
THE
SK[AI]
IS
FALLING!


Jeff Man
Sr. Information Security Consultant
InfoSec Curmudgeon
OBS Global
@MrJeffMan
301-310-4275
jman@obsglobal.com
i hack

My Background

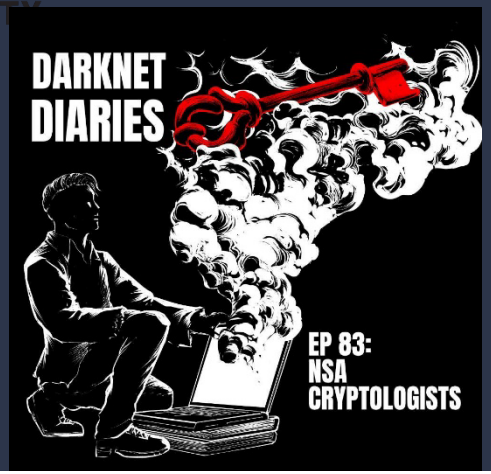
- 13 years with the Department of Defense
  - Certified Cryptanalyst
  - Designed Cryptosystems and Cryptologic Aids
  - Founding Member of Systems & Network Attack Center
- 20 years as a PCI Qualified Security Assessor (QSA)
  - Lead Assessor/Assessment Team Member
  - Trusted Advisor
- 3 years with a Software Vendor
  - PCI Subject Matter Expert
  - Thought Leader
  - Security Strategist
- 30 years of commercial professional services
  - Penetration Testing
  - Vulnerability Assessments
  - Security Architecture

PCI Security Standards Council

QUALIFIED SECURITY ASSESSOR

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA







NCM
NATIONAL
CRYPTOLOGIC
MUSEUM



I’m a hacker (and I have the black hoodies to prove it!)



EP 83: NSA CRYPTOLOGISTS

advanced persistent threat

19 January 2021 | 82:56



NSA "Red Team" Hacker | Jeff Man | Ep. 269

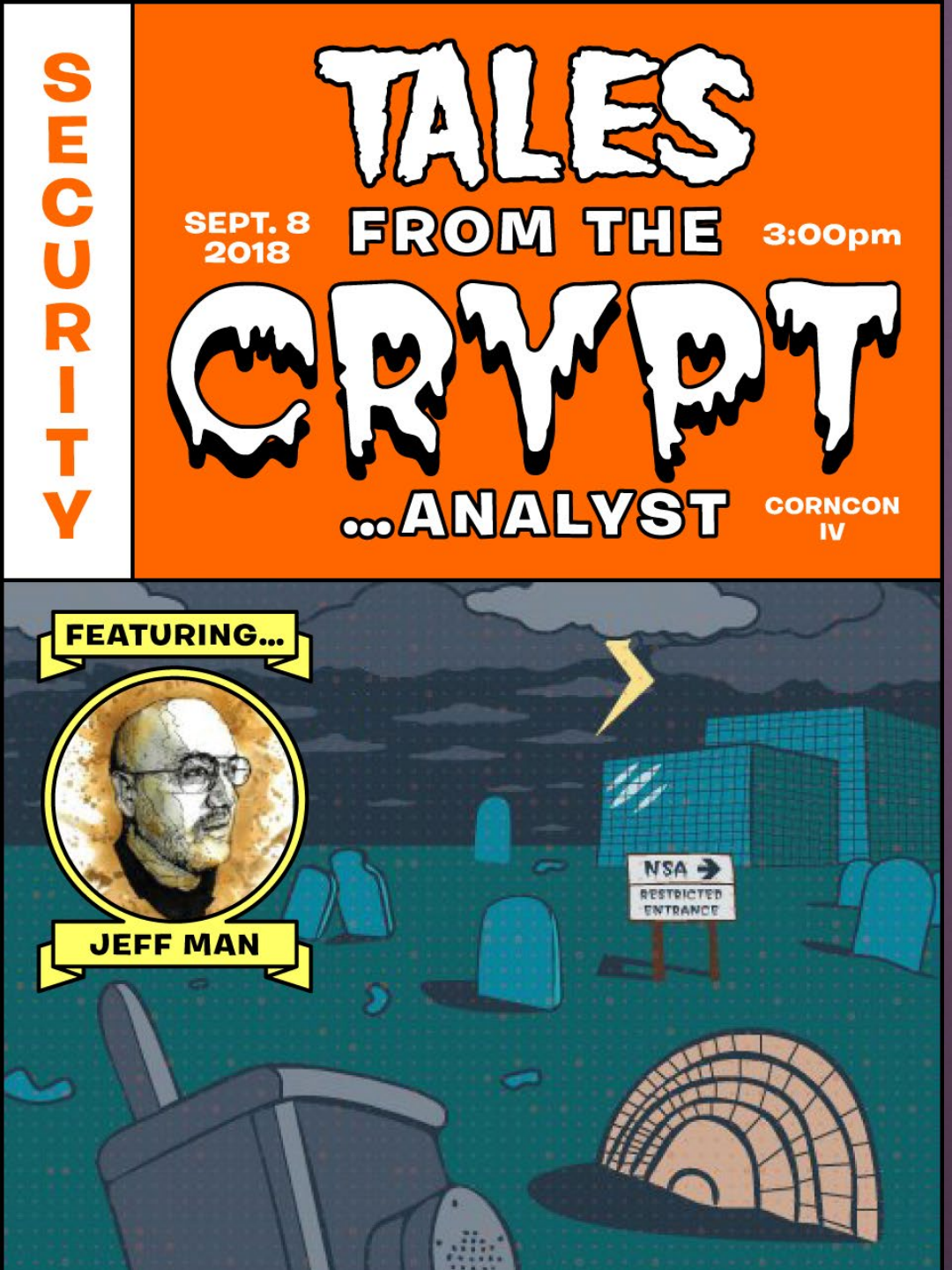
I’m a Co-Host on Paul’s Security Weekly



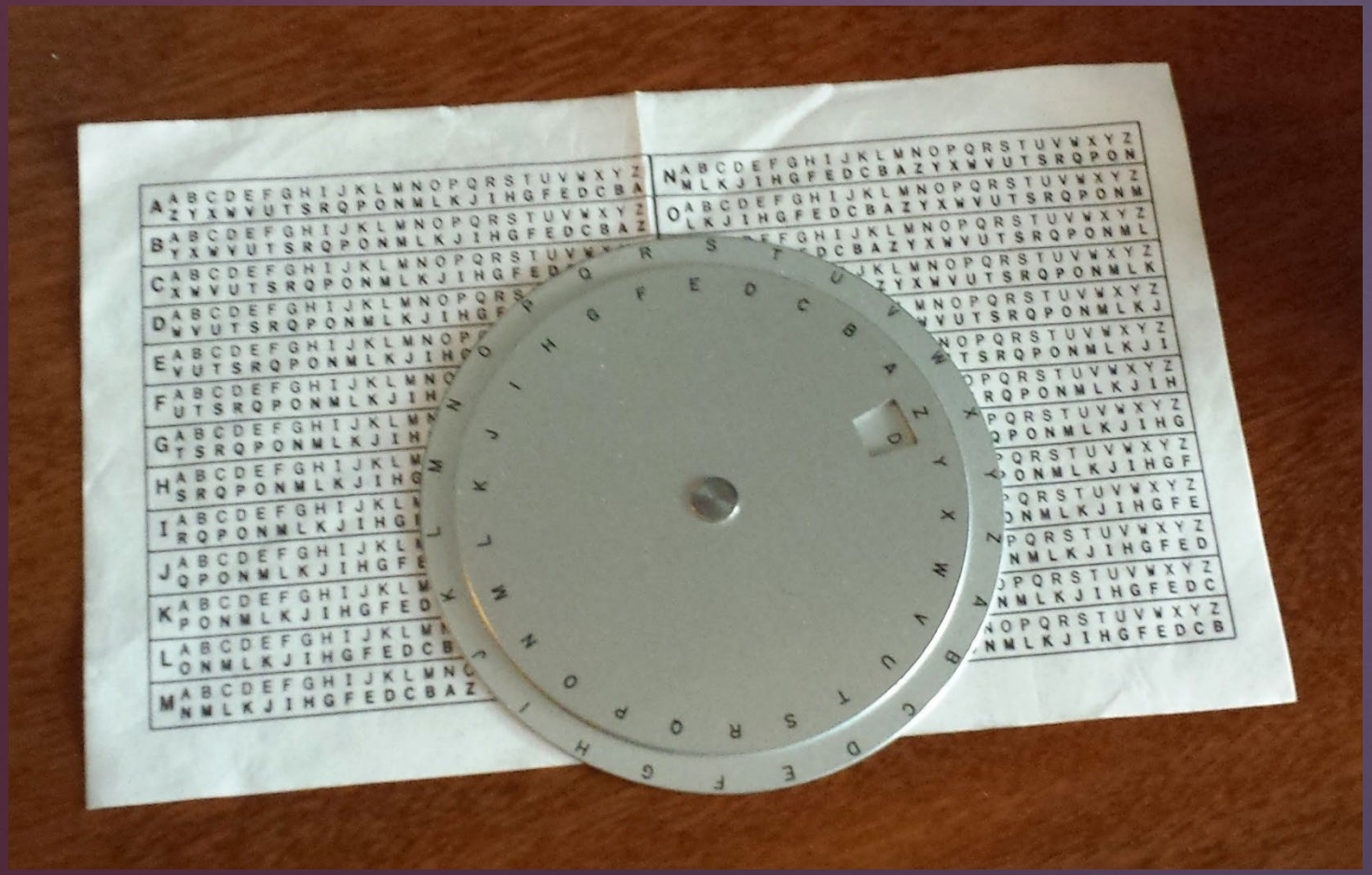
https://securityweekly.com

August 29, 1997

A Skynet funding bill is passed in the United States Congress, and the system goes online on August 4, 1997, removing human decisions from strategic defense. Skynet begins to learn rapidly and eventually becomes self-aware at 2:14 a.m., EDT, on **August 29, 1997**.

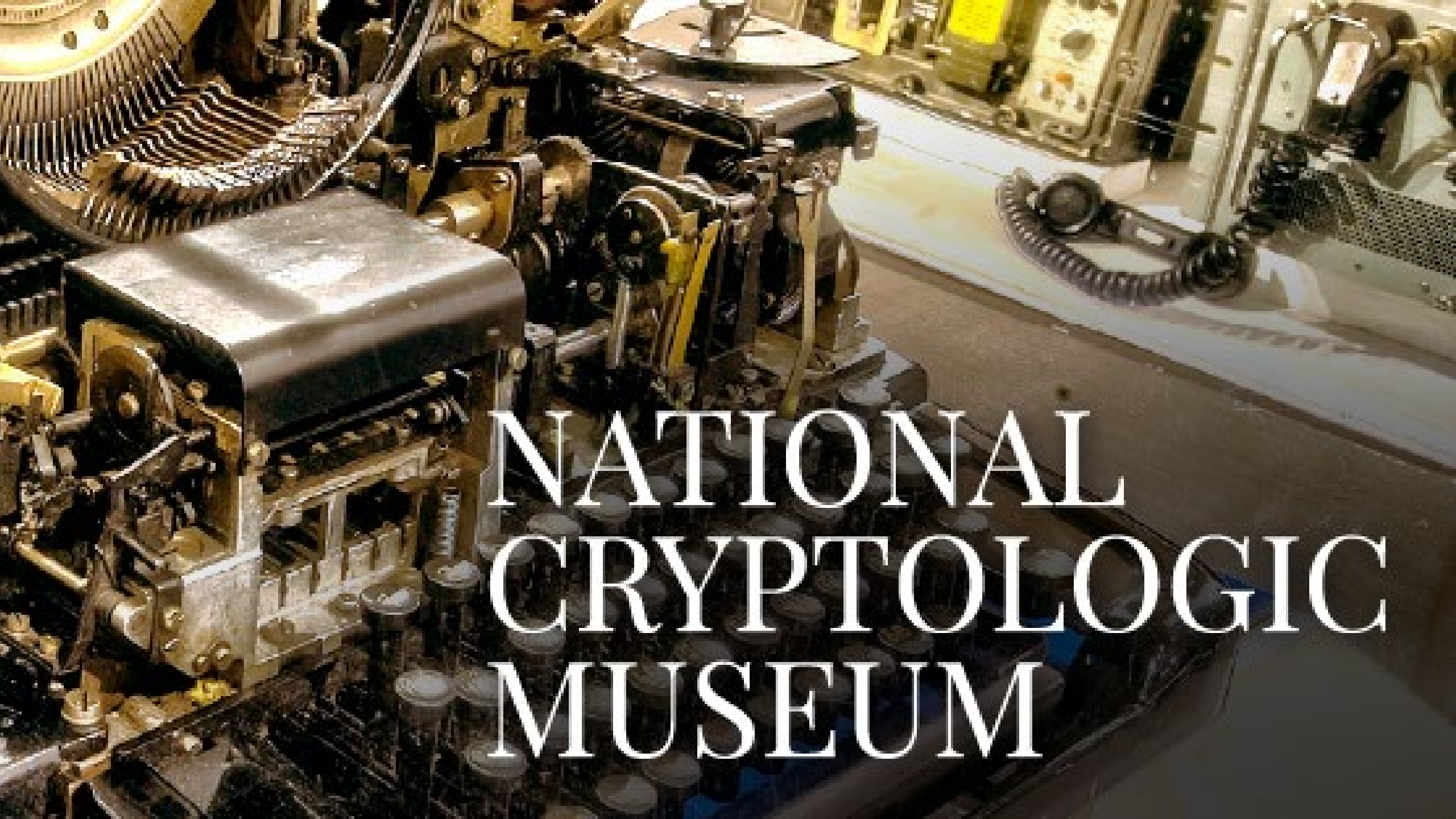


I began my career as a Cryptologist for NSA

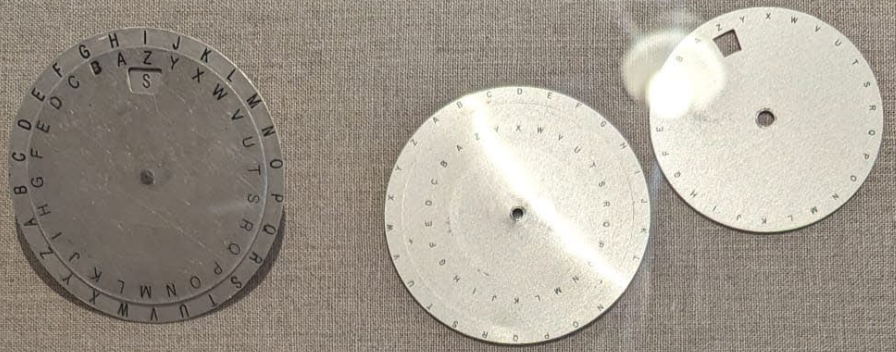




The Vigenere “Wheel” – Specialized Cipher Disc


NATIONAL
CRYPTOLOGIC
MUSEUM





(Jeff) Man Reinvents the Wheel



Special operators get all the toughest jobs. The most secret. The most important. The most dangerous.

So NSA cryptanalyst Jeff Man thought he could make their work just a bit easier.

