

Using Science Fiction to Teach Cybersecurity

Brad E. Rhodes

VetSecCon '22

October 29, 2022

Outline

WHOIS: Brad Rhodes

Why Teach Cybersecurity with Science Fiction?

1960s

1980s

1990s

2000s

Star Trek

Star Wars

WHOIS: Brad Rhodes

- TLDR:
 - Senior Manager, Accenture Federal Services
 - COL, Cyber (17A), 76th Operational Response Command G6/CIO
 - Military Cyber Professionals Association, HammerCon Co-Lead
 - Speaker, Author, Professor, Coach
 - #toomany Pro-Certs, highlights: CISSP-ISSEP, CISM, CDPSE, PMP, CEH, GMON, GCIH, Cloud+, CySA+
 - Extra Class Amateur Radio (HAM): KG4COS

Feel to view/listen/grab my previous presentation/articles here:

<https://github.com/cyberguy514>



Why Teach Cybersecurity with Science Fiction?

Science fiction influenced technology

Everyone loves a good (relatable) story

There really is science in science fiction

Education does not have to be boring

Cybersecurity training should be memorable

The Italian Job (1969, 2003): Smart City Hacking



Credit: © & TM Oakhurst Productions



Credit: © & TM Paramount Pictures

War Games (1983): Bug Bounty Programs



Credit: © & TM United Artists

Die Hard (1988): Building/Control Systems Attack



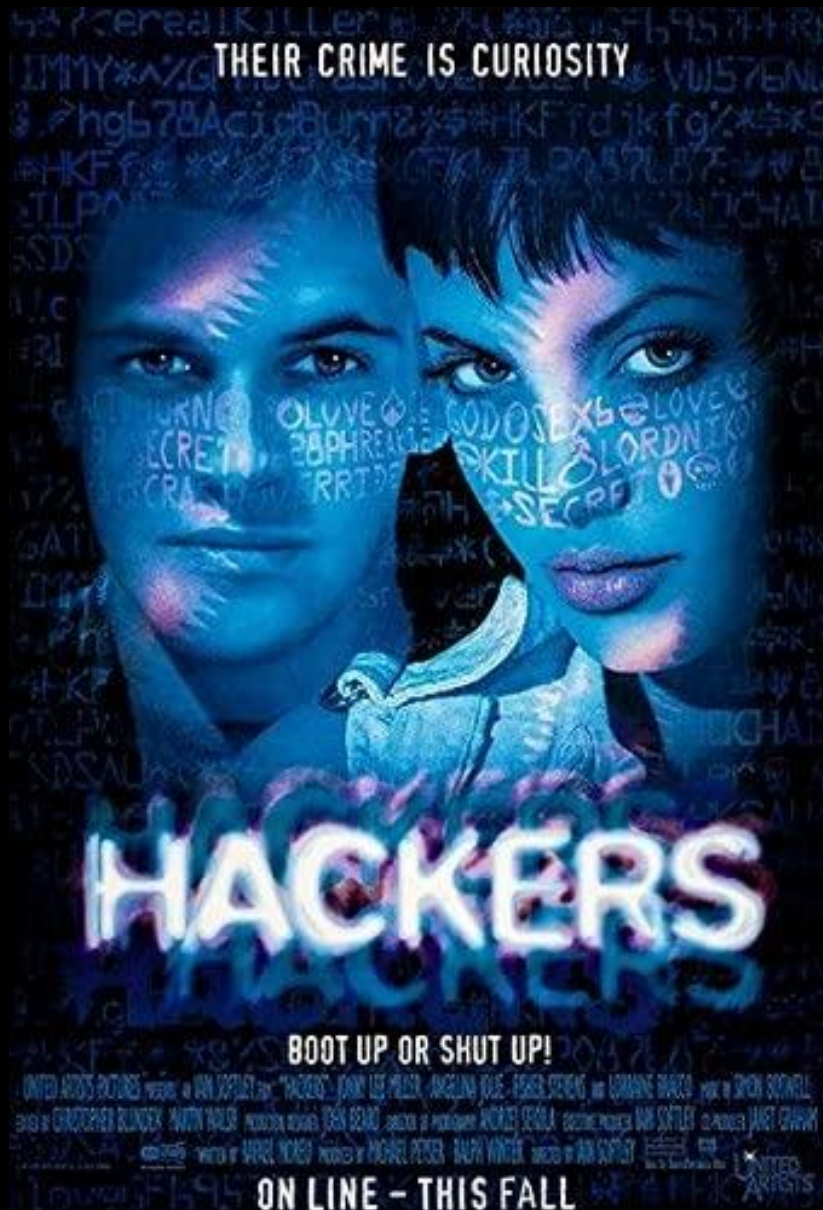
40 STORIES OF SHEER ADVENTURE!



