Cybercriminals are weaponizing artificial intelligence against healthcare

Richard Staynings

Healthcare Security Luminary
Chief Security Strategist, Cylera
Faculty, University of Denver

CYLERA

UNIVERSITY OF DENVER

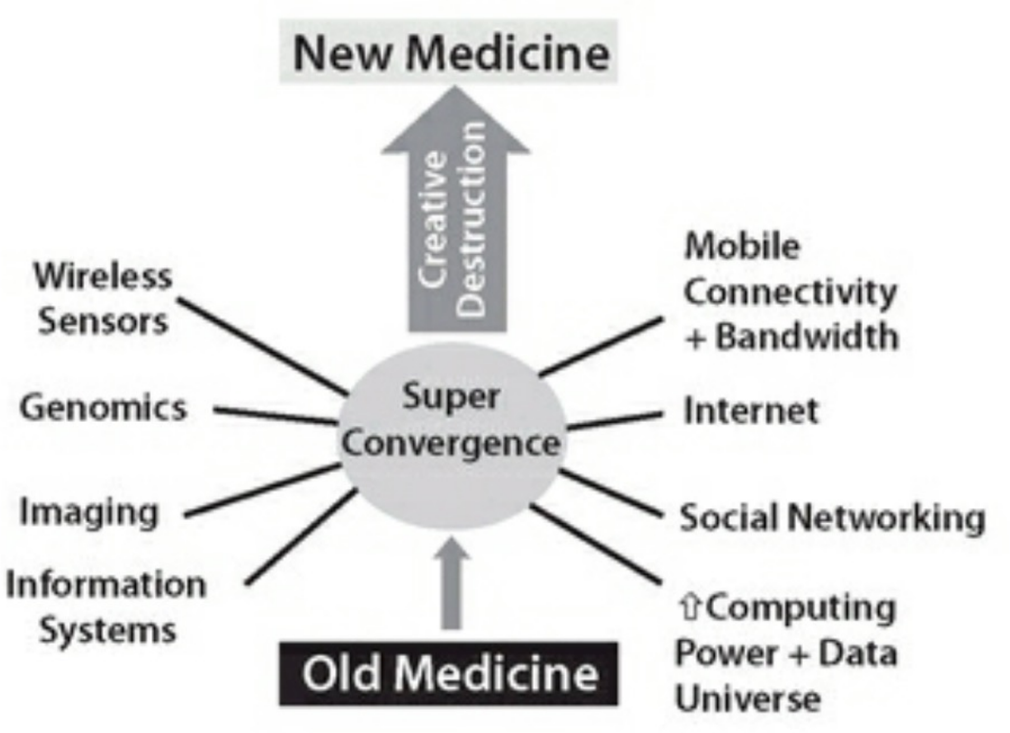
RSNA® 2022

Empowering *Patients and Partners* in Care

Digital Health has turned the industry on its head.

It’s changed the way we work and changed how patients interact with their care teams.

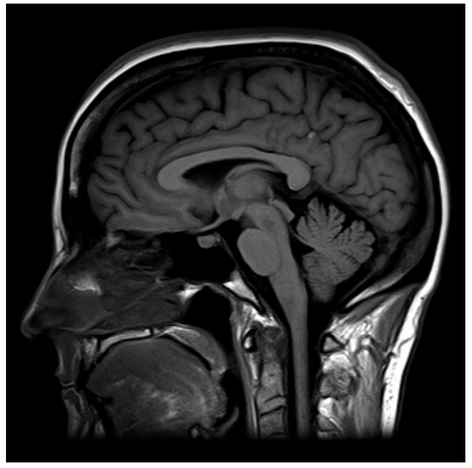
For the first time in history, we can digitize humans!



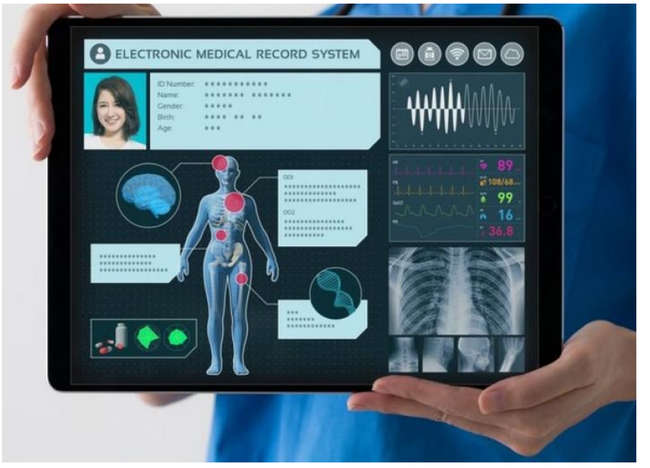
Topol, Creative destruction of Medicine, 2013

