake news.” But what does Trump have to do with deepfakes? Well, as this technology grows more prominent, the “liar’s dividend” will become available to everyone. People are circulating a video that makes you look bad? Well, it must be fake. If you doubt that Trump – the American President – will use deepfakes to advance his agenda, think twice. He’s already gleefully exploited cheapfakes, which are miscontextualized or crudely edited images, audio clips, or videos. In 2018, for instance, the White House retweeted a doctored video originally circulated by the far-right website InfoWars. The video made it seem as if CNN White House correspondent Jim Acosta had physically assaulted a White House intern. The reality was far more benign – and the Presidential press office knew it. But Acosta was still stripped of his White House access, with that cheapfake as justification. There’s no doubt that Trump is making the United States a more divided and dangerous country. He normalizes polarization, distrust, and deceit. It seems the US is heading Deepfakfoes and the I r a scary infocalypse tipping point.

The Infocalypse is a problem for the whole world – not just the West. If mis- and disinformation are harmful for democracies, think about what they could do to countries where freedom of speech is limited, and the rule of law is nonexistent. In 2019, the human rights organization Witness asked journalists and activists from Brazil, South Africa, and Malaysia how they felt about the threat of deepfakes. Their answers were strikingly similar; all agreed that their own governments were far more dangerous than foreign states. The key message here is: The Infocalypse has deadly consequences in countries with less robust democracies. In India, deepfakes have already been used as a tool against political opposition. Take the case of Rana Ayyub, an investigative journalist and fierce critic of India’s ruling party, BJP.

In 2018, a series of fake tweets were posted online. They all appeared to come from Rana and said things like “I hate India,” “I hate Indians,” and “I love Pakistan” – India’s longtime political adversary. Rana quickly assured her followers that the tweets were fake. But things were about to get much worse. The day after those fakes appeared on Twitter, a fake porn video featuring Rana began circulating online, too. Shockingly, it was even shared by the ruling party’s social media fan page. Rana’s phone blew up with lurid, demeaning private messages. But attackers didn’t stop there. Rana was doxxed – her personal phone number was published online. And people who shared it illustrated their messages with the deepfake porn. Rana received hundreds of death and rape threats. It’s still unclear who released that deepfake video of Rana. But it worked. Rana stopped writing; she had been silenced. In Myanmar, mis- and disinformation have actually killed people. In 2014, an ultranationalistic Buddhist monk spread a lie that the Muslim owner of a tea shop in a town called Mandalay had raped a Buddhist employee. In response, enraged mobs stormed Mandalay, destroying cars and ransacking shops. Extremists used Facebook to amplify their message of hate and promote threats against the country’s Muslim population. Eventually, the animosity reached a boiling point. In 2015, Myanmar’s Rakhine State began a large-scale campaign of ethnic cleansing against the Muslim Rohingya people. By the time Facebook finally began to ban online extremists, 25,000 Rohingya had been murdered – and a further 700,000 had fled the country .

The COVID-19 pandemic has sent shockwaves across the world. It has taken countless lives, devastated economies, and dramatically transformed our day-to-day routines. But the disease hasn’t just affected people. It has also hit our information ecosystem. One country that’s been exploiting the pandemic to spread disinformation is – you guessed it – Russia. Much like it did with AIDS and “Operation Infektion,” Russia has also promoted a conspiracy about the novel coronavirus. The claim is that COVID-19 was created by the US government as a bioweapon against China. And, to muddle things up even further, Russia has also been saying that the virus is actually a Chinese bioweapon. Yes, these narratives are the exact opposites of each other. But Moscow is using them on purpose to exploit the mounting political tensions between the US and China.

The key message here is: State actors have been spreading disinformation about the COVID-19 pandemic. Unfortunately, Russia is not at all the only nation exploiting the COVID-19 pandemic. China, too, has been adopting Russian-style disinformation tactics. At the beginning of the pandemic, China censored any discussion of the disease. Doctors, whistleblowers, and even ordinary citizens were silenced. The Chinese Communist Party also censored outbreak-related keywords on social media. Once the pandemic reached other countries, China focused on damage control. Beijing’s purpose was to improve its image abroad. Triumphant but wildly exaggerated reports described how well the country was handling the crisis. The government also tried to deny that the virus had originated in China. Meanwhile, in America, Trump was spreading disinformation about the pandemic in his own way. In February 2020, around the beginning of the pandemic, Trump downplayed the risk of the virus. He accused Democrats of politicizing the disease. This was, he said, his opponents’ “new hoax” – an attempt to smear his name. But by mid-March, the number of coronavirus cases in the US had reached 10,000, and the economy was dipping into a recession. On March 17, Trump made a U-turn. He contradicted everything he’d been saying before and boasted, “I felt that this was a pandemic long before it was called a pandemic.” Throughout the crisis, Trump has spread misinformation at his press briefings. Once, he suggested that a disinfectant could be administered by an “injection inside.” In a pandemic, accurate information is essential. Mis- and disinformation can literally cost lives. But what is the truth? When there are so many conflicting narratives out there, it can be very hard to tell.

It’s clear that the Infocalypse presents an imminent danger to societies all around the world. But what can each of us do to fight it? Well, we can start by recognizing just how serious the problem is. You've already taken a first step by reading these blinks. But in order to fight the threats posed by deepfakes and the Infocalypse, we need to go further – much further. We need to find common language and agree on terminology. The good news is, society as a whole is becoming more familiar with the terms “disinformation,” “misinformation,” and “deepfakes.” The key message here is: Fighting the Infocalypse will involve both a reactive and a proactive approach. When deepfakes become commonplace, it will be more important than ever to support credible journalism. And fact checking services will become crucial. In the United States, these include Politifact, Snopes, and AP Fact Check. In Europe, there’s Fullfact, the BBC’s Reality Check, and the Agence France Presse Fact Check. There are also simple, laptop-based tools that can protect you from mis- and disinformation. NewsGuard, for instance, is a browser plug-in that tells you whether a website is trustworthy. So you can already do quite a lot to ensure that the information you consume is true. But simply defending yourself against the Infocalypse is not enough. We must also proactively fight it. Fortunately, some countries have already won battles against cyberattacks and information warfare. Take Estonia, a small, former Soviet state in the Baltics. In 2007, Russia conducted a series of vicious cyberattacks on Estonia’s government, media, and banking infrastructure. Rather than fold in the face of this onslaught, Estonia took a proactive approach. It first launched an early warning system, which alerted citizens to Russian disinformation attacks. Next, it assembled a group of volunteers – experts in IT and communications. They helped people prepare for cyberattacks, and respond to them. And finally, the country built robust, multilayered cyberdefense systems. As Estonia’s example shows, societies do have a choice. It’s up to us to decide whether or not we want to live in a world where the real and the fake are hopelessly intertwined. If we don’t, then we must work together to fend off the threat of deepfakes and the Infocalpyse.