This Photo by
Unknown Author is
licensed under [CC](#)
[BY-NC](#)

Credit: © & TM 20th Century Fox

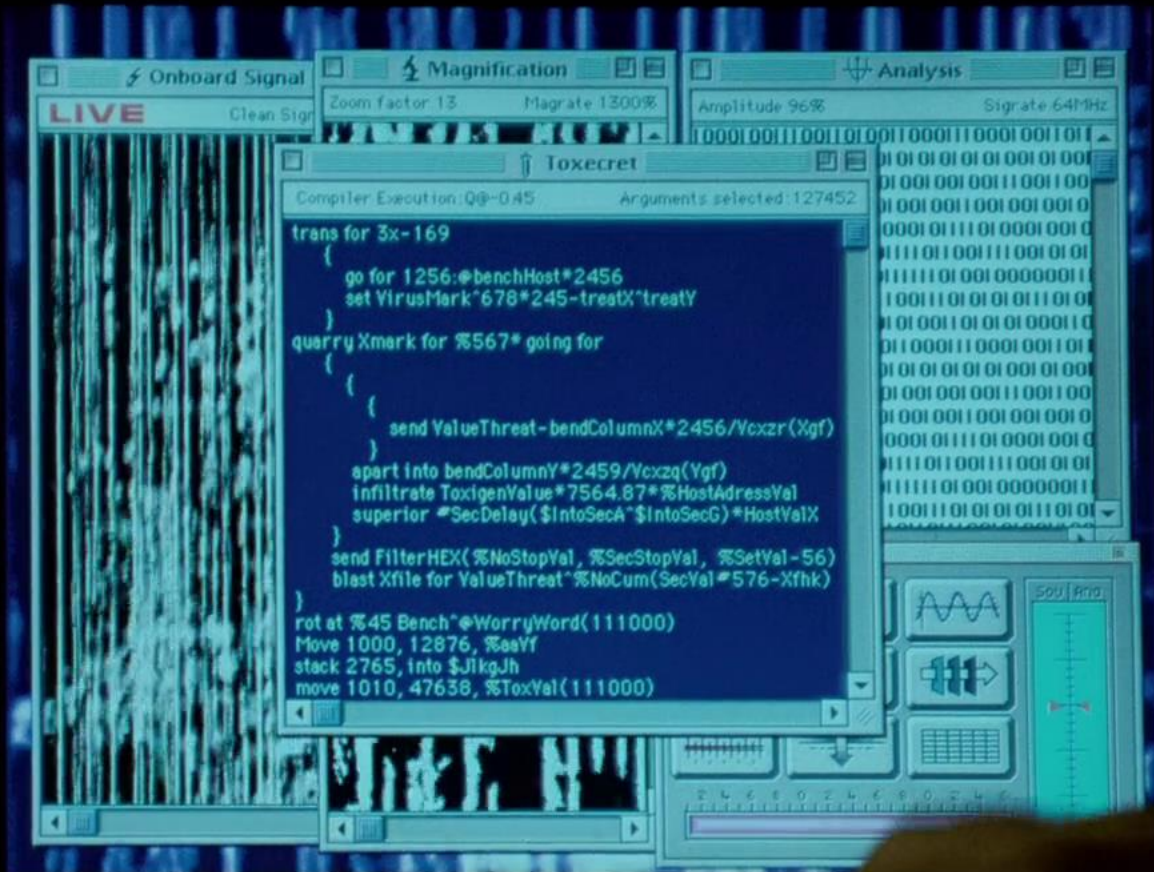
Hackers (1995): Physical World Impacts



<https://www.bbc.com/news/technology-40685821>

Credit: © & TM United Artists

Independence Day (1996): Secure your exposed systems!