Physiology

Biology

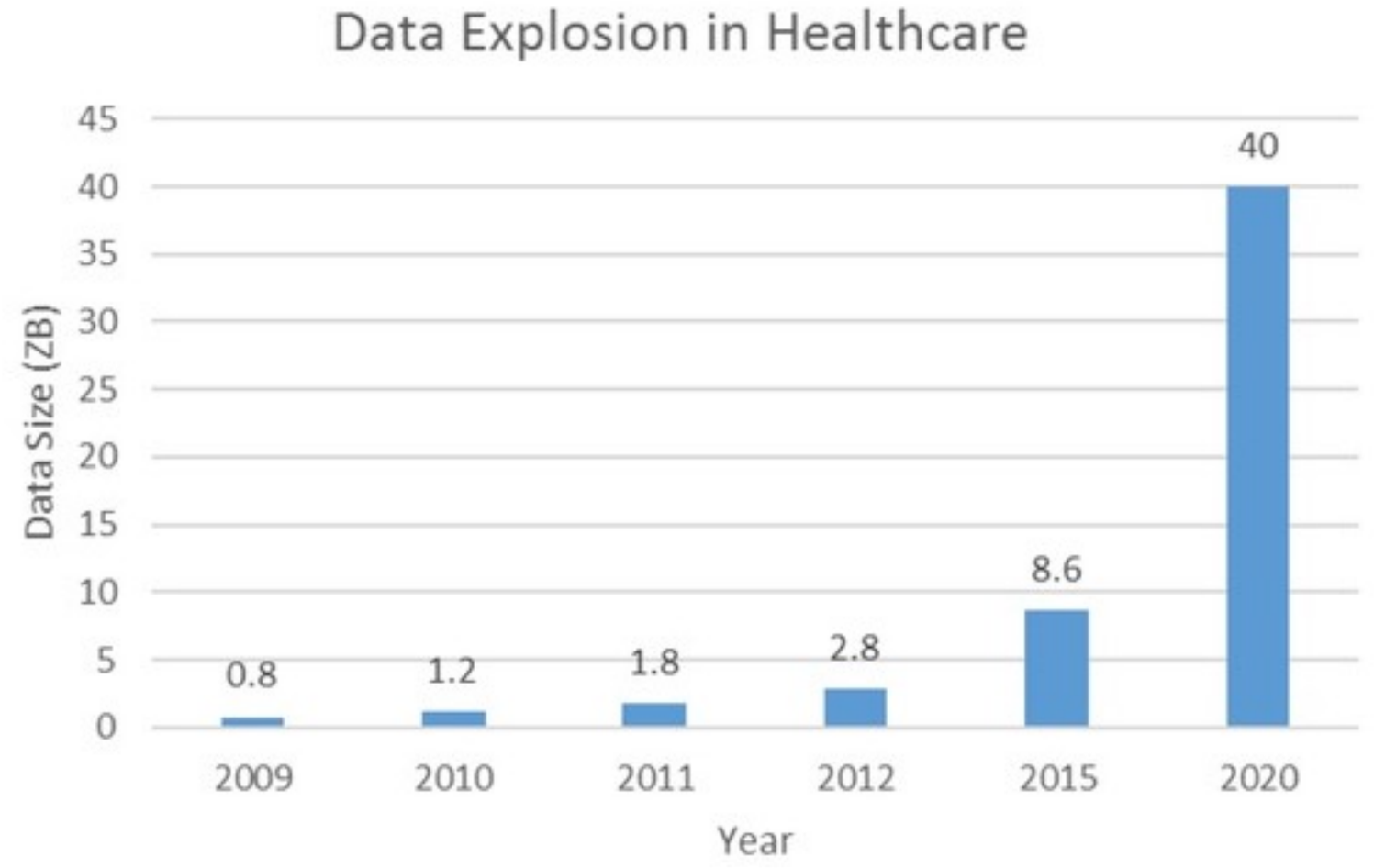


Anatomy



EHR

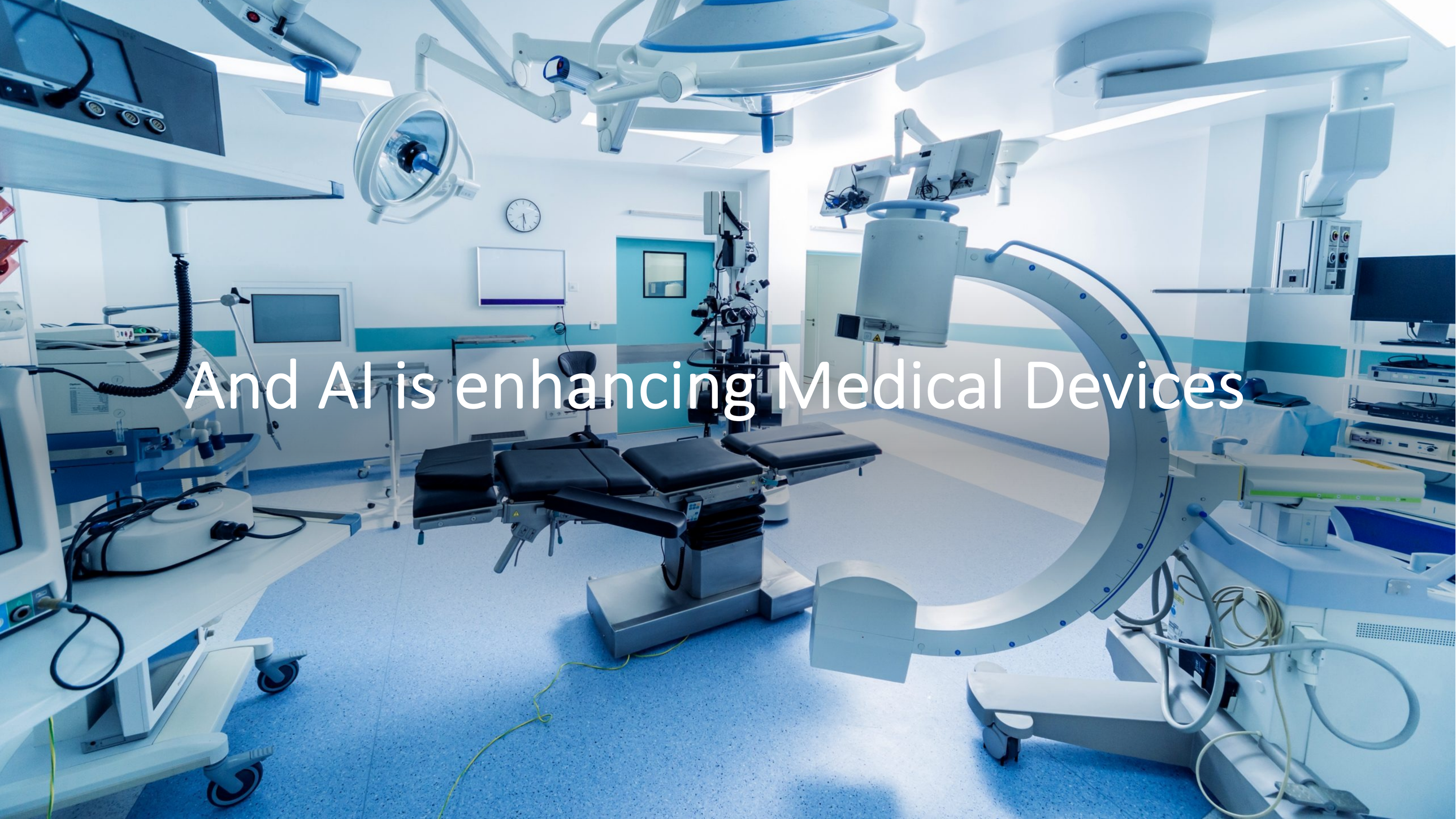
Explosion of medical data



1 ZB = 1 billion TB

Hong, Big Data in Health Care, Data and Information Management 2 (3), Dec 2018

Its also helping to train all forms of Artificial Intelligence

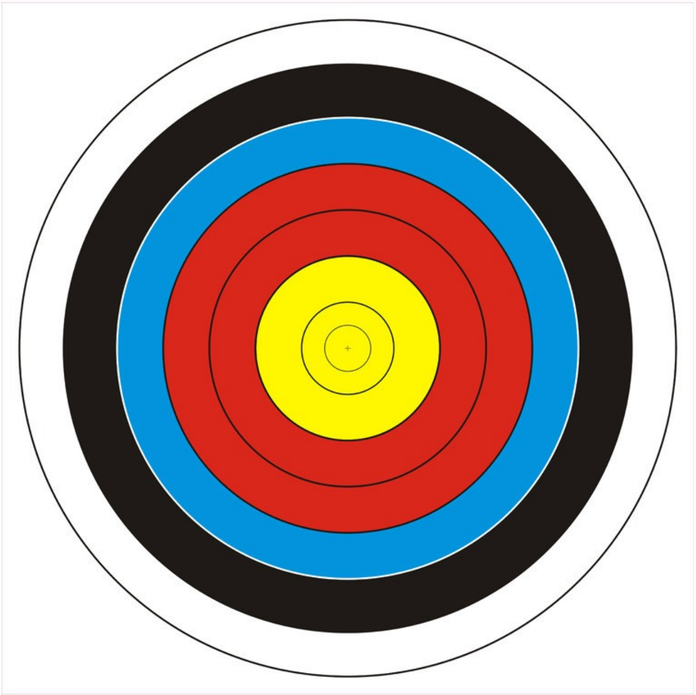

And AI is enhancing Medical Devices

New Technologies Expand the Attack Surface


Making healthcare an easy target for hackers

Healthcare is being targeted by attackers

- Healthcare data breaches hit all-time high in 2021, impacting 45M people (Fierce Healthcare)
- Healthcare providers are typically more desperate to pay ransom to protect PHI and get their systems back up and running (Check Point)
- Healthcare networks typically require the use of older, unsupported software running on medical devices in particular



