Artificial Intelligence and Deepfakes- Misuse and Way Forward

drishtiias.com/printpdf/artificial-intelligence-and-deepfakes-misuse-and-way-forward

This article is based on the editorial, The dangers posed by AI-driven 'deepfakes',that appeared in live Mint on 13th June 2019. It talks about Artificial Intelligence and its misuse and suggests a way forward.

We are stepping into the age of AI where machines and computers might control our very existence. The world of cyber crime has already entered a new era where computers will take much of the decisions on both the sides. Use of AI to **manipulate appearances and voices of people into real-looking footage highlights** the need to question the rise of **Artificial Intelligence and its misuse.**

Artificial intelligence, or AI, involves using computers to perform tasks normally requiring human intelligence, such as taking decisions or recognizing text, speech or visual images.

How can AI become a danger?

- **Deepfakes:** AI-powered algorithms that manipulate appearances and voices of people into real-looking footage.
    As deepfakes are created through AI, they don't require the considerable skill that it would take to create a realistic video otherwise, which implies that just about anyone could create a deepfake to promote their chosen agenda.
- **Cyber crime:** AI can be exploited to mount automated hacking attacks, commit financial frauds, cut through a nation's security framework, can even facilitate terrorism and radicalisation.
- **Invasion of privacy and social grading:** governments can use the data to govern through AI, people's social media habits, introduce policies to police people with the help of Face IDs, like it's done in countries such as China.
- **Existential risk** from artificial intelligence is the hypothesis that substantial progress in artificial intelligence could someday result in human extinction or some other unrecoverable global catastrophe because of its "super intelligent" powers that could

become difficult to control in future.
- **Social manipulation:** Cambridge Analytica and others associated with the firm who used the data from 50 million Facebook users to try to sway the outcome of the 2016 U.S. presidential election and the U.K.'s Brexit referendum, illustrate AI's power for social manipulation.

Several researchers have revealed that the malicious use of AI poses imminent threats to **digital, physical and political security by allowing for large-scale, finely targeted, highly efficient attacks.**

Social Grading through AI: A process through which authorities can use AI to analyze people's behavioral patterns and model hypothetical situations. It can be used for surveillance over the internet.

- AI can be applied for dating, recruiting, advertising, prevention of terrorism and suicides, fraud detection and other tasks.
- Social Credit Score system assigns a certain grade to every citizen. It is based on economic, social and online activity. This score can influence access to transport, credits, employment, permission to leave the country and other public services.

Significance of Artificial Intelligence

From software to smart devices, **Artificial Intelligence is present in our day to day**, in the form of smartphones, cameras, Internet of Things (IoT) devices, voice assistant to biometrics.

Key Terms

- **Internet of Things**
  It is a network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect, collect and exchange data.
- **Virtual Reality (VR)** is the use of computer technology to create a **simulated environment.**
  - Unlike traditional user interfaces, VR places the user inside an experience i.e Instead of viewing a screen in front of them, users are immersed and able to interact with 3D worlds.
  - VR Enables simulation of as many senses as possible, such as vision, hearing, touch, even smell.
- **Augmented Reality** is the use of sensors and algorithms by computer to determine the position and orientation of a camera.

- **AI in conjunction with** Internet of Things (sensors and wearables), robotics, virtual

reality (VR) and augmented reality (AR) is playing a very important role.

- **AI in Healthcare**

  Diagnosis: AI systems helps radiologists in improving their ability to diagnose and track **prostate cancer** and Google researchers used a deep learning neural network (a machine learning technique, which itself is considered a subset of AI) that trained on retinal images to identify **cardiovascular risk factors.**

Machine learning is an application of artificial intelligence (AI) that provides systems the ability to **automatically learn and improve from experience** without being explicitly programmed.

- The process of learning begins with observations or data, such as examples, direct experience, or instruction, in order to look for patterns in data and make better decisions in the future based on the examples that we provide.
- The primary aim is to allow the computers to learn automatically, without human intervention or assistance and adjust actions accordingly.

Nowadays, artificial intelligence is used for many good causes including to help us make better **medical diagnoses,** find new ways to **cure cancer** and make our **cars safer**. Unfortunately, as our AI capabilities expand we will also see it being used for **dangerous or malicious purposes.** Since AI technology is advancing so rapidly, it is vital for us to develop best ways for positive adaptation to AI while **minimizing its destructive potential.**

Way Forward

- **Policy-makers and technical researchers** need to work together now to understand and prepare for its possible misuse.
- Government should incentivise **core and advance research in AI.** Offering incentives for **manufacturers, creating regional innovation clusters for manufacturing automation and robotics** in partnership with universities and start-ups.
- **Machine intelligence** is a critical element of **national security strategy**, hence governments should evaluate models of defense research in collaboration with the private sector and universities that are dealing with AI.

Drishti input:

In the era of fourth industrial revolution, one cannot isolate oneself from the impact of Artificial Intelligence. However, the benefits can be maximized and losses can be minimized by putting necessary infrastructure and policy in place. Comment.