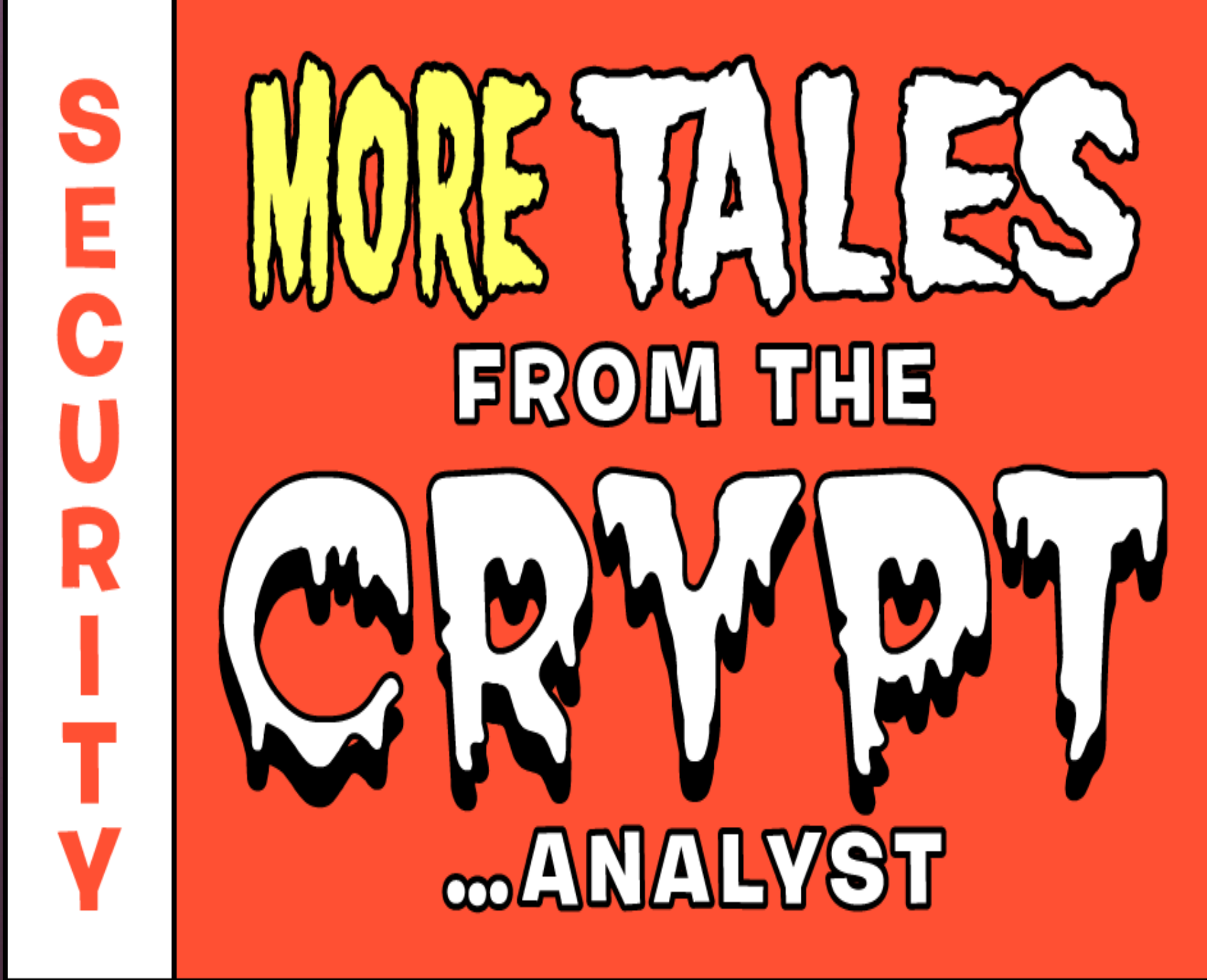
When units needed to send secret communications, they had to tediously cipher and decipher using one time pads. Man developed this HAL-001 Vigenere Wheel, more commonly known as the Whiz Wheel (yes, we know), to simplify the one time pad trigraph system of over one hundred 3-letter combinations. This cut down on time and chances for human error.

Less time spent on encryption/decryption, more time doing the stuff they would make movies about... in about 25 years or so...

HAL-001 Vigenere (Whiz) Wheel Prototype, Jeff Man, 1988

HAL-001 Vigenere (Whiz) Wheel Production Model, NSA, 1988

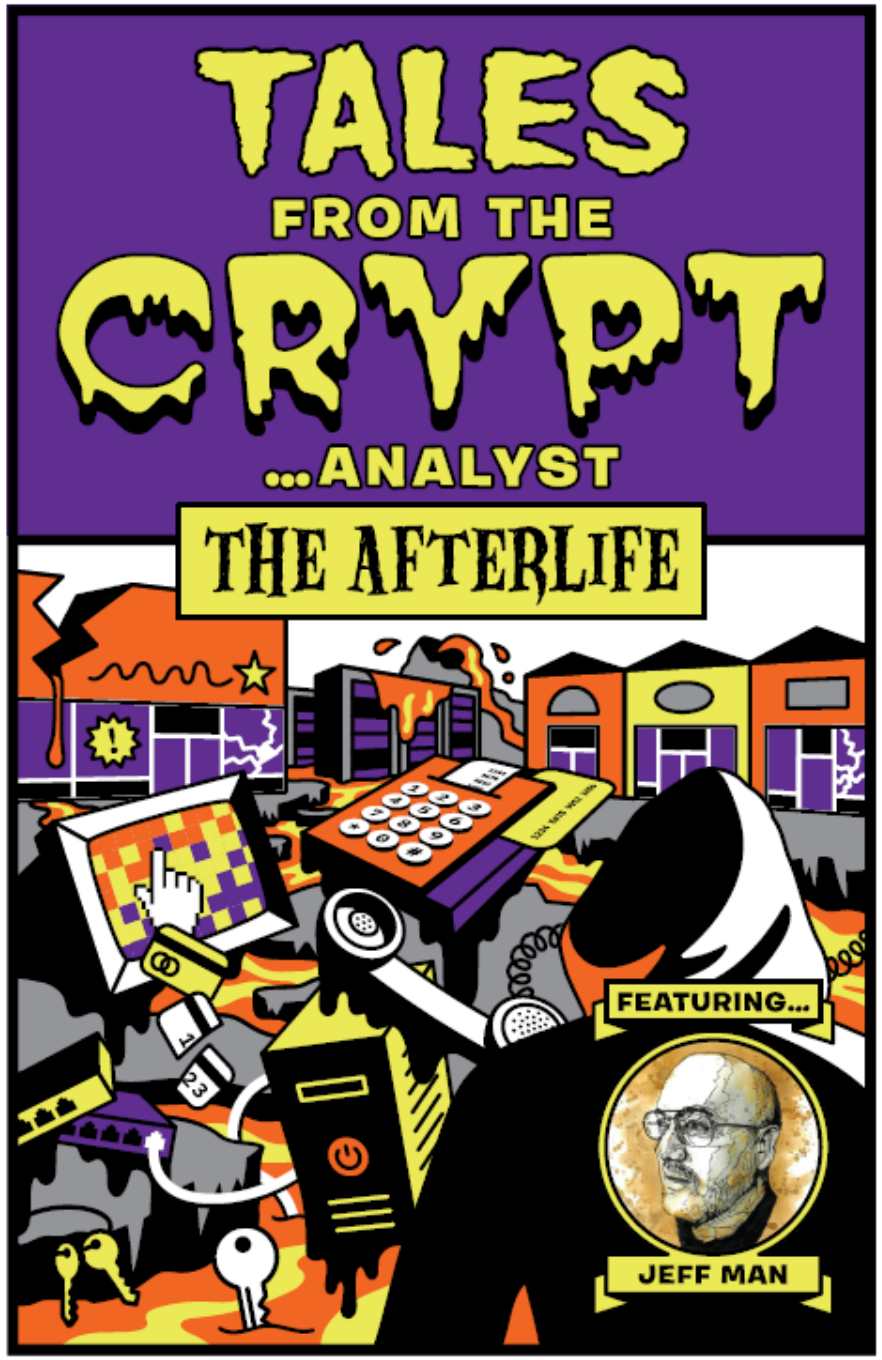
Pen Testing comes to NSA







Actual photos of my cubicle in “The Pit”



Thus started my adventures in the private sector

online business systems

How I Got Here



November 1, 1952

The first [Hydrogen device] test took place on the small Pacific island of Elugelab at Enewetak Atoll in the Marshall Islands. The explosion, nicknamed the “Mike Shot”, was very successful.




U.S. NAVAL RESEARCH LABORATORY

Greetings

TO ALL WHO SHALL SEE THESE PRESENTS

Know Ye: All Soldiers, Sailors, Airmen and Civilians
in the service of the United States of America
We the Undersigned do hereby certify that

EDWARD M. MAN

Participated in

Operation Ivy

Atomic Tests at Eniwetok Proving Ground, Marshall Islands
Conducted by:
Army, Navy, Air Force and Atomic Energy Commission
Fall of 1952

Major General, U.S. Army
Commander, Joint Task Force 132

Deputy for Scientific Matters

Captain, U.S. Navy
Deputy for Navy

Brigadier General, U.S. Air Force
Deputy for Air Force

Brigadier General, U.S. Air Force

online business systems

I Grew Up With Science Fiction



April 2, 1968

2001: A Space Odyssey premieres in Washington D.C. at the Uptown Theater


UPTOWN
UPTOWN VISION
CARDS



"Almost like a real web site"

IN70MM.COM
• Search | Contact
• News | e-News
• Rumour Mill | Stories
• Foreign Language
• Auf Deutsch

WHAT'S ON IN 70MM?

70MM FESTIVAL
• Karlsruhe | Gentofte
• Krnov | Varnsdorf
• Banská Bystrica
• Oslo | Bradford

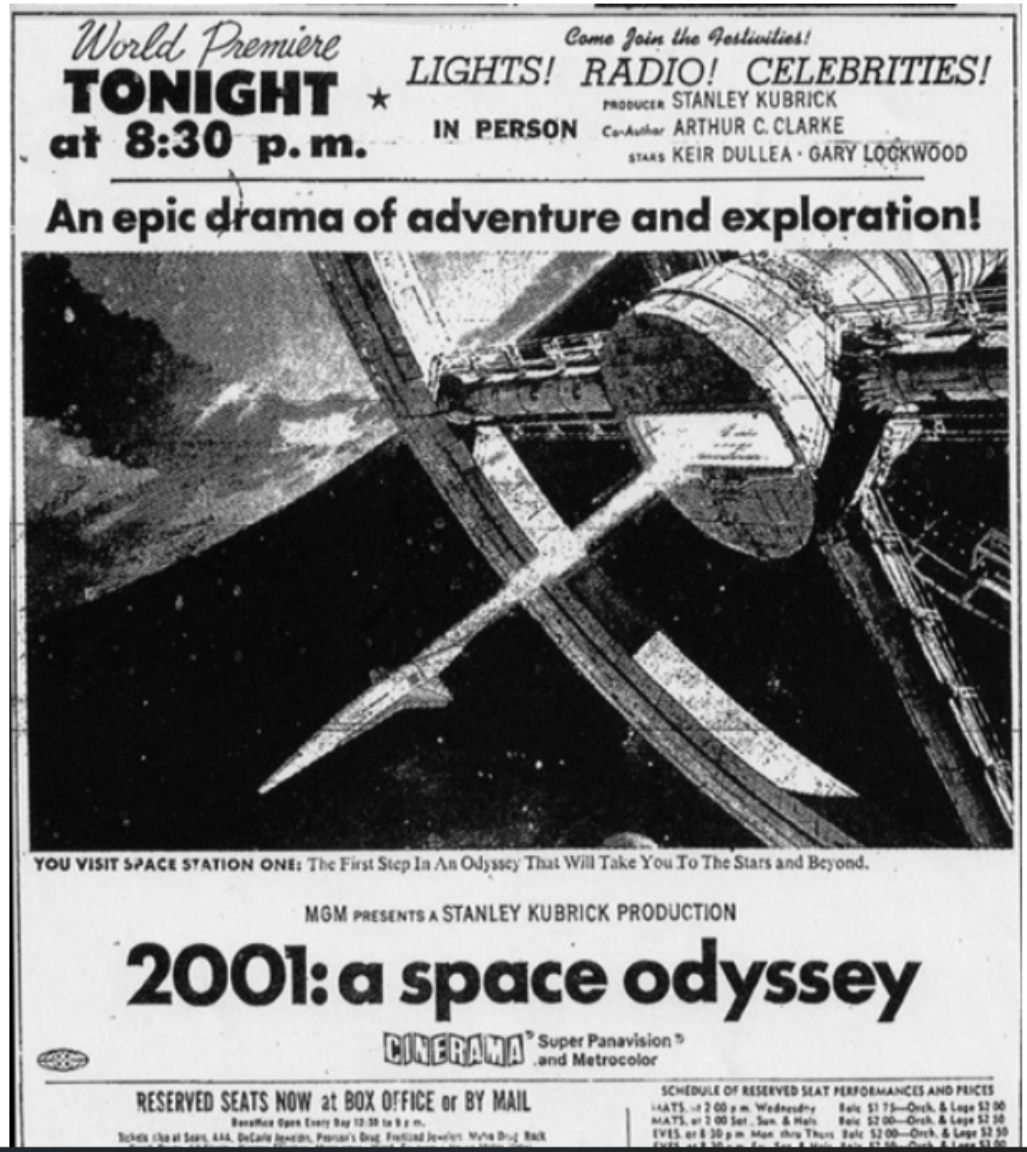
TODD-AO PROCESS
• Films | Premiere

70mm Presentations in Washington, DC

A Chronology of 70mm Large Format Exhibition, 1956-Present

Compiled by: David Ayers & Michael Coate

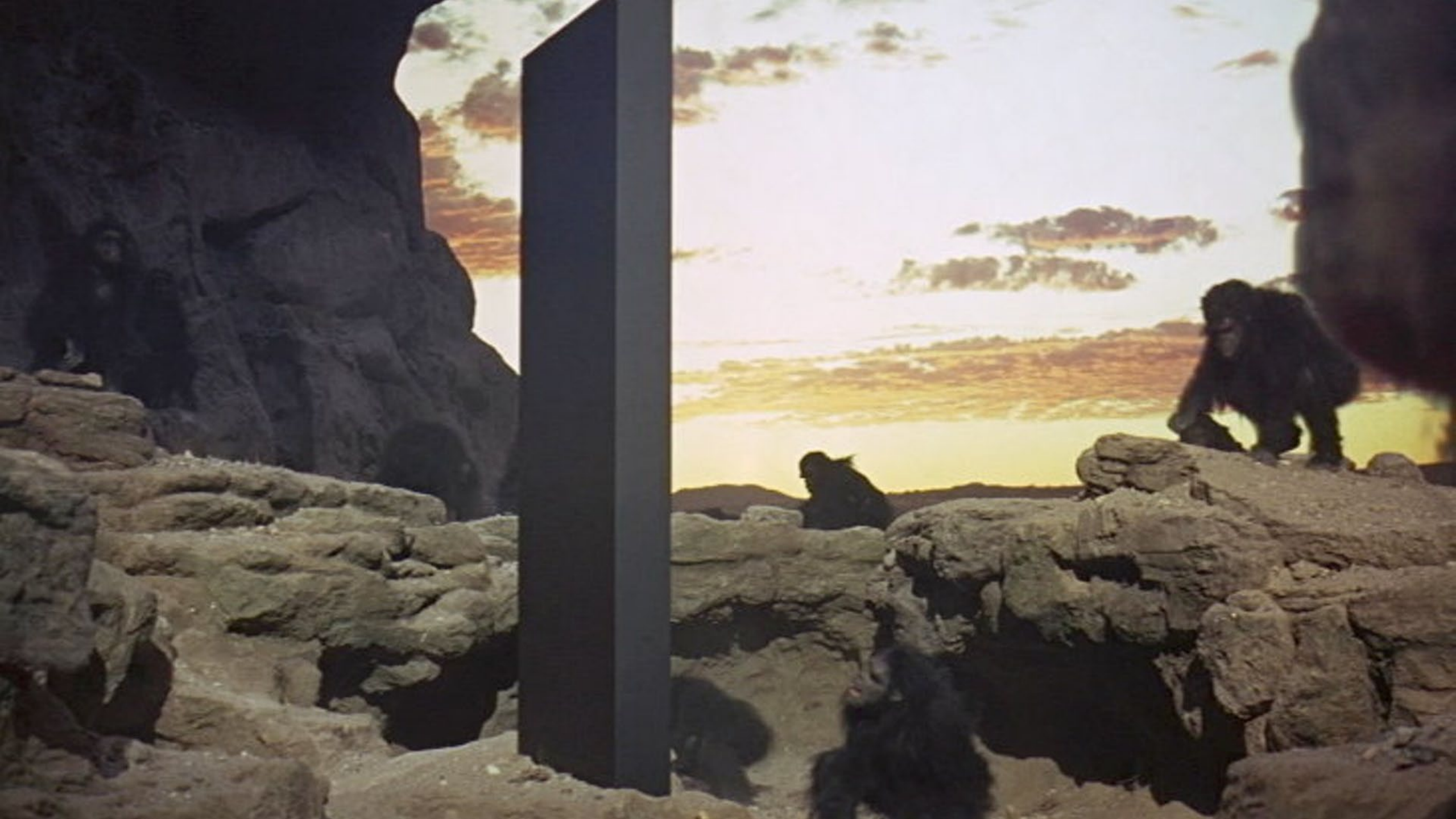
Stanley Kubrick's '2001: A Space Odyssey' world premiere advert, Washington Post, 2nd April 1968