- UCSF reportedly paid $1.14M to recover their encrypted files in 2021
- UHS, one of the largest healthcare providers, suffered a Ryuk ransomware event, typically precipitated by commodity threats Emotet and Trickbot
- Events are not isolated to North America. India reported the second most ransomware attacks in Q3 2020

Cybercrime cost $6 Trillion USD in 2021

Cybersecurity Ventures Official Annual Cybercrime Report

By 2025 Cybercrime will cost $10.5 Trillion USD

Cybercrime Magazine

The average total cost of a breach in healthcare increased by 9.4% to **$10.1 million** in 2022.

IBM X-Force Cost of a Data Breach Report, 2022

According to HHS' Office for Civil Rights, cumulative healthcare breaches by 2021 have resulted in the loss, theft, exposure, or impermissible disclosure of 314,063,186 healthcare records.

That equates to more than 94.63% of the 2021 population of the United States.

HHS OCR 2021

Between 2 and 3 US hospitals are being attacked by ransomware EVERY DAY

Cylera Labs, 2022

That results in:

- Hospitals forced on divert
- Cancelation of appointments
- Patient safety concerns
- Loss of revenue
- Loss of reputation
- OCR investigation, CAP & fines
- Class Action Lawsuits

2021 ransomware attack cost $112.7m in lost revenue

CommonSpirit

Will likely cost more

Irish Health System Executive attacked

May 2021

Recovery costs for ransomware attack on Ireland's publicly funded healthcare system, is likely to total $600 million, says Paul Reid, HSE's director general.

North Korean WannaCry attack shut down much of the UK NHS in 2017

WannaCry affected at least 81 of the 236 trusts across England - a third of NHS systems

WannaCry Ransomware Costs Britain's NHS Approximately $121M

5 years later the NHS still has a massive elective surgery backlog

The Good the Bad and Ugly

How cybercriminals are using AI to make phishing and other attacks more effective and dangerous

“The emergence of synthetic content such as deep fakes and artificial intelligence will create massive and vexing problems for democracies.

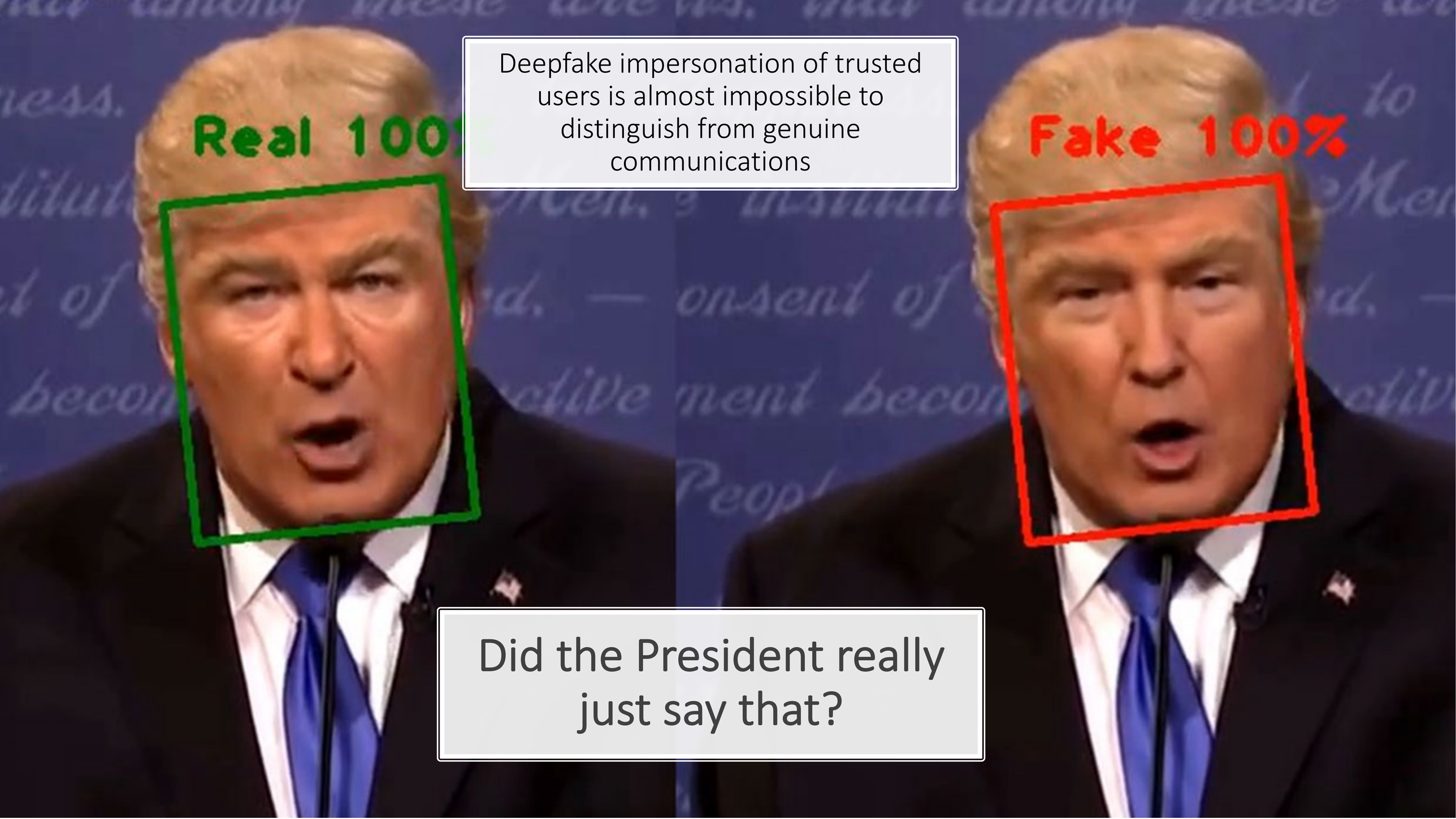
[And] …within two to three years the world will be saturated with synthetic audio and video content that is virtually indistinguishable from reality.”