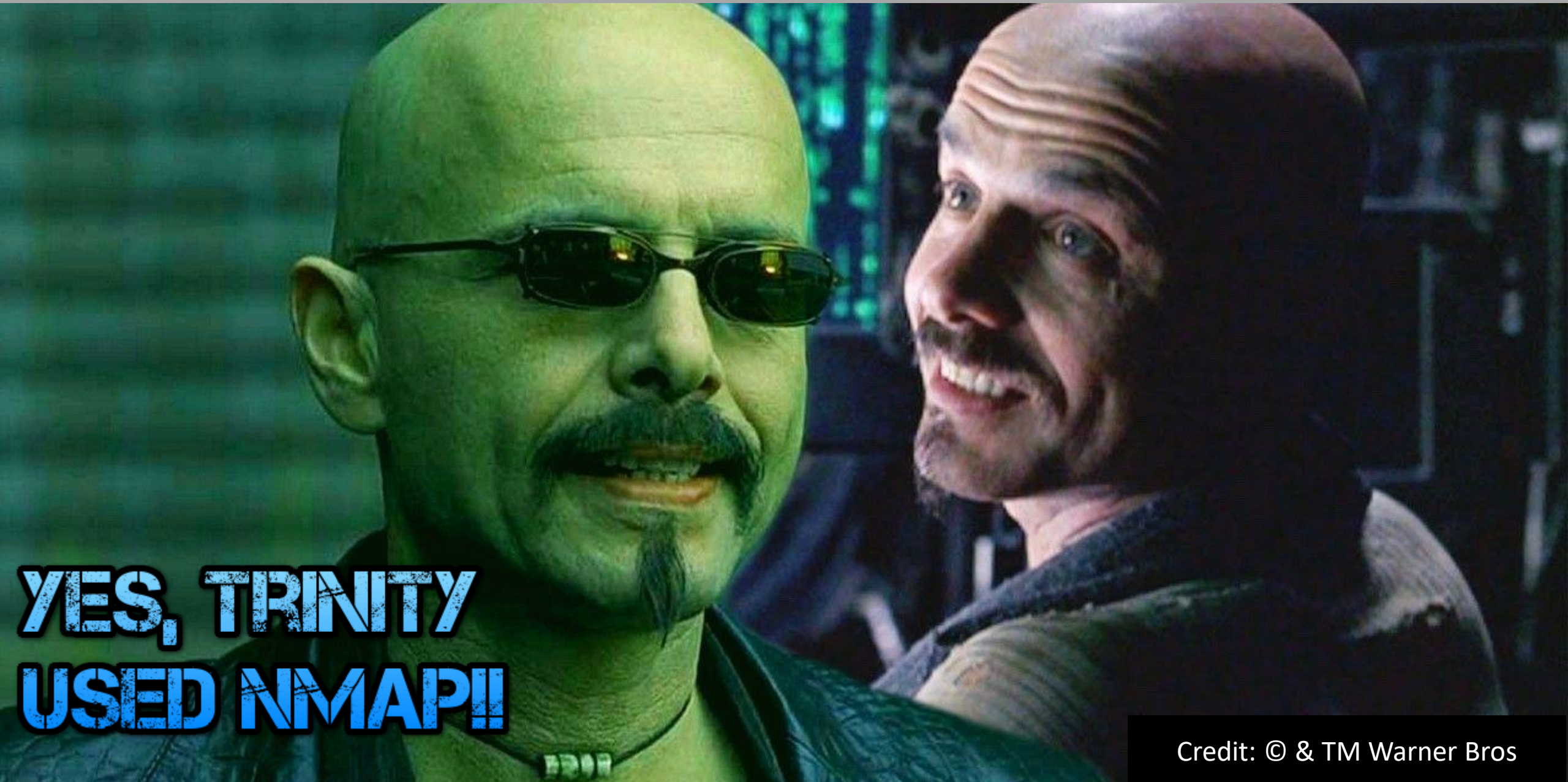


Office Space (1999): Salami Slicing



Credit: © & TM 20th Century Fox