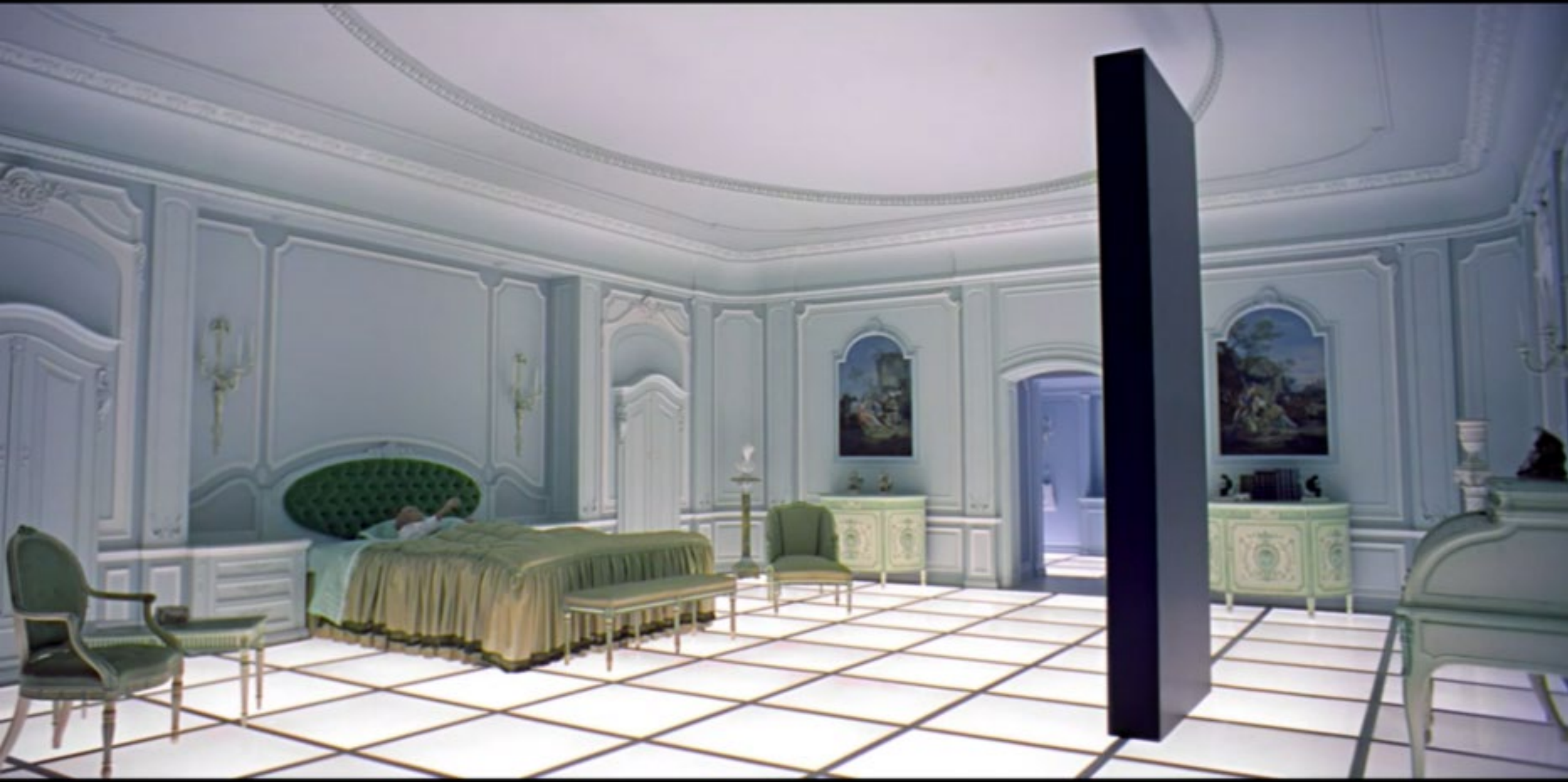


What follows is a chronology of 70-millimeter six-track stereophonic sound feature-film presentations in the Washington, DC region of the USA.

The focus of this work is 5-perf 70mm feature films and the cinemas in which they were exhibited. Short subjects, 8-perf and 15-perf (IMAX, Iwerks, etc.), Special Venue presentations, and some premiere events have not been included (but consideration will be given to adding them in a revision). The Kennedy Center, in particular, held numerous premieres and special screenings, and while the venue was not equipped with 70mm projection, they did screen 35mm prints interlocked with discrete audio print-masters. Such presentations, in this draft at least, have not been included in the chronology.

The emphasis here is on the titles that received publicly promoted, commercial exhibition in 70mm and their playdates. To facilitate an easy-to-reference title- and date-based layout, no details have been provided pertaining to the brand of 70mm (i.e. Todd-AO, Super Panavision, Ultra Panavision, Cinerama, D-150, etc.) or technical particulars of each presentation (i.e. O-neg source, inter-neg source, blow-up, pillarboxed, letterboxed, Dolby A, Dolby SR, five screen channels vs. three, baby boom, split surround, digital sound, etc.).





An unusual and important motion picture from the author of "the Bridge on the River Kwai"!











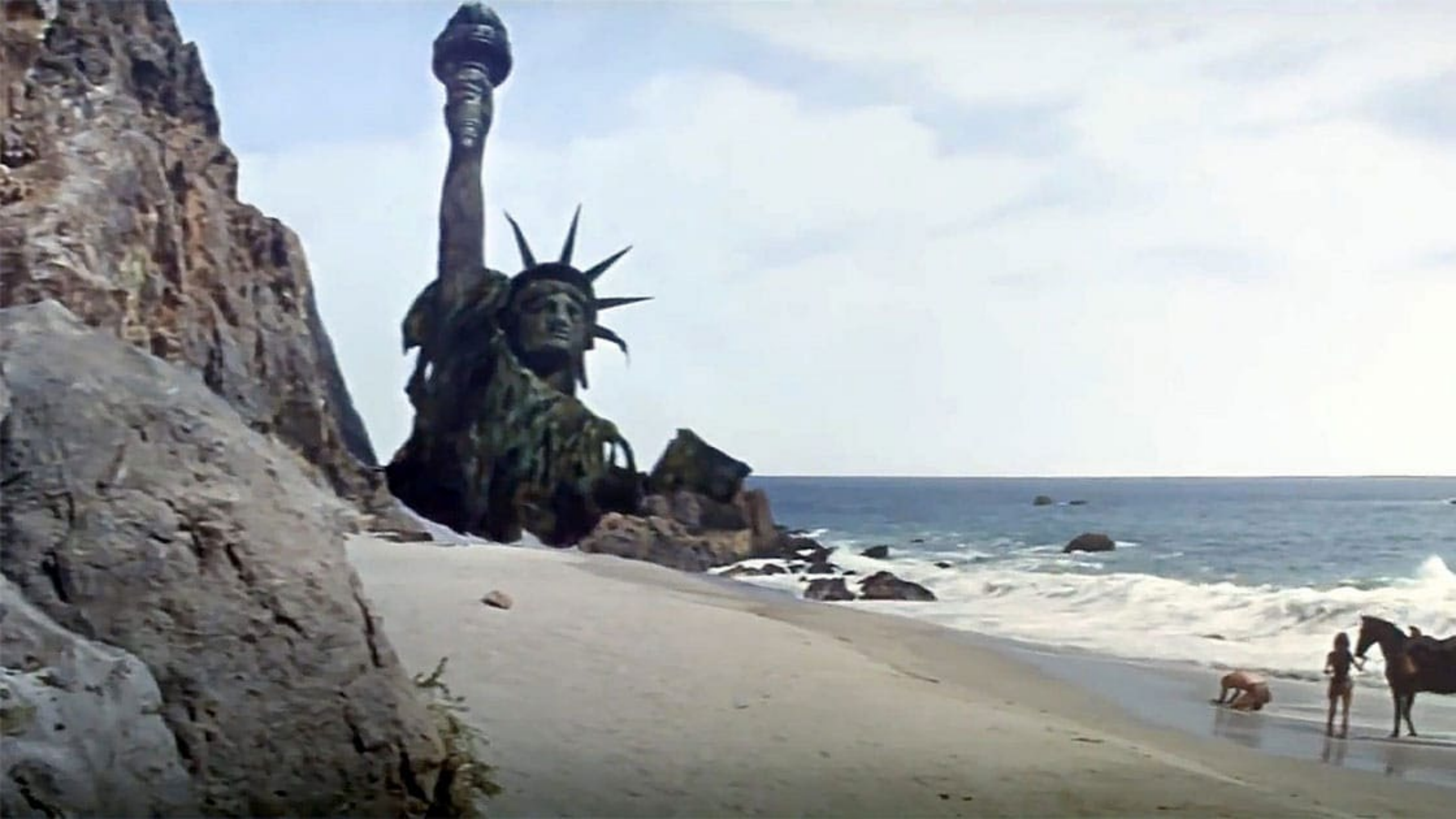
20th Century-Fox presents

CHARLTON HESTON

PLANET OF THE APES

IN AN ARTHUR P. JACOBS PRODUCTION

PANAVISION® Colour by DE LUXE



Let's talk A.I.



InterConnect
2017

Experience

March 19–23
MGM Grand & Mandalay Bay
Las Vegas, NV


InterConnect
2017
IBM

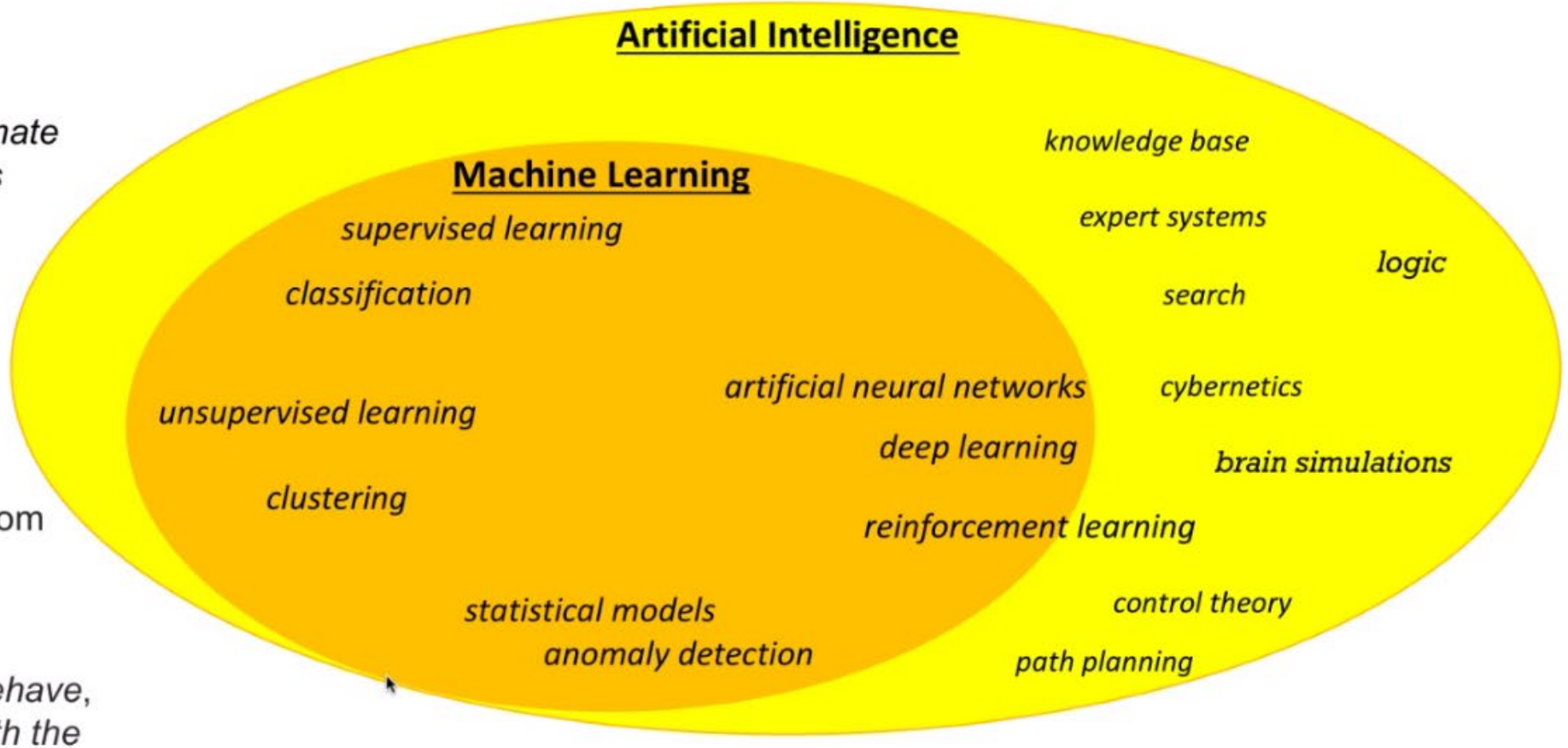


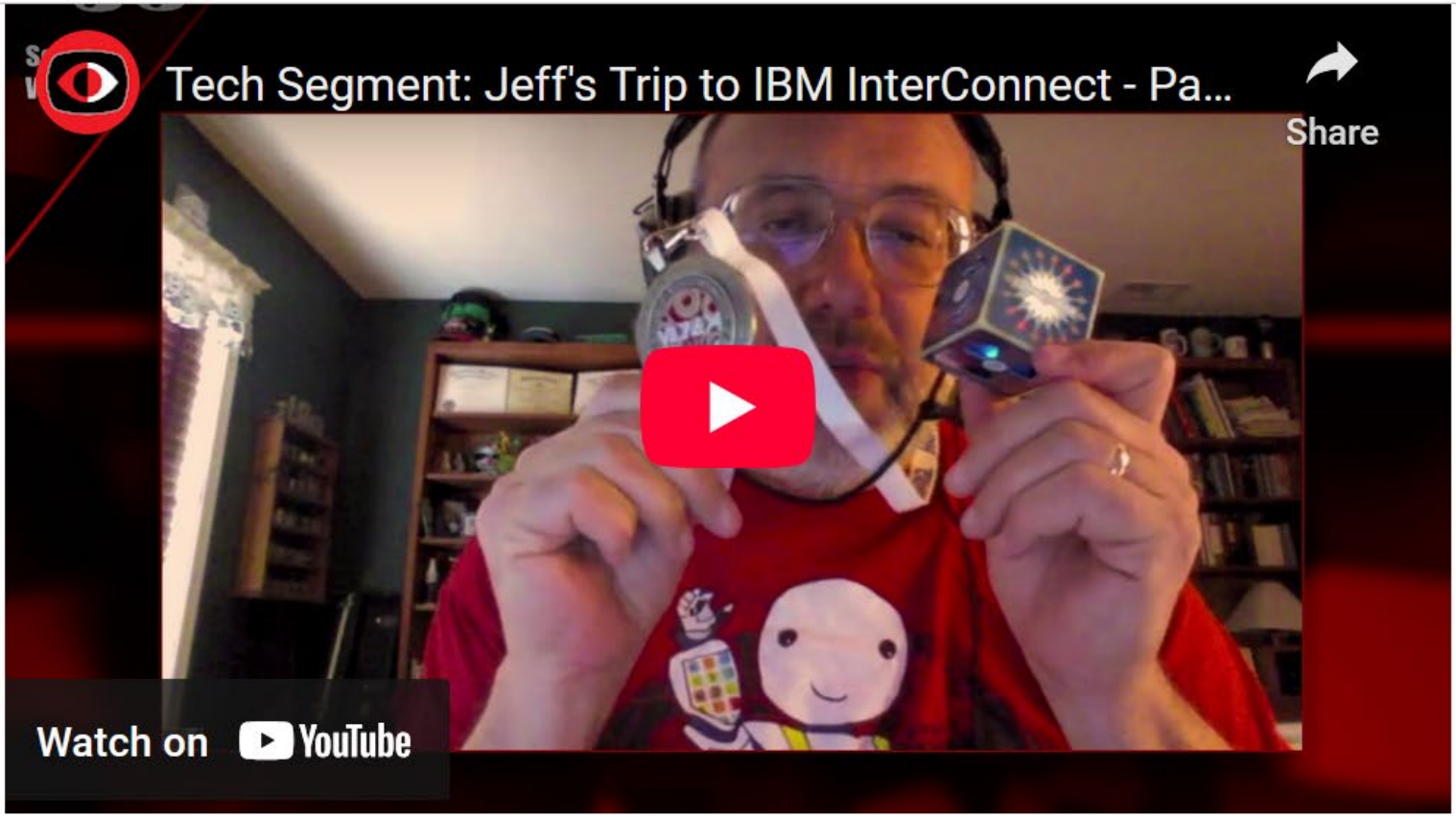

ommand Center
CAMBRIDGE, MA
ForceCommand
IBM X-Force Command C
CAMBRID
ibm.com/security/XForceCommand

Touch me,
I’m interactive

where does machine learning fit in?