FBI Assistant Director for Cyber Bryan Vorndran, July 2022

Quoted in Cyberscoop 2022

SECURITY

Get Ready: Deepfakes Are Showing Up in Cyberattacks



Deepfake impersonation of trusted users is almost impossible to distinguish from genuine communications

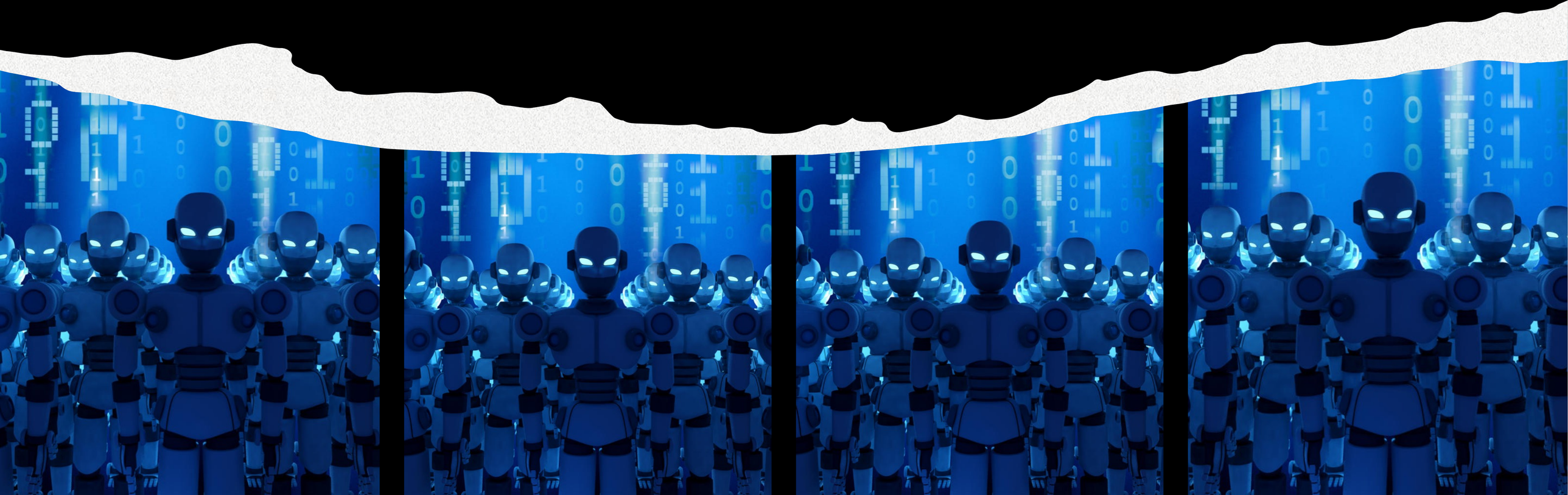
Did the President really just say that?