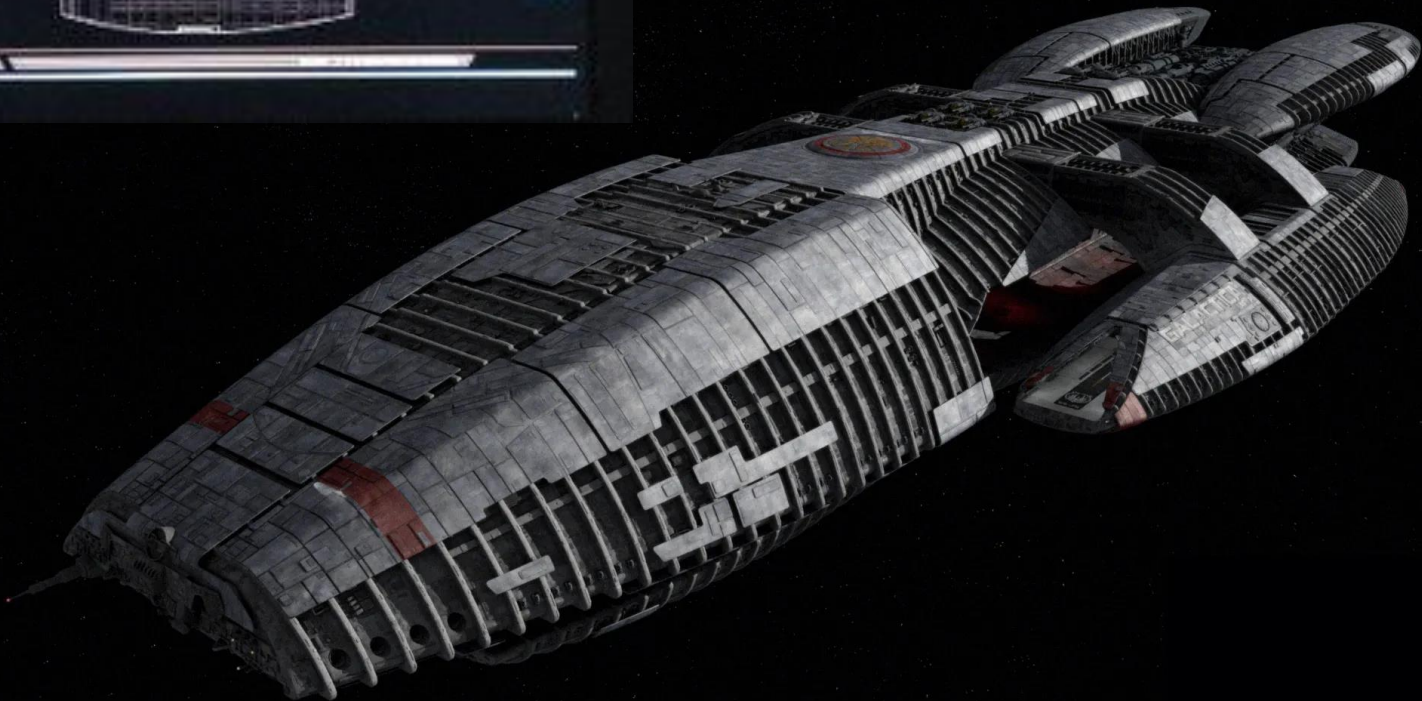
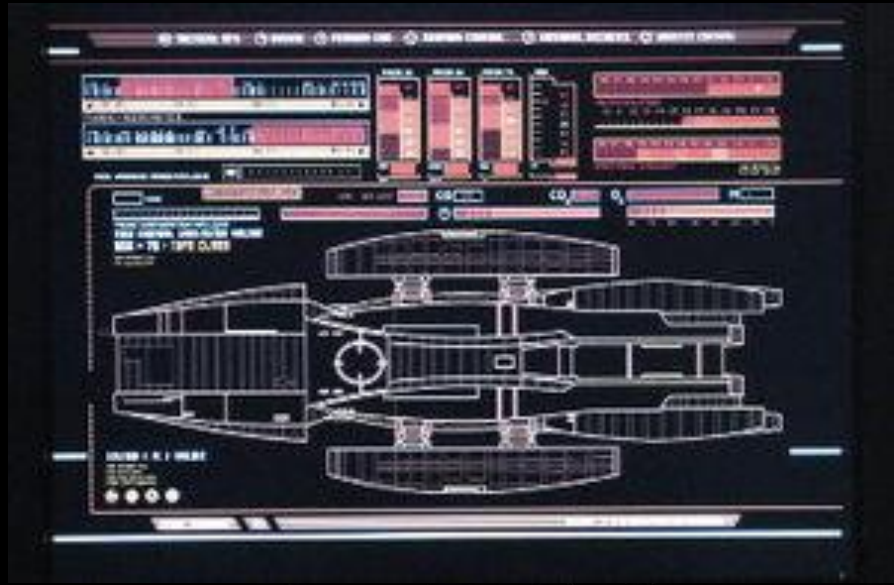
The Matrix (1999): Malicious Insider “Cypher”