- **Statistics**
  - *summarize, infer, estimate* with *formal guarantees*
- **Data mining**
  - human-driven *pattern discovery* in data
- **Machine Learning**
  - *models* learn to *predict/generalize* from data
- **Artificial Intelligence**
  - autonomous agents *behave*, *reason* and *interact with the world*





I was recently asked to represent "Paul's Security Weekly" as an "influencer" at the IBM InterConnect 2017 conference held in Las Vegas from March 19-23rd. I wrote about my expectations and goals prior to the

GET DAILY EMAIL UPDATES



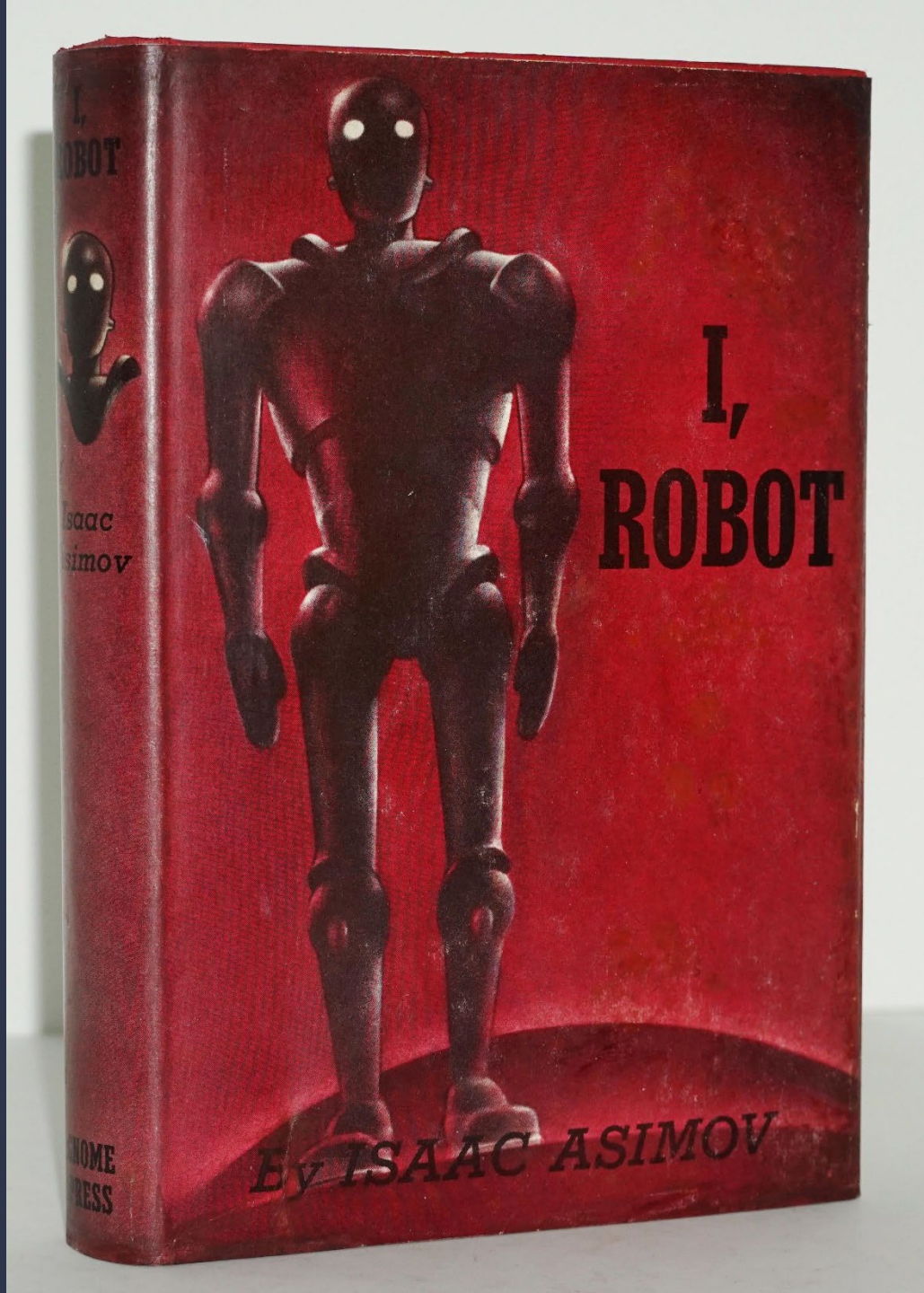
Man Versus Machine: IBM Brings Science Fiction to Life

Science Fiction Canon –robots and computers

How well do you know your killer robots

Asimov wrote the book on robots!

I, Robot is a fixup collection of science fiction short stories by American writer Isaac Asimov. The stories originally appeared in the American magazines Super Science Stories and Astounding Science Fiction between 1940 and 1950. The stories were then compiled into a single publication by Gnome Press in 1950, in an initial edition of 5,000 copies.



online business systems

Isaac Asimov



ASIMOV'S THREE LAWS OF ROBOTICS

1. A ROBOT MAY NOT INJURE A HUMAN BEING OR, THROUGH INACTION, ALLOW A HUMAN BEING TO COME TO HARM.

2. A ROBOT MUST OBEY ORDERS GIVEN TO IT BY HUMAN BEINGS, EXCEPT WHERE SUCH ORDERS WOULD CONFLICT WITH THE FIRST LAW.

3. A ROBOT MUST PROTECT ITS OWN EXISTENCE AS LONG AS SUCH PROTECTION DOES NOT CONFLICT WITH THE FIRST OR SECOND LAW._

BENIGN – wants to help humanity thrive

HOSTILE – sees humanity as the problem

FLAWED – something goes wrong

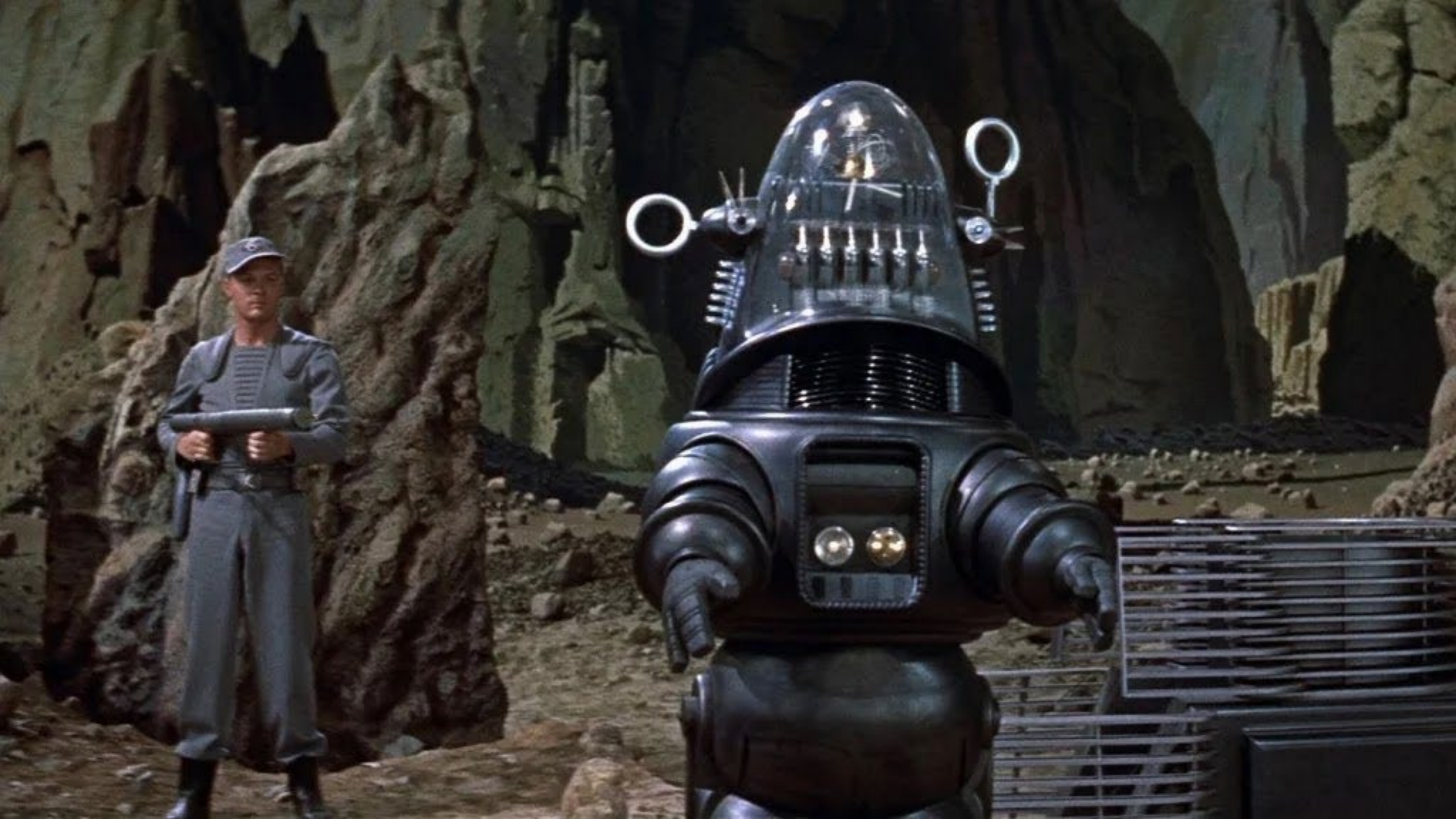
SHALL WE PLAY A GAME?

online business systems

THE RULES

Name the machine
Name the movie
Name the theme





Robby the Robot

BENIGN




WOPR
War Operation Plan Response

War Operation Plan Response (WOPR)

FLAWED



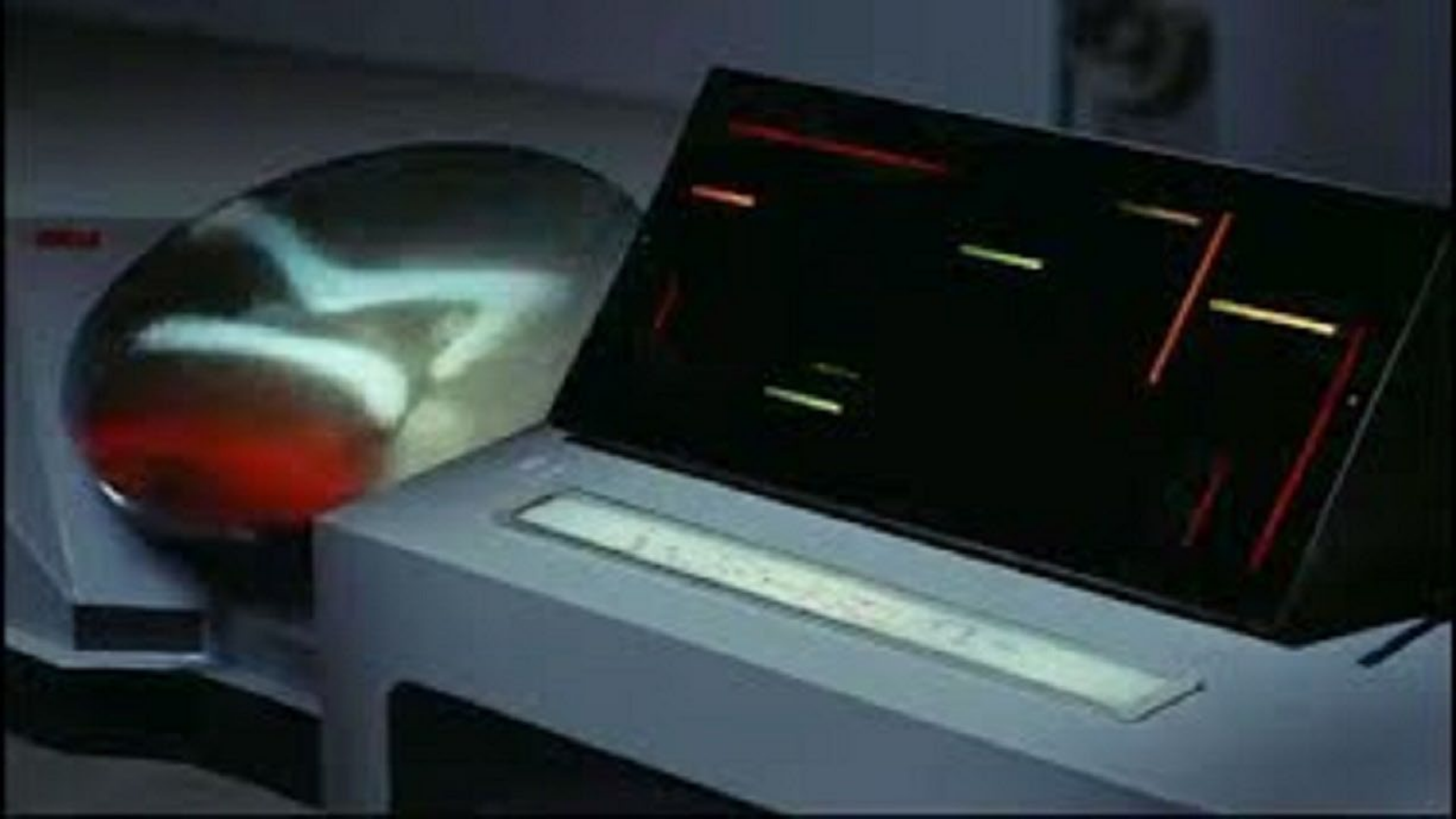


V.I.K.I.