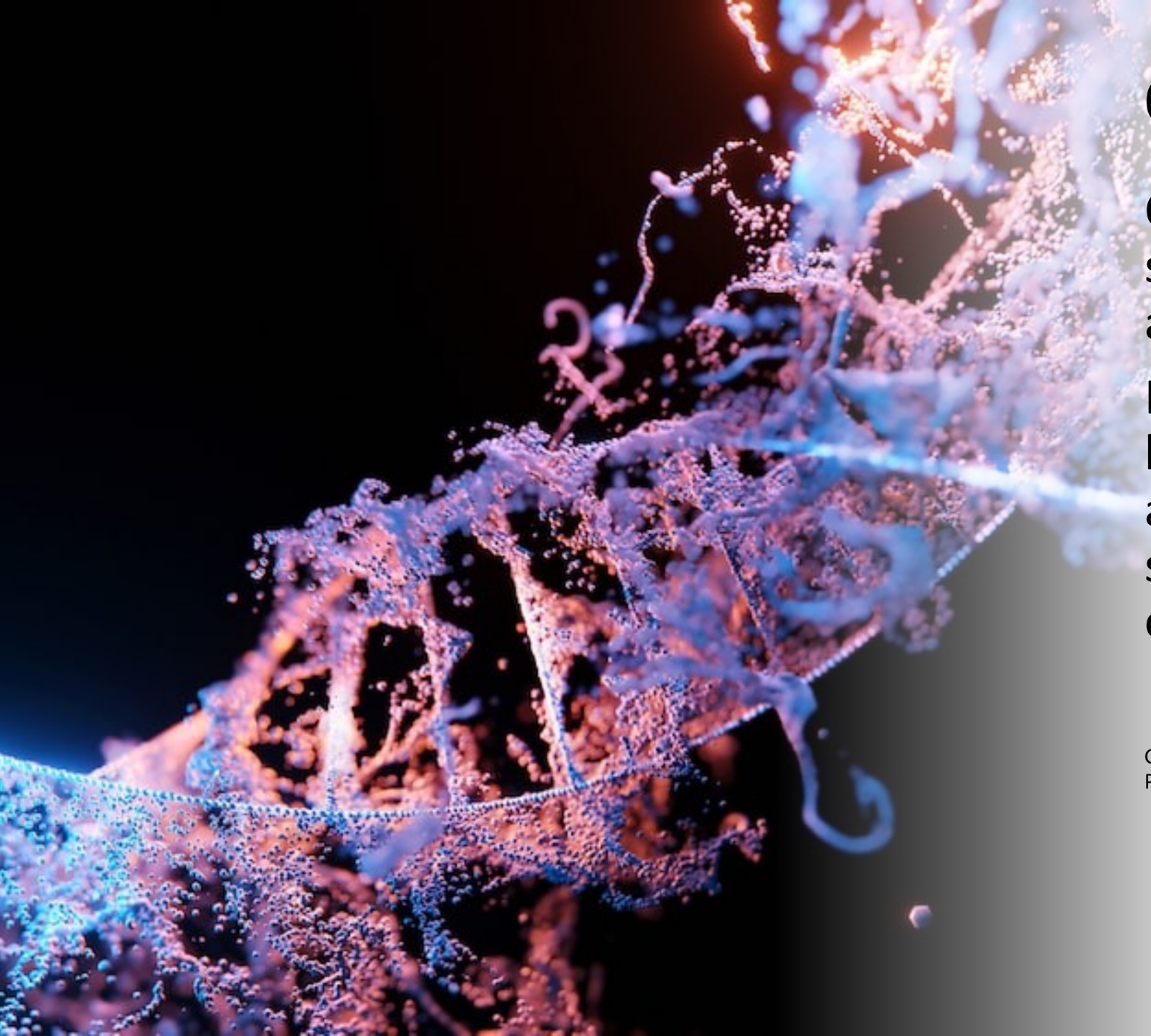
A New Type of Attack

Was that really the CEO on the phone telling me to transfer money to a numbered Cayman Island bank account or a deepfake audio bot?

Offensive AI

Cybercriminals are now supercharging their attacks with AI
to get past our cyber defenses





Offensive AI

Offensive AI is highly sophisticated and malicious attack code

It is able to mutate itself as it learns about its environment, and to expertly compromise systems with minimal chance of detection

Gartner Report: 2021 Market Guide for Security Threat Intelligence Products and Services

Offensive AI is being used by attackers

- Ability to blend into the background – uses APT techniques learn the dominant communication channels blending in with routine activity to disguise itself amid the noise
- Faster attacks with more effective consequences- could lead to exponential growth in number, speed and effectiveness of attacks
- AI’s ability to understand context means AI attacks will be even harder to detect
- Traditional security controls will be impotent against this new threat

Offensive AI already being used

- Emotet Banking Trojan has evolved:
  - to self-propagate and to use a spreader module that contains a password list that it uses to attempt to brute force access to other machines on the same network
  - to generate contextualized email using AI's ability to learn and replicate natural language by analyzing the context of the email thread
  - an AI-powered Emotet trojan could create and insert entirely customized, more believable phishing emails.