**YES, TRINITY
USED NMAP!!**

Credit: © & TM Warner Bros

Battlestar Galactica (2004-09): Network Segmentation



Battlestar Galactica (2004-09): Networked = Hackable



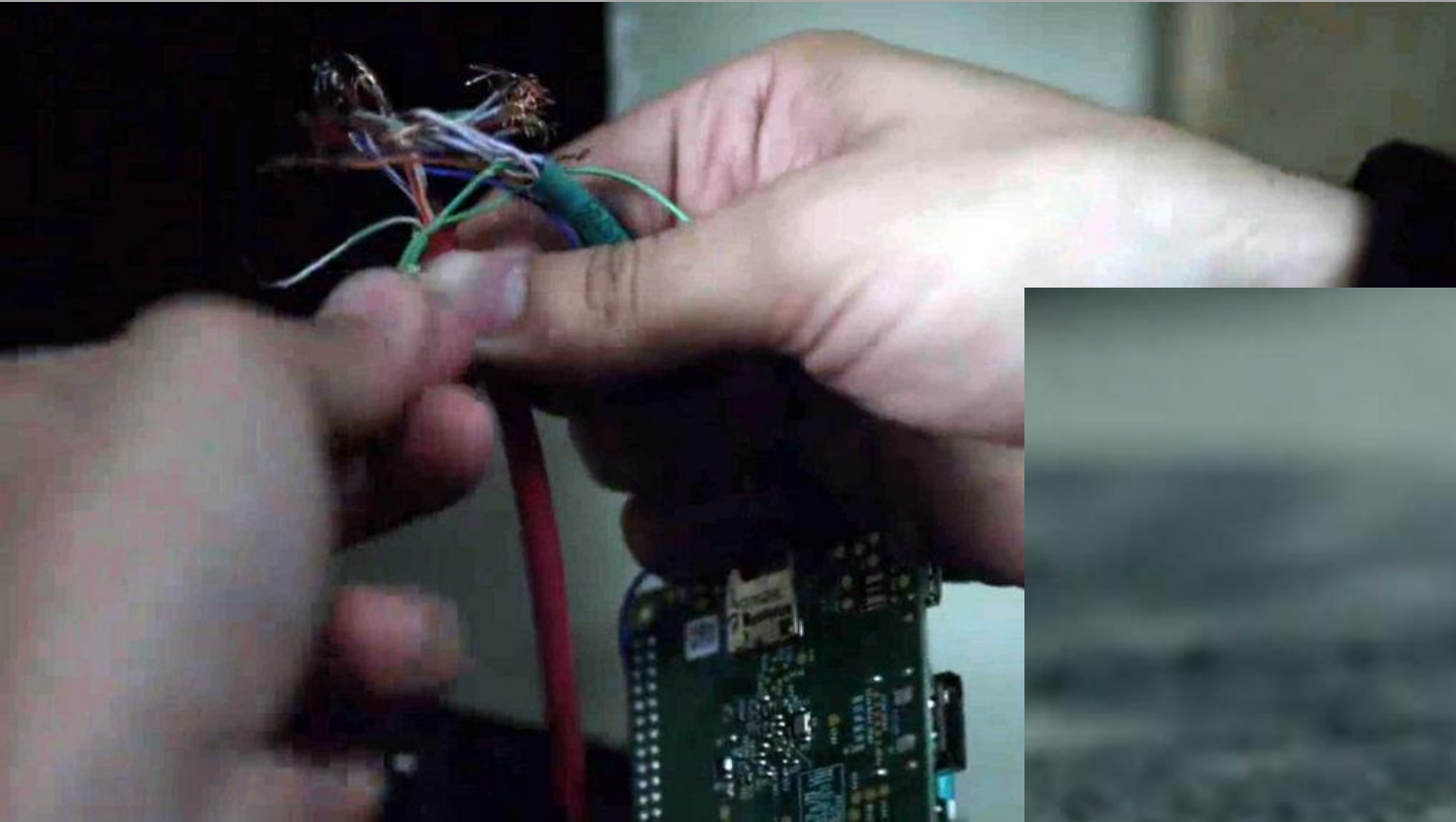
Credit: © & TM NBC Universal

G-Force (2009): Internet of Things / Supply Chain



Credit: © & TM Disney

Mr. Robot (2015-19): Physical Access and USB Drops



Credit: © & TM NBC Universal Television

The Orville (2017): Misinformation/Disinformation



Credit: © & TM Fox Television

Ready Player One (2018): Virtual Reality



Credit: © & TM Warner Brothers

Star Trek (1960s+): Change Your Passwords!