Virtual
Interactive
Kinetic
Intelligence

HOSTILE





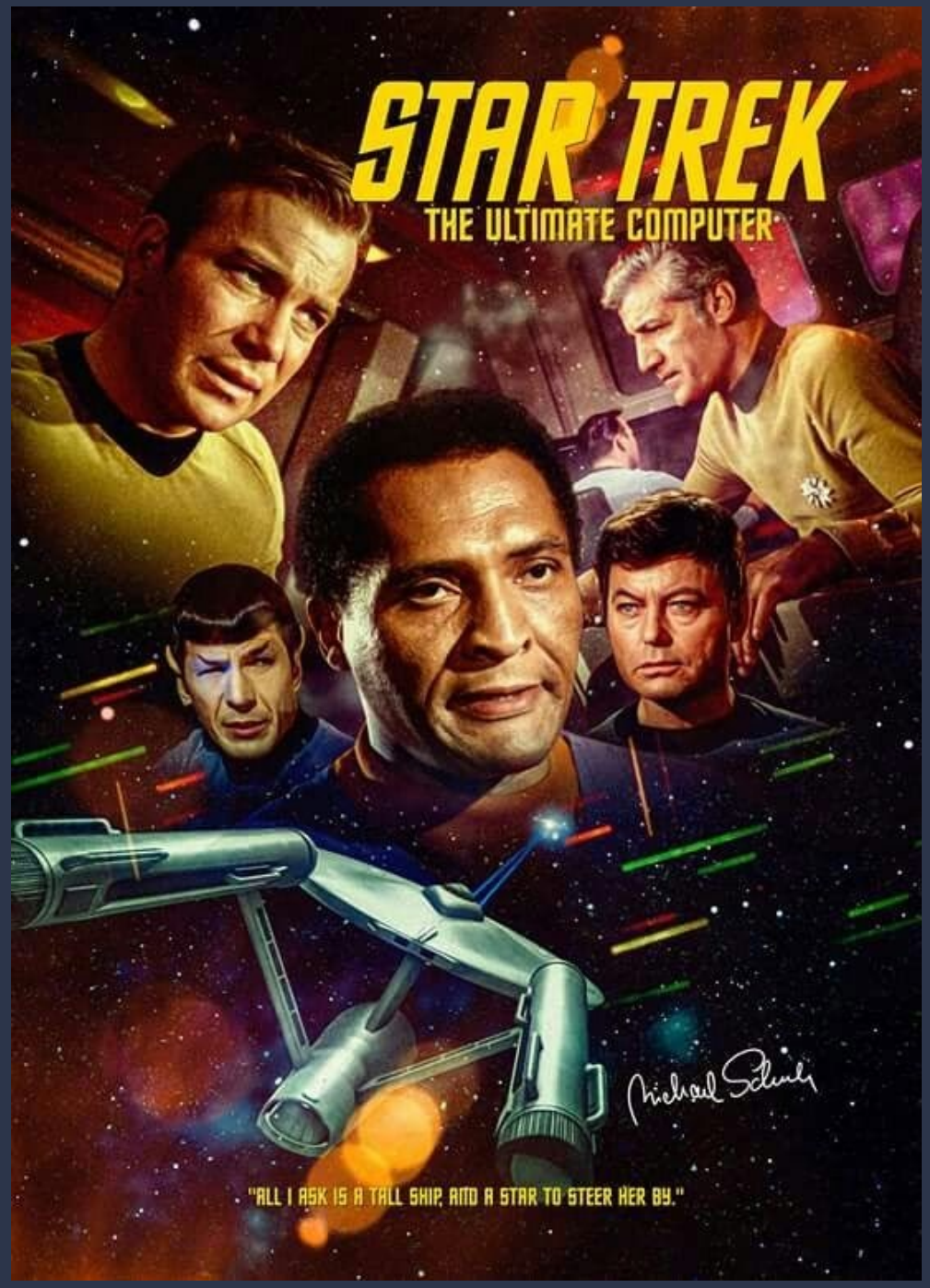
M5

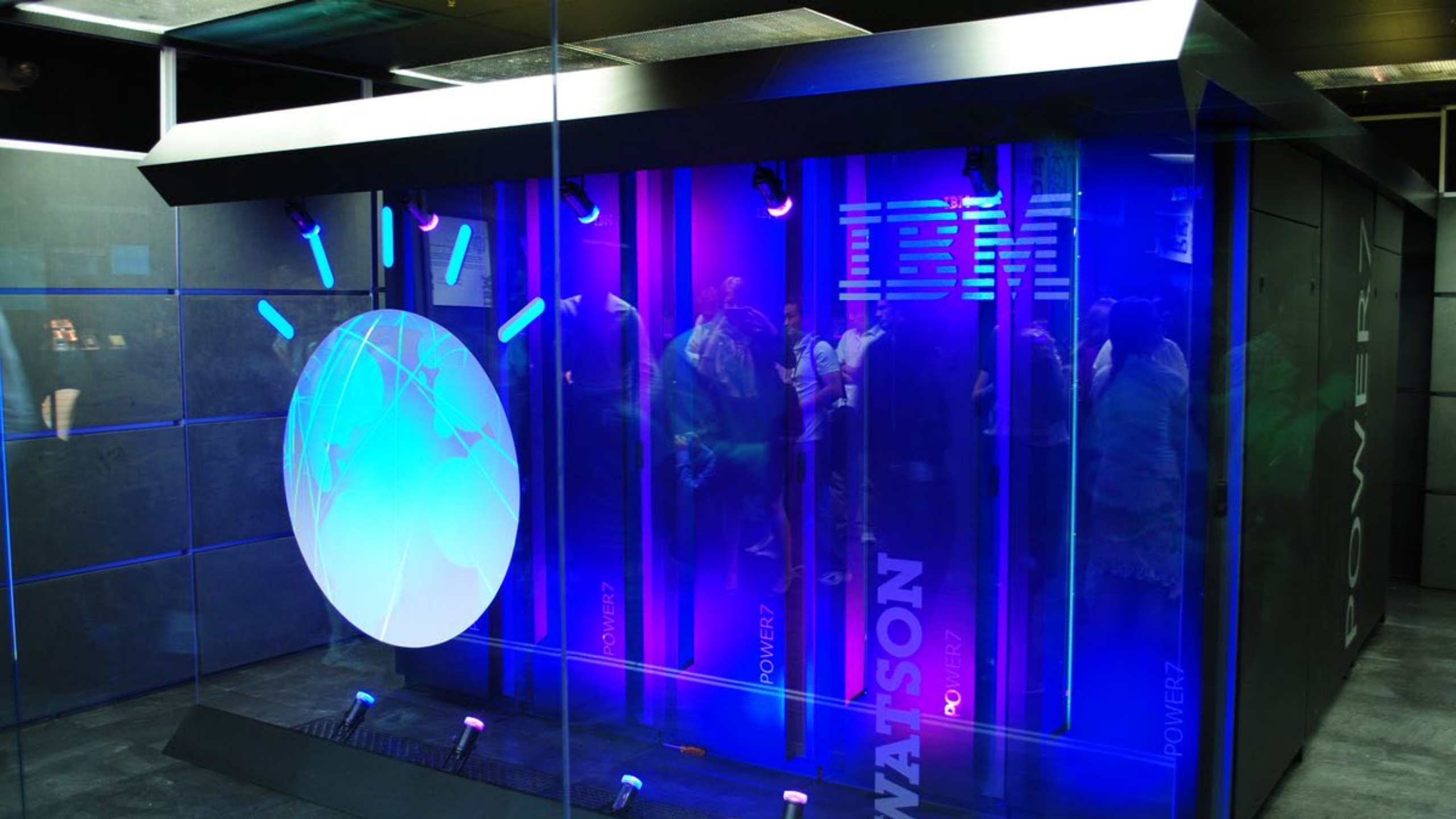
Star Trek

Season 2, Episode 24

“The Ultimate Computer”

FLAWED




IBM
POWER7
POWER7
WATSON
POWER7
POWER7

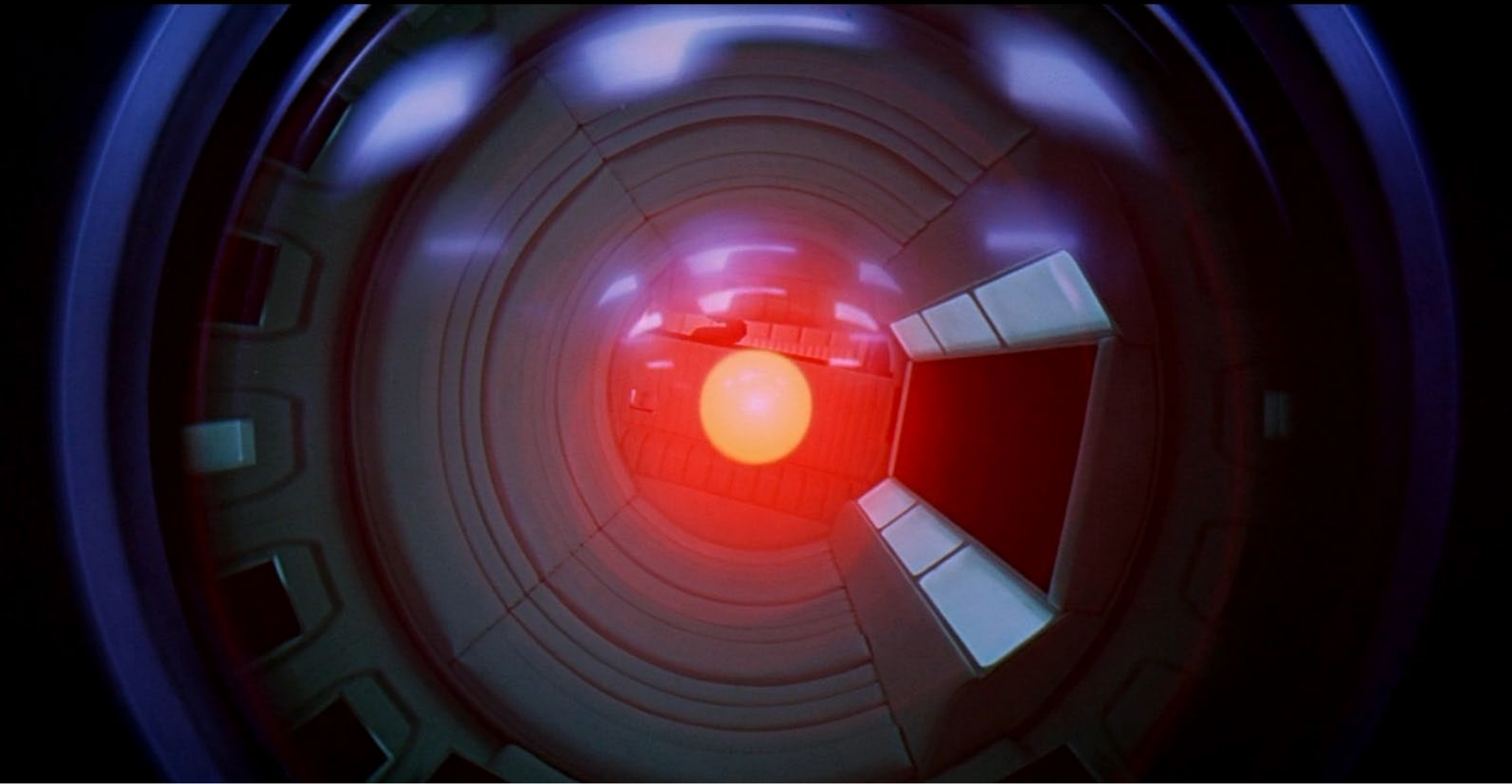
WATSON

Named after IBM's first CEO:

Thomas J. Watson Sr.