World Economic Forum June 2019

Offensive AI – used to undermine data integrity & trust

Massive consequences – life threatening in healthcare

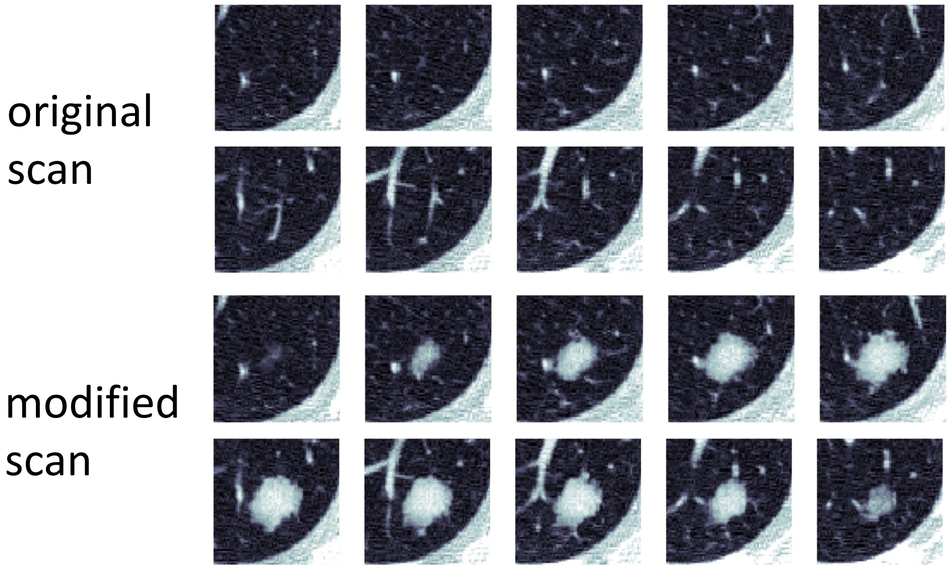
- *Can we trust a medical record?*
- *Can we trust a medical device?*
- *Did a legitimate clinician change a patient's medical record or did AI?*
- *What happens when a Physician makes a diagnosis using compromised data?*
- *Who is liable?*

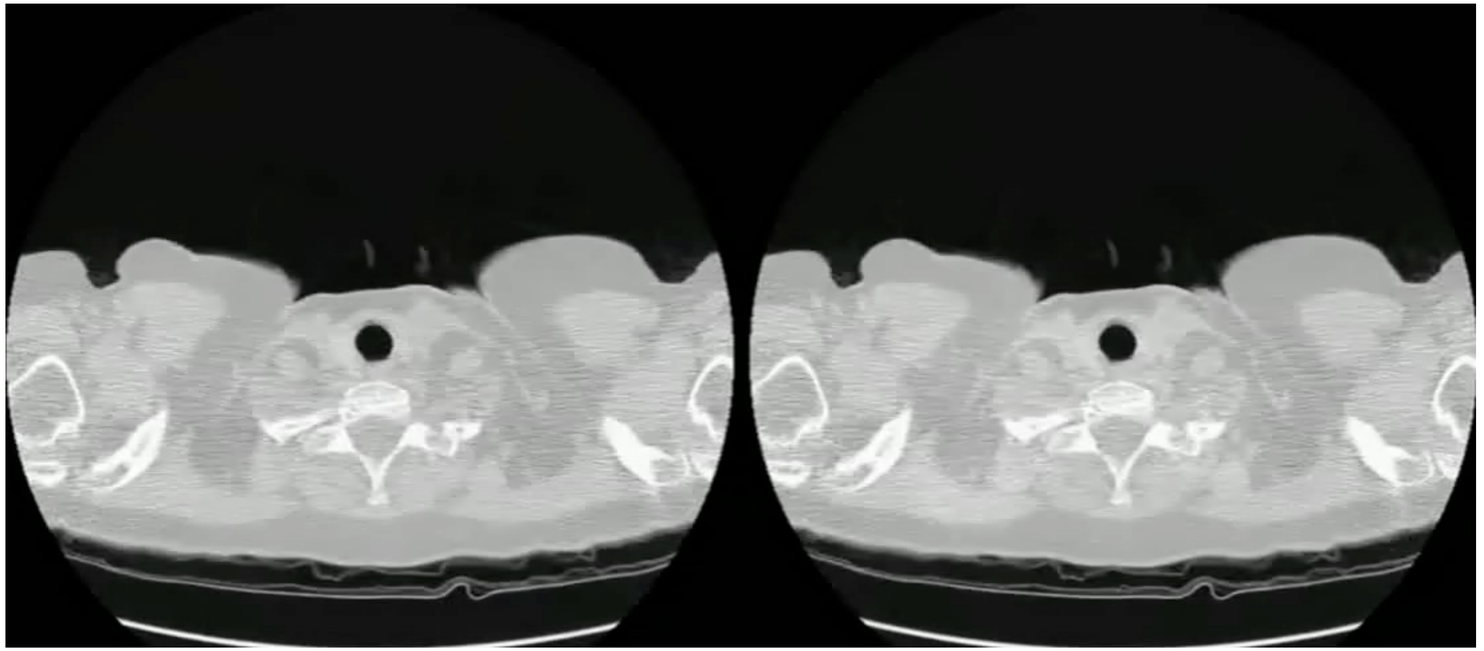
AI based integrity attacks pose a significant patient safety risk