1-6-3-0-9

Credit: © & TM Paramount

Star Trek (1960s+): Deception / Honeypots & Nets



“No uncoded transmissions on an open channel...”



Star Trek (1960s+): Defense-in-Depth & Perimeters



SHIELD STATUS: PRIMARY SYS ACTIVE
GRAVITON FIELD OUTPUT: 625 MCH
SHIELD MODULATION: 257.4 MHz

SHIELDS  **UP**

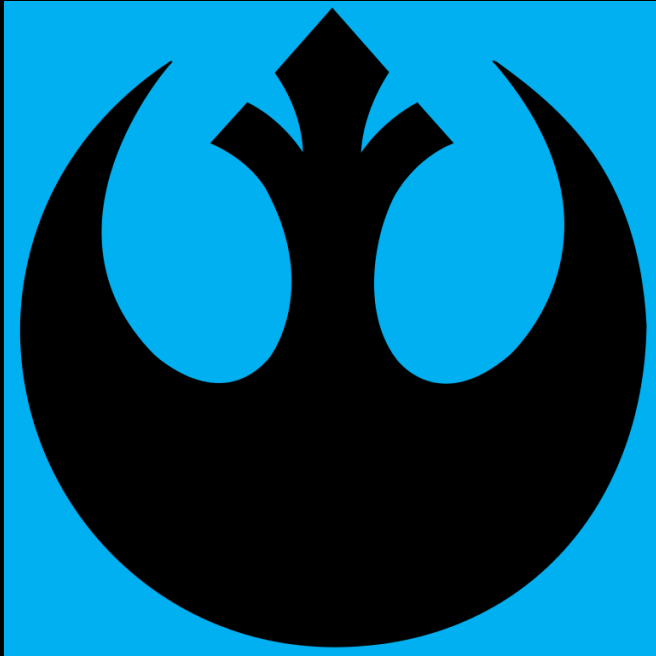


<https://www.cisa.gov/shields-up>

Credit: © & TM Paramount

Star Wars (1970s+): Good, Bad, & Gray Spaces

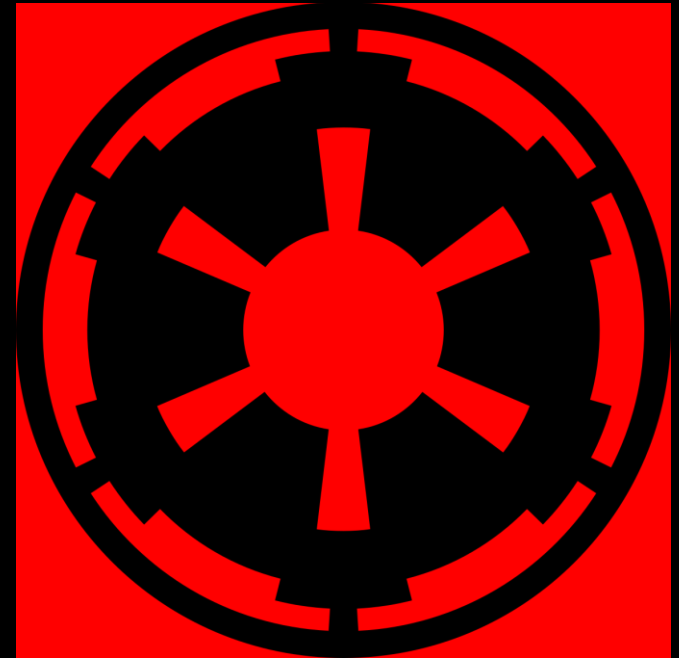
Blue Space (Good)



Gray Space (Internet)



Red Space (Bad)