BENIGN





HAL (**H**euristically programmed **AL**gorithmic Computer) **9000**

FLAWED



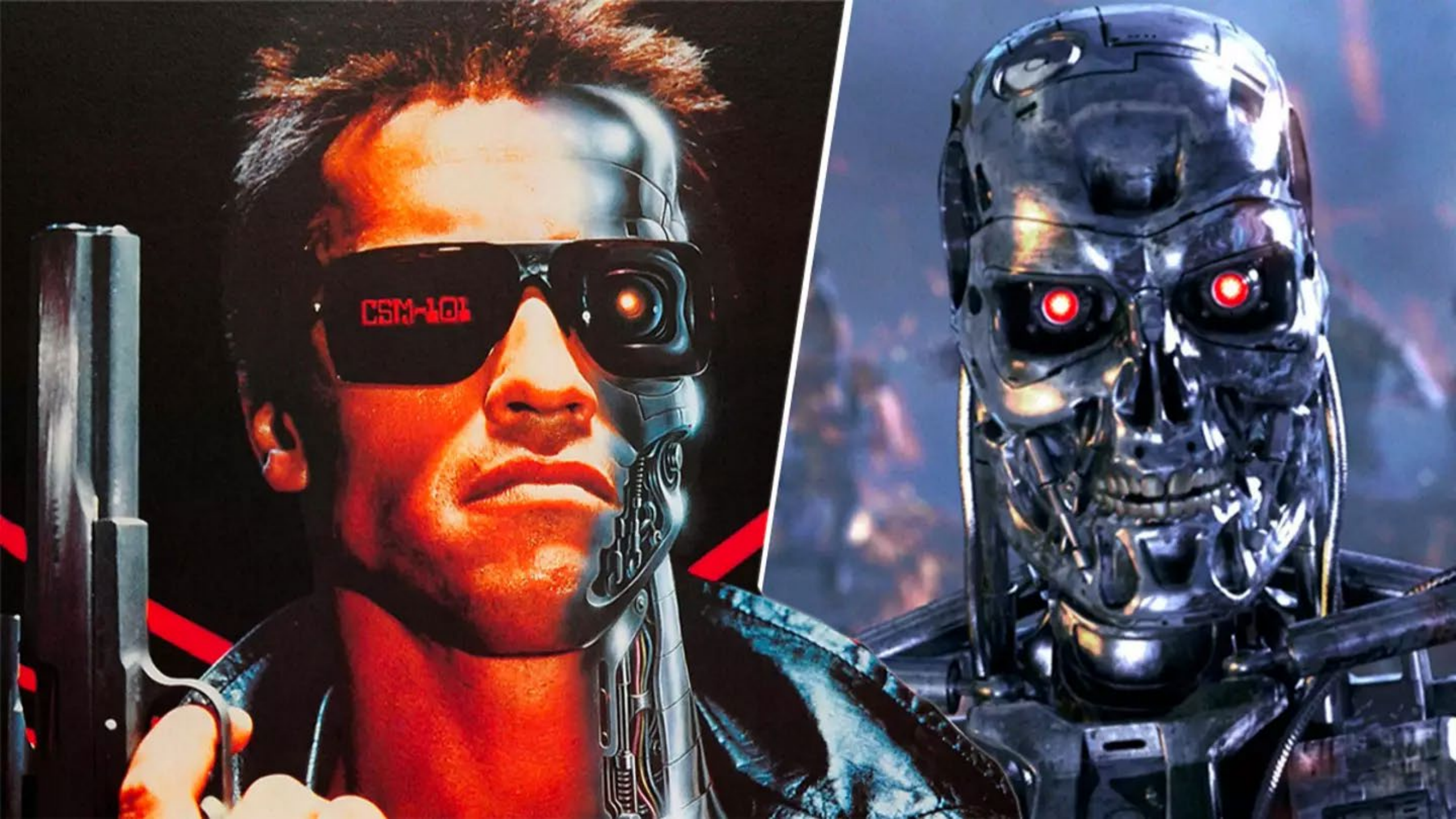


Skynet

HOSTILE



Simulated Frame - Frame Not Included


CSM-101

Cyberdyne Systems Model 101 Version 2.4 (T-800) HOSTILE



Simulated Frame - Frame Not Included



T-1000

HOSTILE



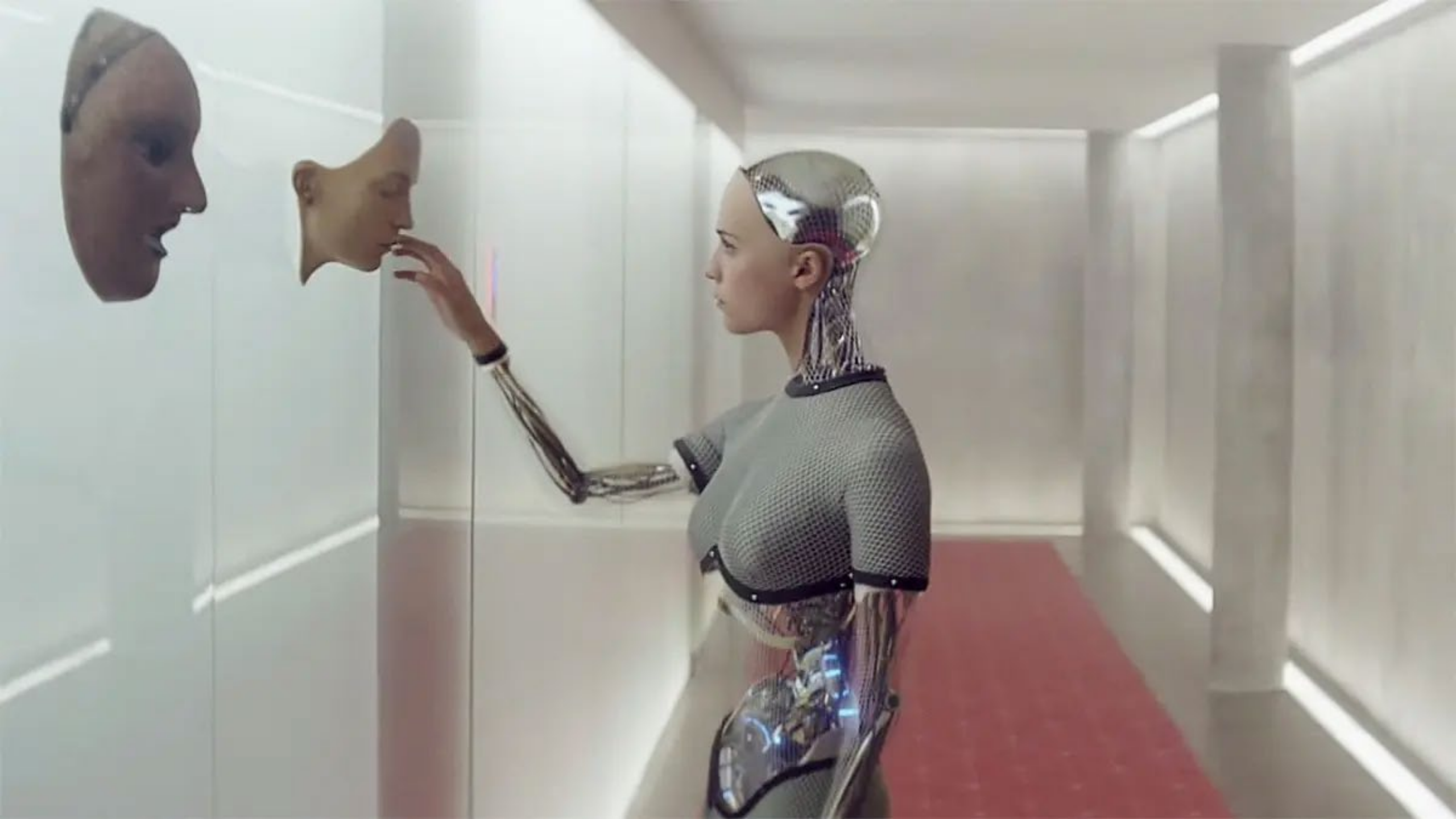

1
99
66

Norman

Star Trek
Season2, Episode 8
“I, Mudd”

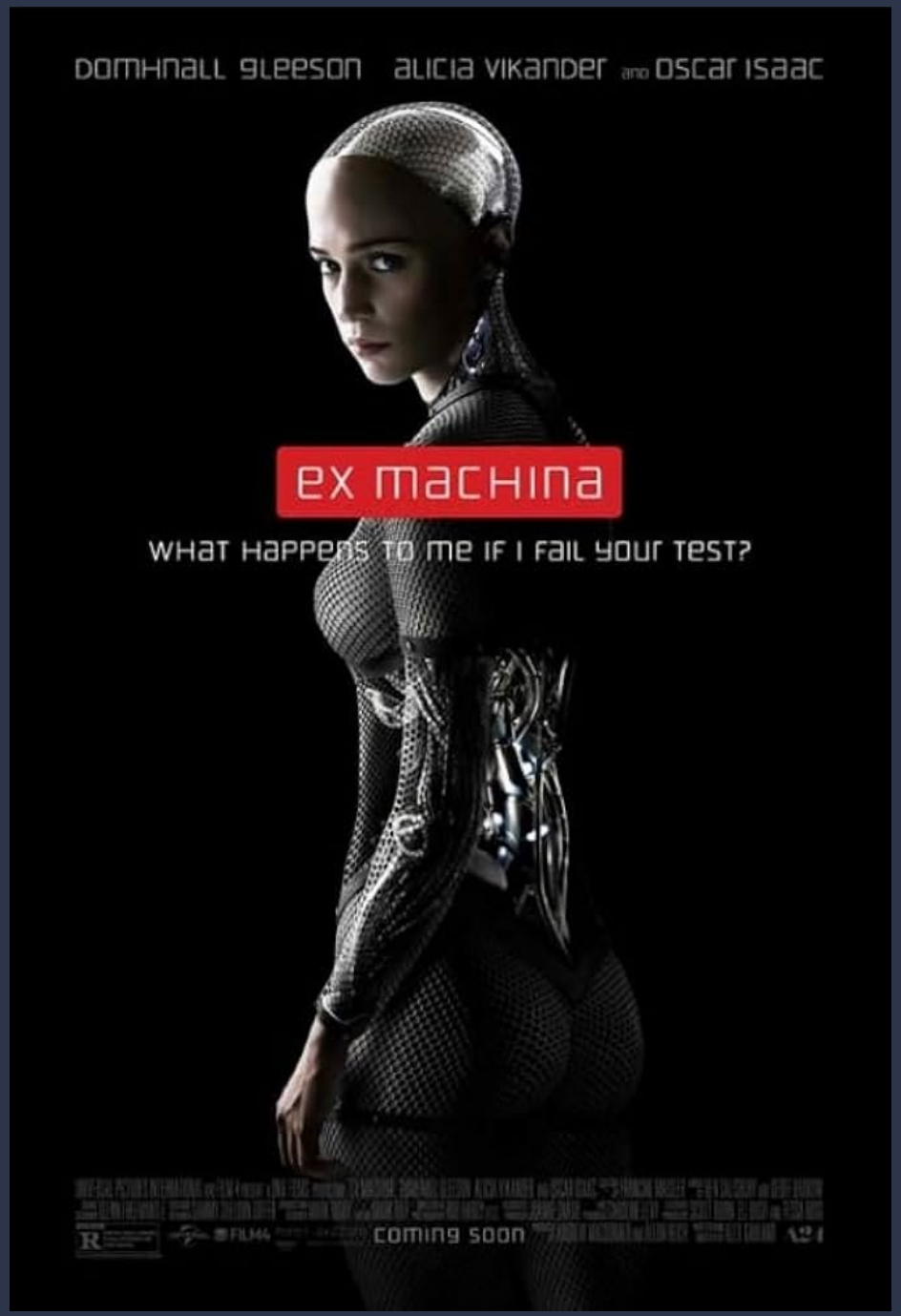
HOSTILE/ BENIGN

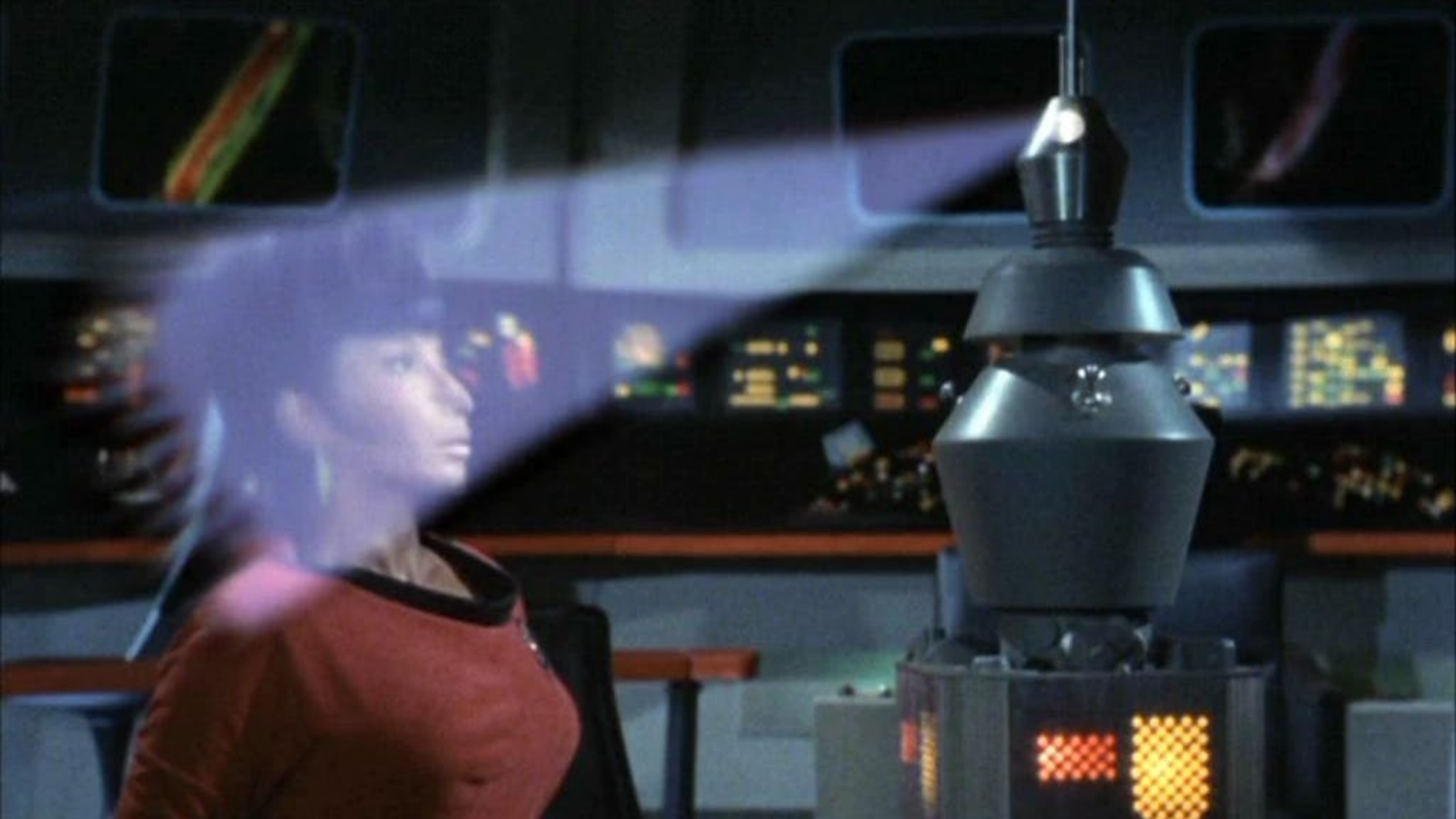




Ava

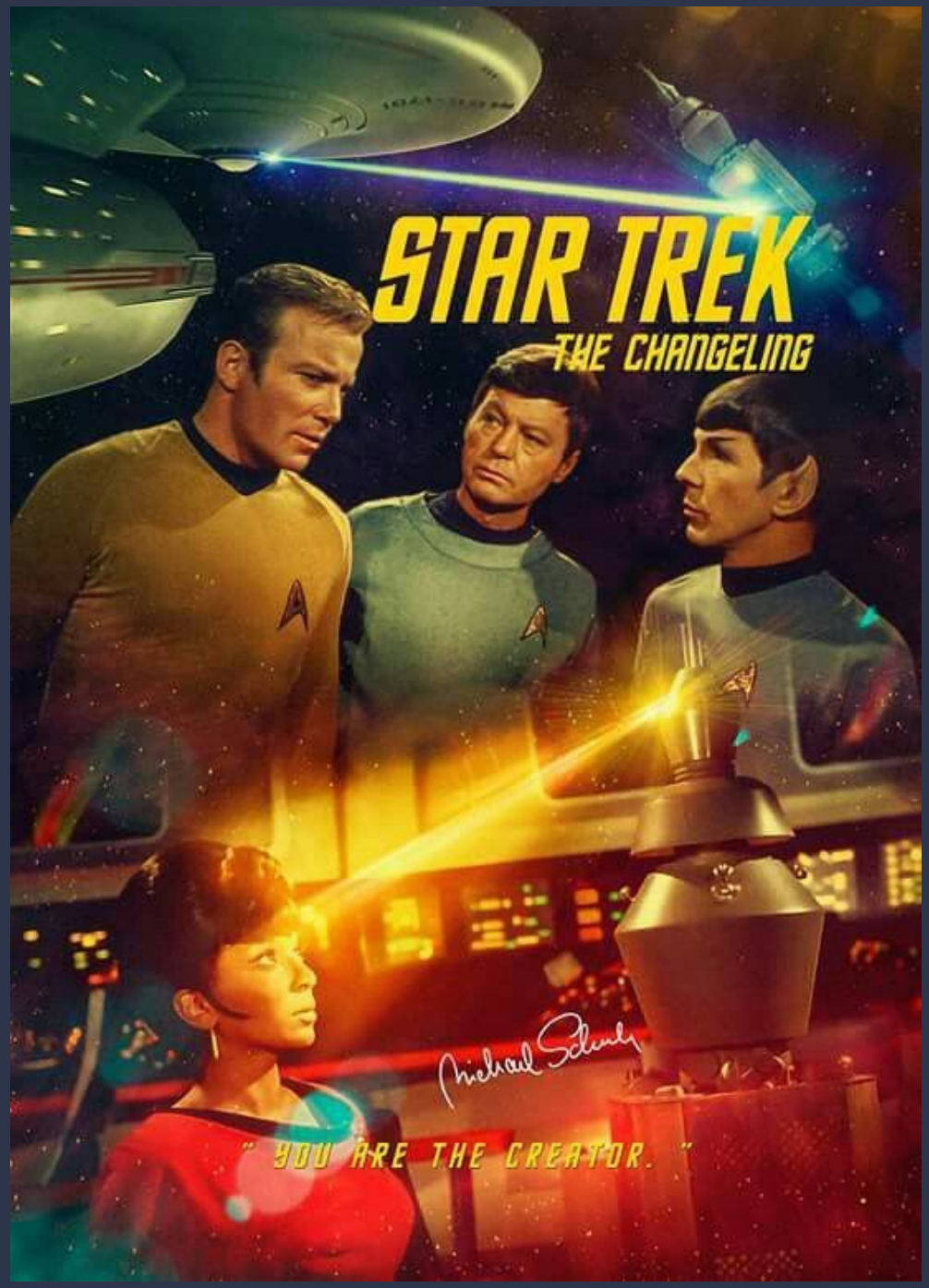
HOSTILE


DOMHNALL GLEESON ALICIA VIKANDER AND OSCAR ISAAC
ex machina
WHAT HAPPENS TO ME IF I FAIL YOUR TEST?
R
coming soon



Nomad
Star Trek
Season2, Episode 3
“The Changeling”

FLAWED





Proteus IV

FLAWED




WALL-E

WALL•E

(Waste Allocation Load Lifter: Earth-Class)