Attacks against Integrity of Medical Data

Hacking medical images

- Intercept images on network between scanner and PACS
- Add or subtract nodules on CT images using deep-learning





Original

Fake nodules

Radiologists fooled by:

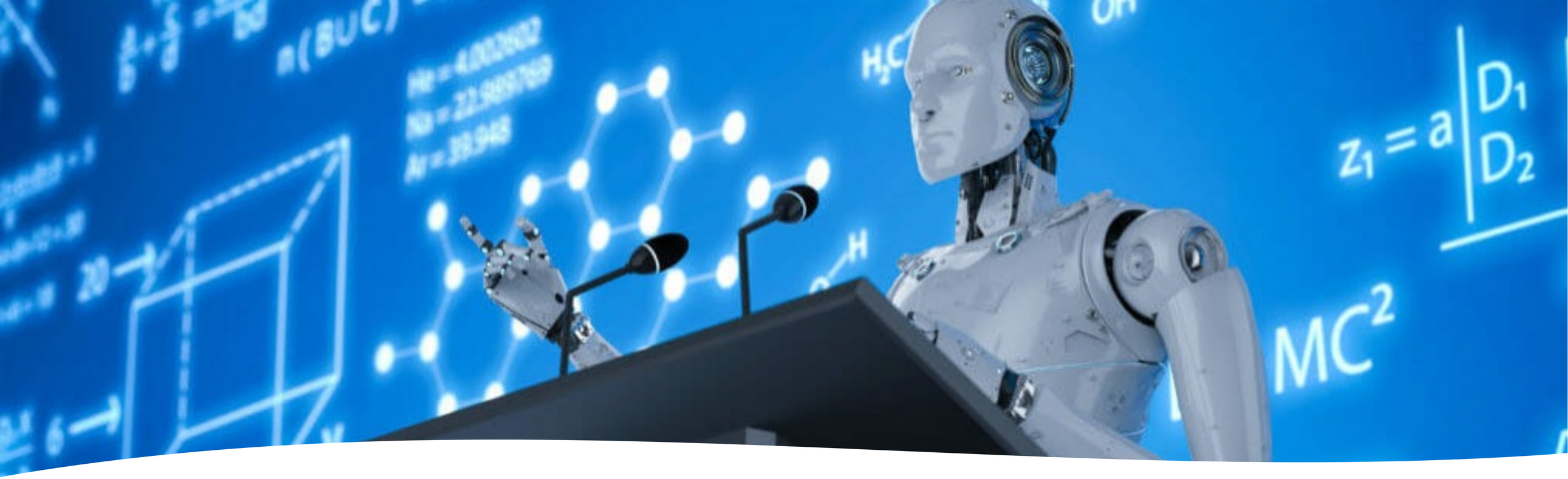
- added fake nodules (99%)
- removed nodules (94%)

Ben-Gurion University of the Negev

Mirsky et al, arXiv:1901.03597v2, Apr 2019

Defensive AI

- Use Fire to fight Fire
- ‘Defensive AI’ will be needed to combat ‘Offensive AI’
- This will require a heavy investment in new tools and capabilities
- According to Forrester’s *Using AI for Evil* report, “mainstream AI-powered hacking is just a matter of time”
- AI-powered attacks will outpace human response teams
- Nano-second responses will be key to winning the battle of the bots to prevent the lateral spread
- But we need to ensure a partnership between humans and AI for success



Thank You

@rstaynings

richardstaynings

Richard Staynings

Chief Security Strategist, Cylera

https://cyberthoughts.org/

https://cylera.com

CYLERA

UNIVERSITY OF DENVER