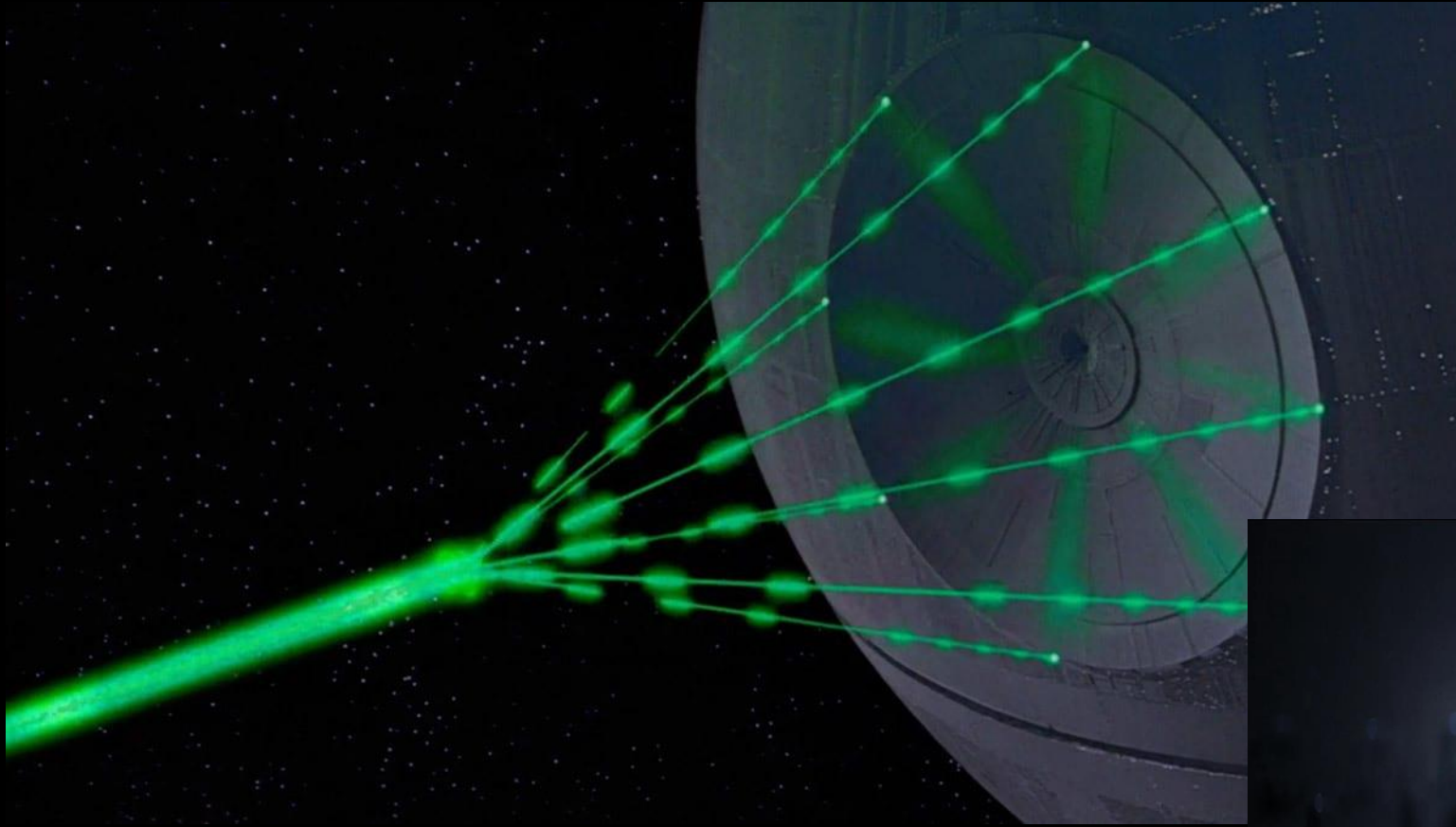


Star Wars (1970s+): Tools & Intent



Credit: © & TM Lucasfilm/Disney

Star Wars (1970s+): Vulnerabilities & Insiders



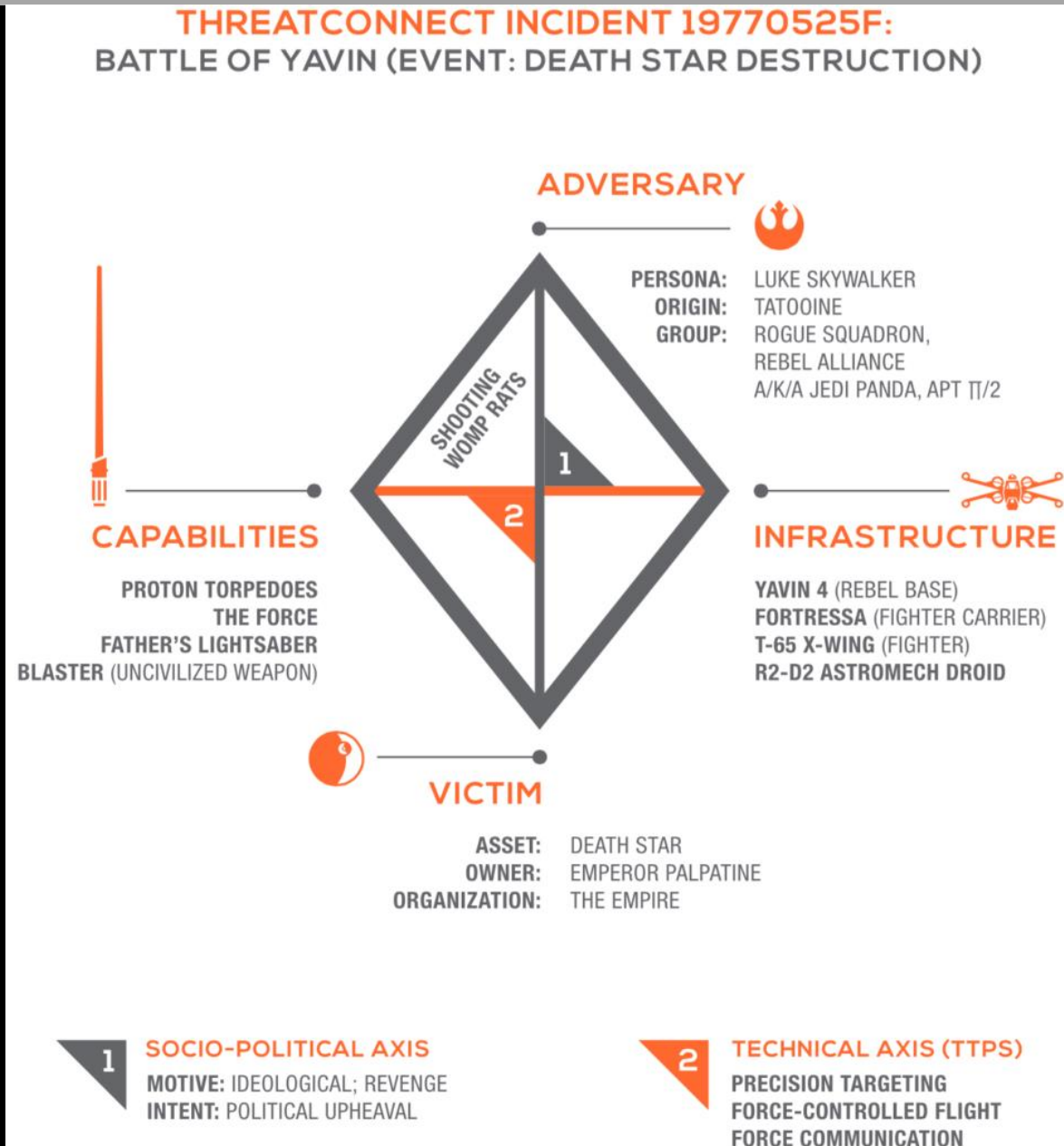
Credit: © & TM Lucasfilm/Disney

Star Wars (1970s+): Tailgating, Social Engineering



Credit: © & TM Lucasfilm/Disney

Star Wars (1970s+): The Diamond Model



Reference:

<https://threatconnect.com/blog/diamond-model-threat-intelligence-star-wars/>

Credit: © & TM Lucasfilm/Disney

Closing Thoughts

Learning should be FUN!

Networked or not, it can be hacked

There is no perimeter

Defend in Depth

Don't trust Mandalorians

And finally...

... “Have you seen my stapler?”



Credit: ® Swingline



VetSec

Thanks & Q&A!

Happy to connect: <https://www.linkedin.com/in/brad-e-rhodes-cissp-issep-cism-gcih-1951ba7/>