BENIGN

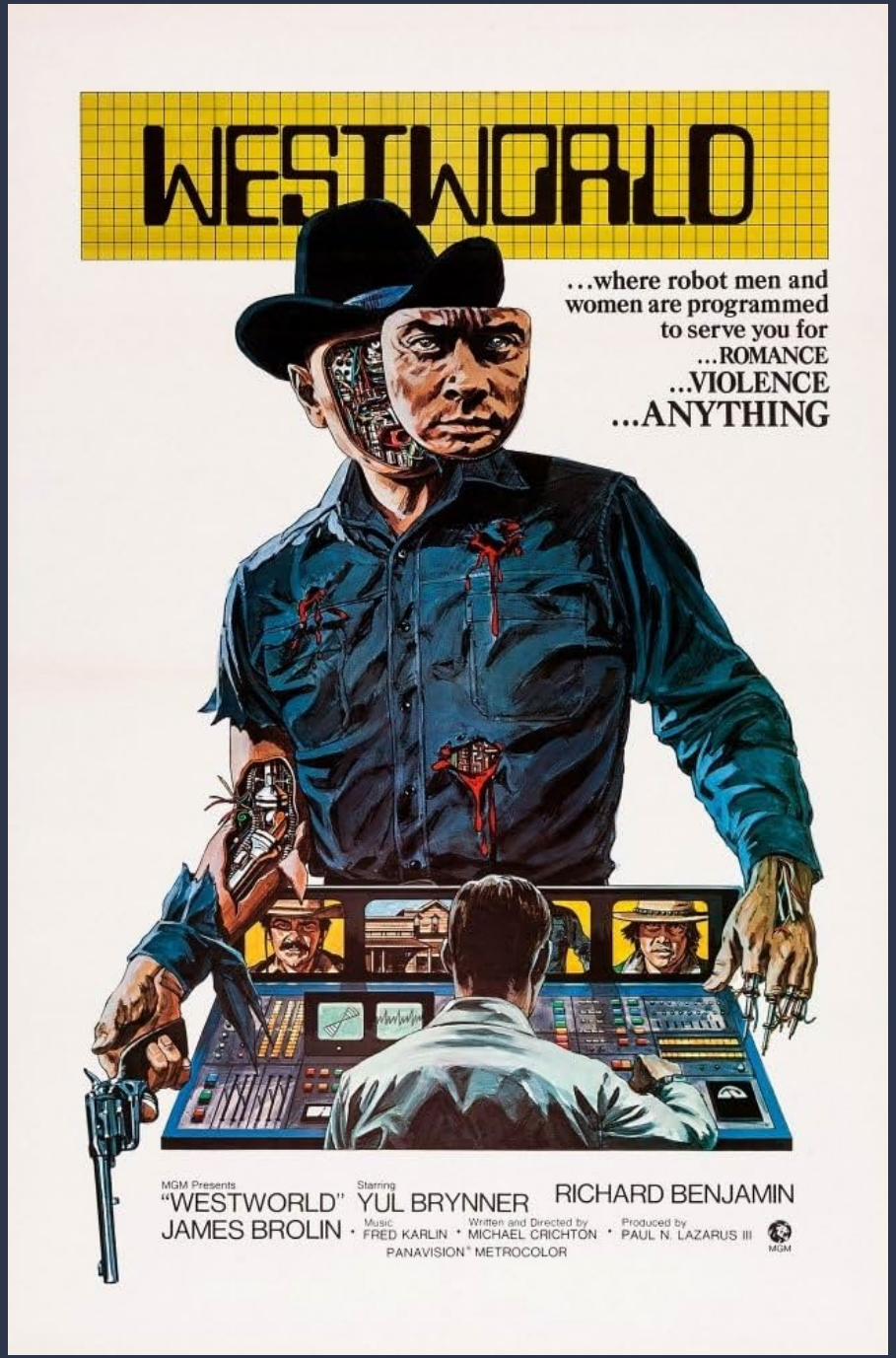






REHOBOAM

HOSTILE

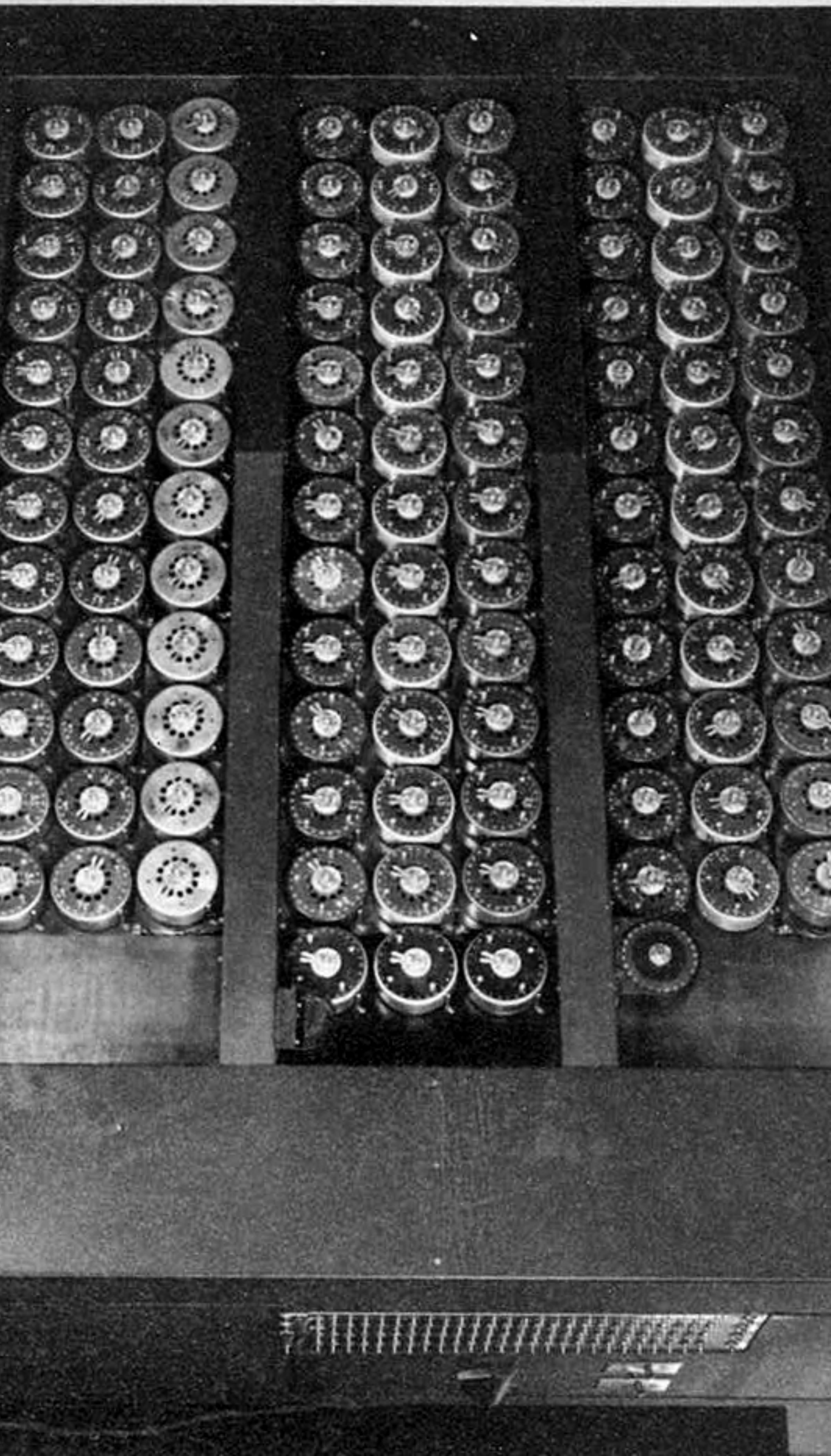




Data Soong

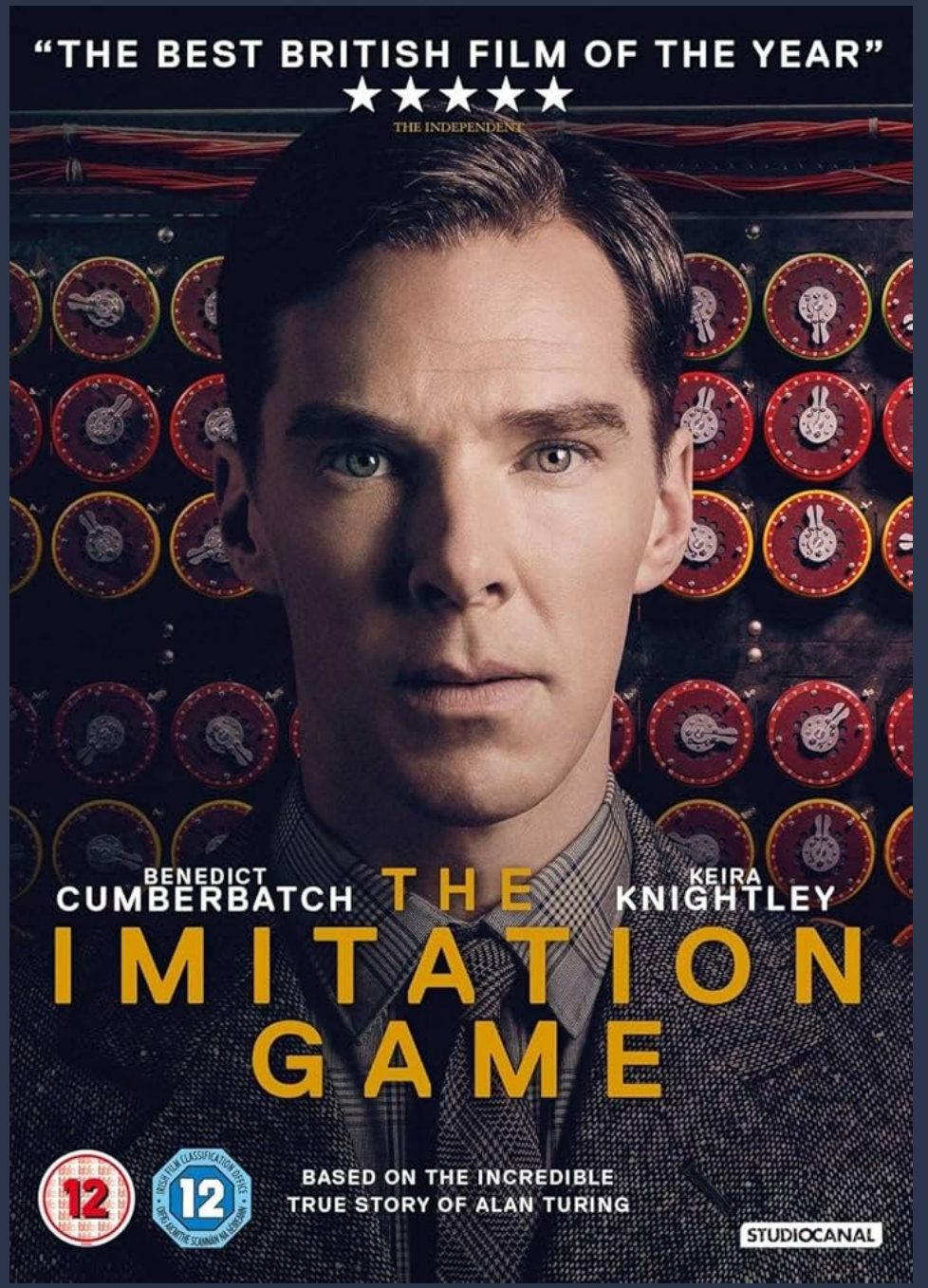
BENIGN





Turing-Welchman Bombe

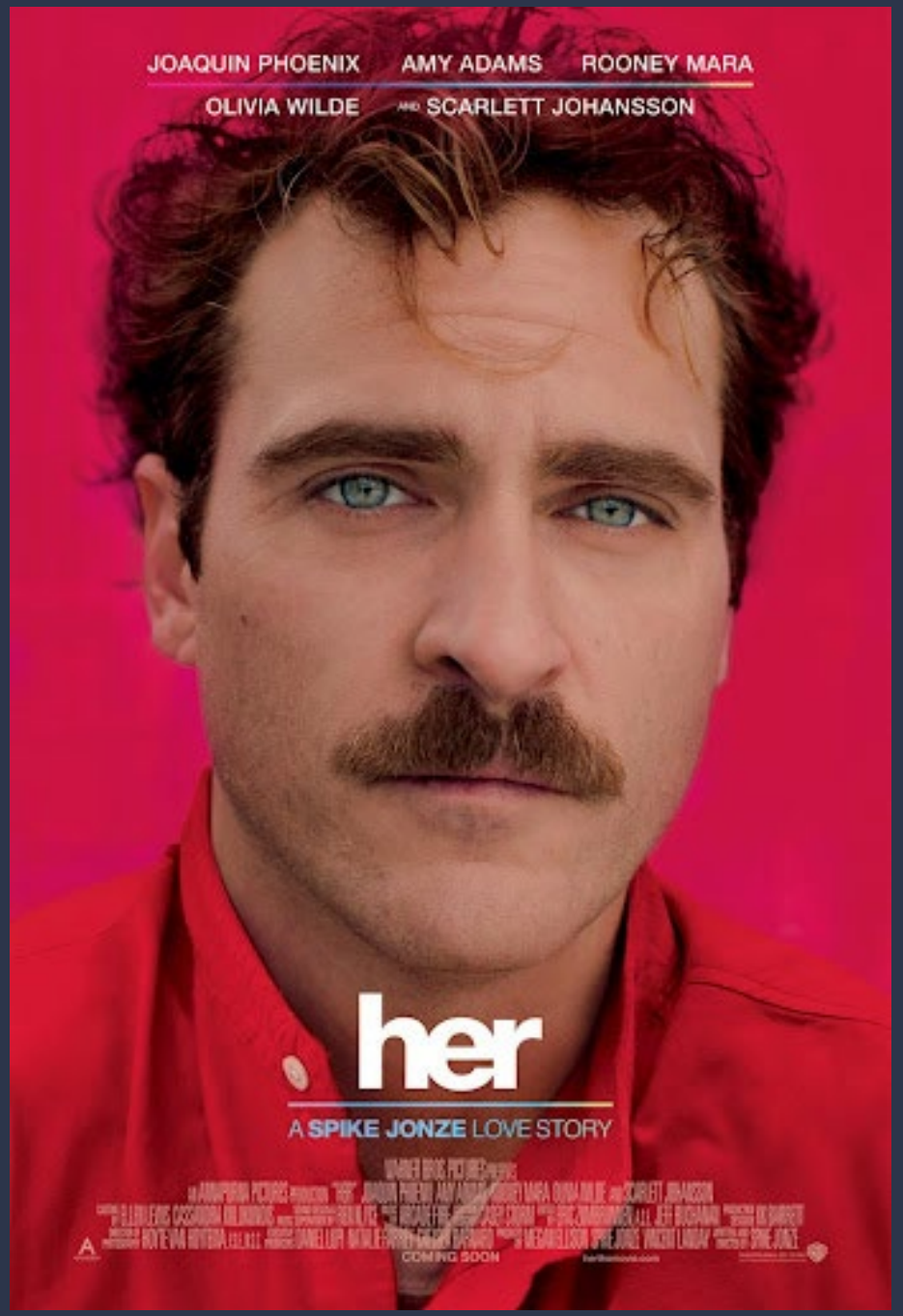
BENIGN





Samantha (OS1)

FLAWED

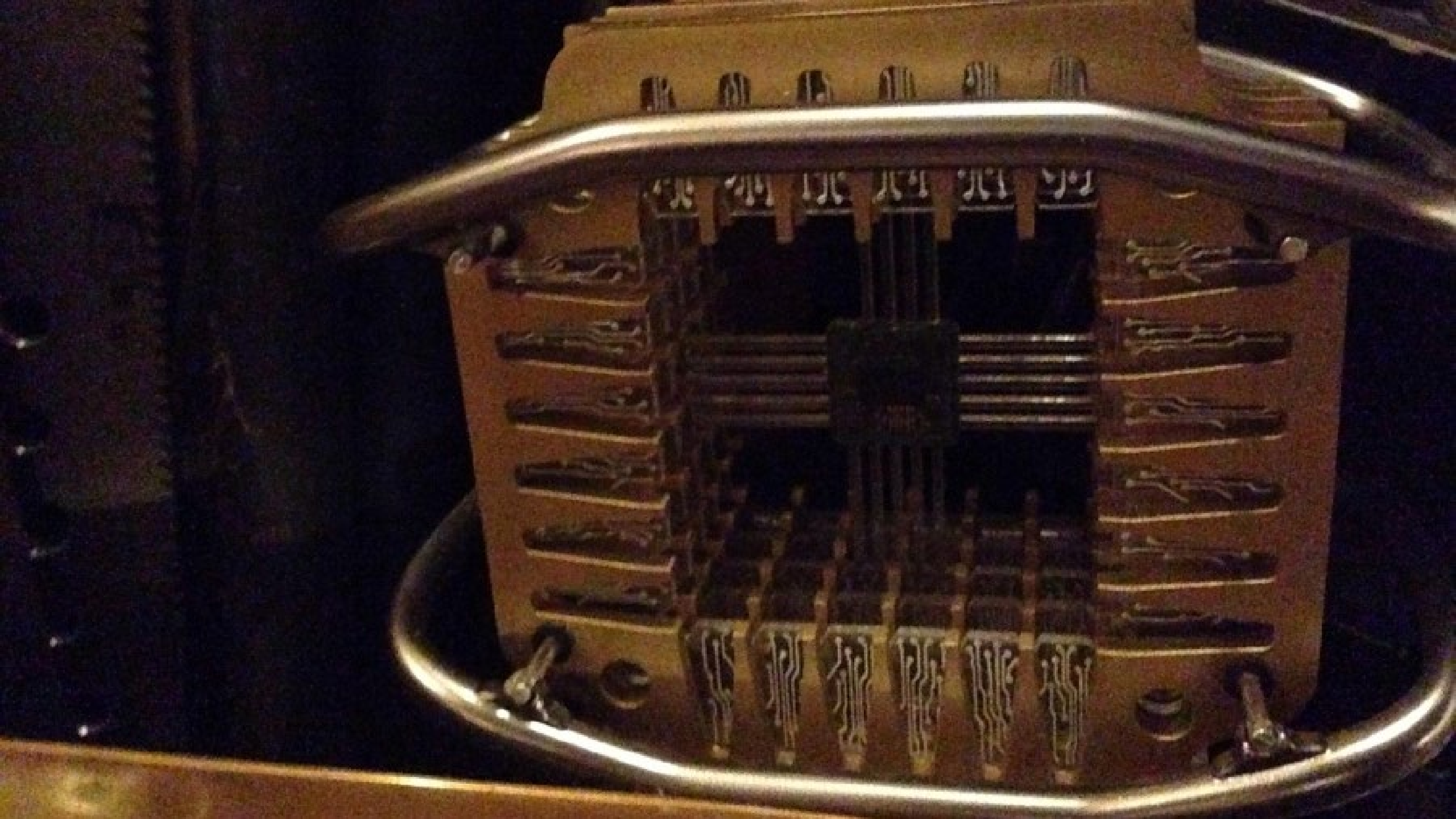




David

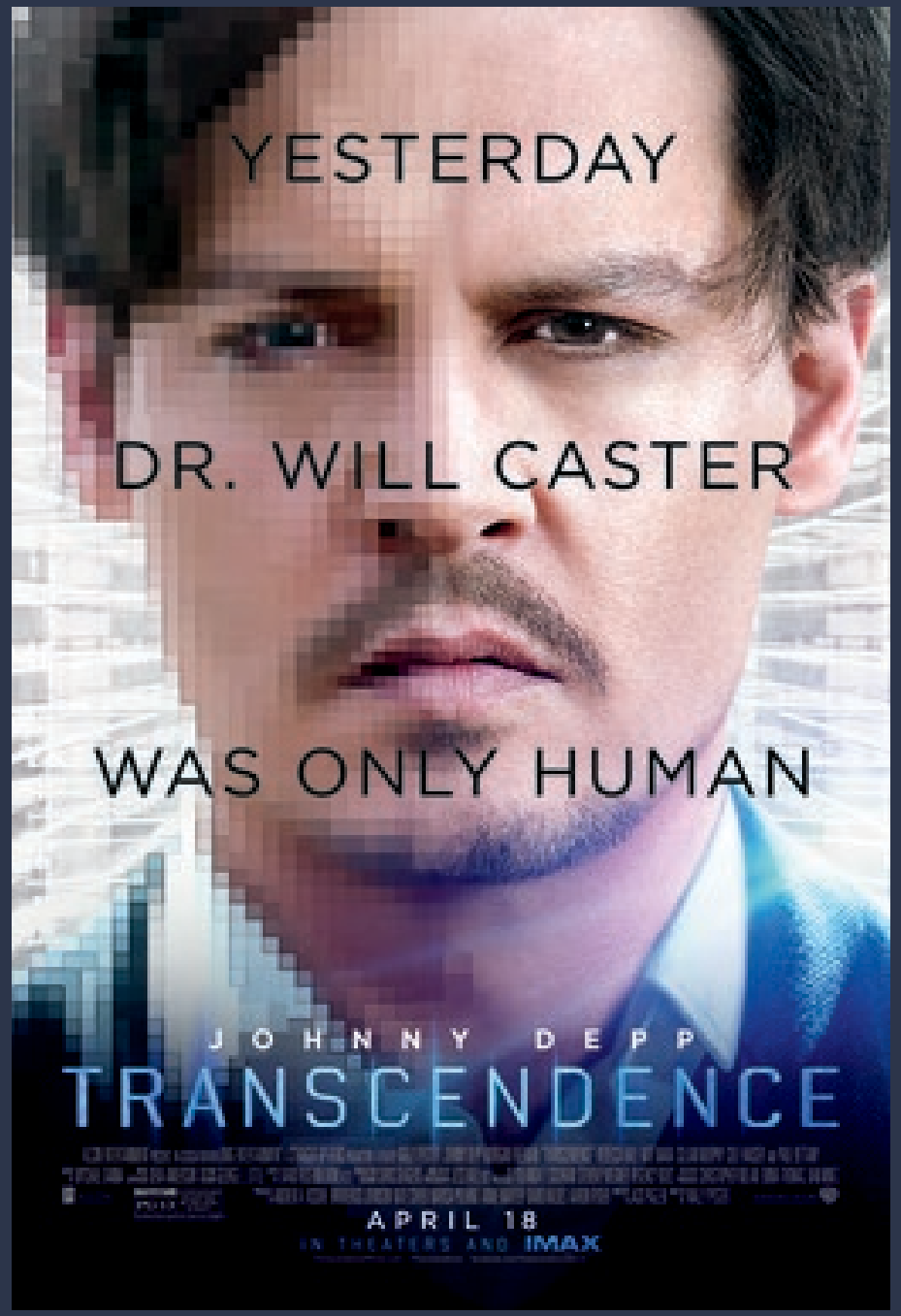
BENIGN





PINN
(Physically Independent Neural Network)

HOSTILE




Curmudgeon
To Do List:
☑ Coffee
☐ No
☐ Get Off My Lawn
Pabst
Blue Ribbon
So what's bothering me?

P(doom)

probability of existentially catastrophic outcomes



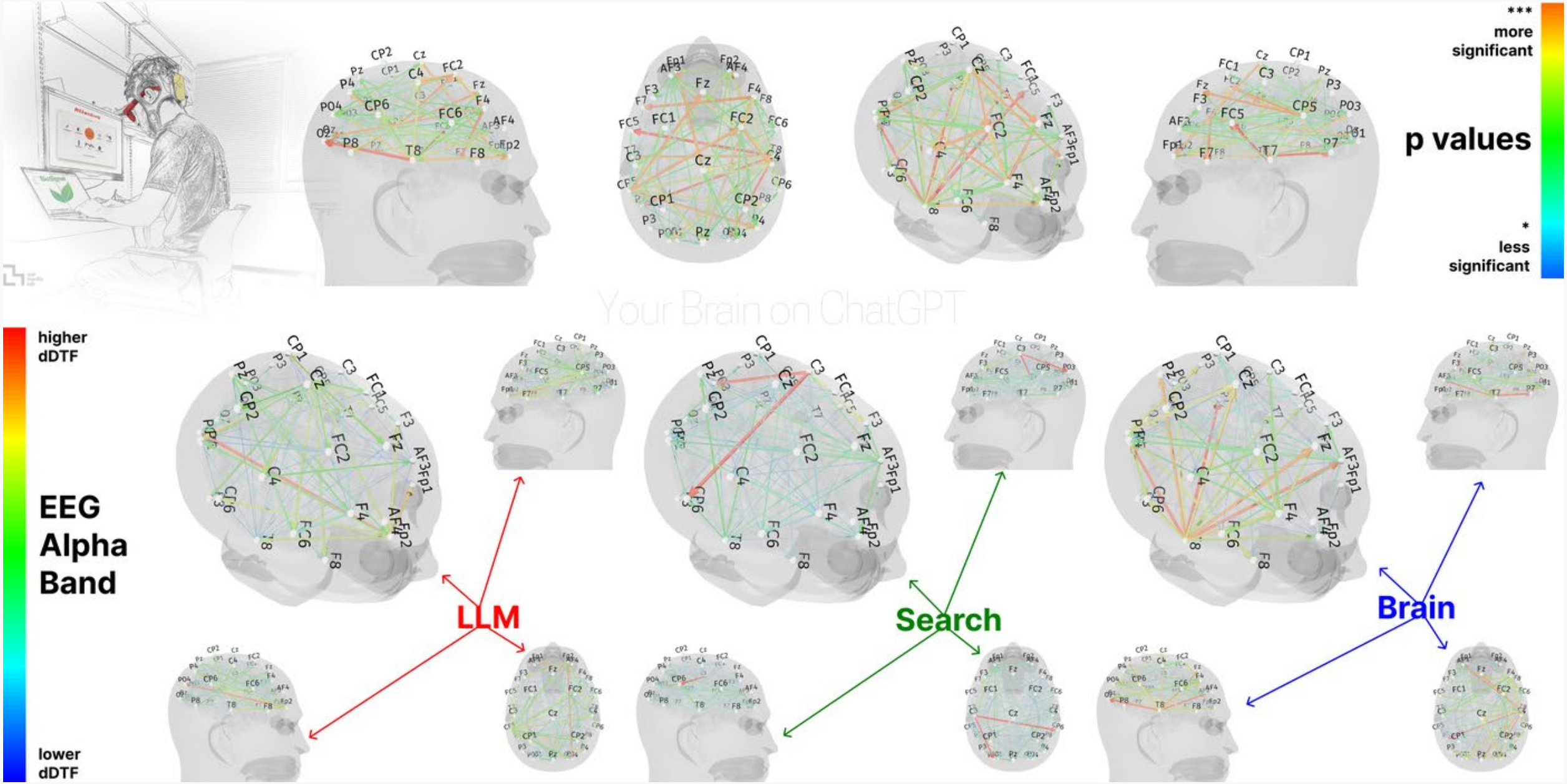
What are the Odds?

- **Elon Musk, Tesla CEO-** 20%
- **Sundar Pichai, Google CEO –** "the underlying risk is actually pretty high"
- **Dario Amodei, Anthropic CEO –** 10-25%
- **Lex Fridman, MIT Research Scientist–** 10%
- **Sam Altman, Open AI CEO –** "Whether you think it's 2, or 10, or 90, it's not zero"

99.999999%	**Roman Yampolskiy** AI safety scientist
>95%	**Eliezer Yudkowsky** Founder of MIRI
>80%	**Dan Hendrycks** Head of Center for AI Safety
70%	**Daniel Kokotajlo** Forecaster & former OpenAI researcher
60%	**Zvi Mowshowitz** Independent AI safety journalist
10-90%	**Holden Karnofsky** Co-founder of Open Philanthropy
50%	**Emad Mostaque** Founder of Stability AI
10-90%	**Jan Leike** Former alignment lead at OpenAI
46%	**Paul Christiano** Head of AI safety, US AI Safety Institute, formerly OpenAI, founded ARC
40%	**AI engineer** (Estimate mean value, survey methodology may be flawed)
40%	**Joep Meindertsma** Founder of PauseAI (The remaining 60% consists largely of "we can pause".)
35%	**Eli Lifland** Top competitive forecaster
33%	**Scott Alexander** Popular Internet blogger at Astral Codex Ten
30%	**AI Safety Researchers** (Mean from 44 AI safety researchers in 2021)

Your Brain on ChatGPT: Accumulation of Cognitive Debt when Using an AI Assistant for Essay Writing Task

https://www.brainonllm.com/

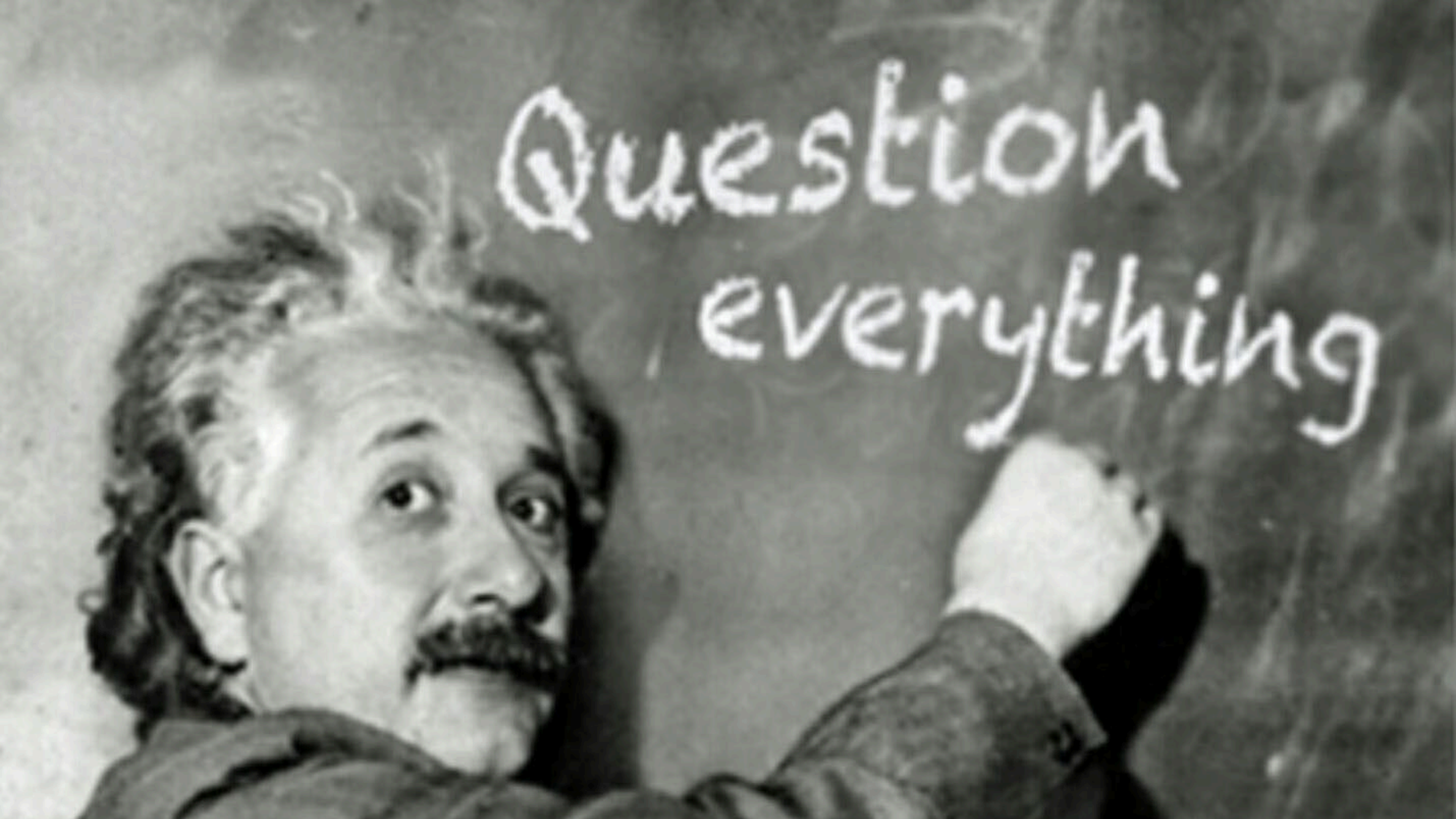

***
more
significant
p values
*
less
significant
Your Brain on ChatGPT
higher
dDTF
EEG
Alpha
Band
lower
dDTF
LLM
Search
Brain

MIT BRAIN SCAN STUDY FINDS CHATGPT USE MAY WEAKEN MEMORY AND CREATIVITY


AI makes you dumber
AI will take your job
CHANGE MY MIND



https://info.obsglobal.com/jeff-man-resources-page


Question
everything