AI and Industry Impact: Job Reorganization, Reskilling and Managing Transformation

By Rod Soto
www.rodsoto.net

$whoami

Over 15 years of experience in information technology and security. He has spoken at ISSA, ISC2, OWASP, DEFCON, RSA Conference,Hackmiami, DerbyCon, Splunk .CONF, Black Hat,BSides, Underground Economy and also been featured in Rolling Stone Magazine, Pentest Magazine, Univision, BBC, Forbes, VICE, Fox News and CNN.

Rod Soto was the winner of the 2012 BlackHat Las Vegas CTF competition and Red Alert ICS CTF at DEFCON 2022 contest. He is the founder and lead developer of the **Kommand && KonTroll/NOQRTRCTF** competitive hacking Tournament series.

Secretary of the board of Hackmiami %27, Co-founder of Pacific Hackers Silicon Valley meetup. Founder & President Pacific Hackers Conference www.phack.org.

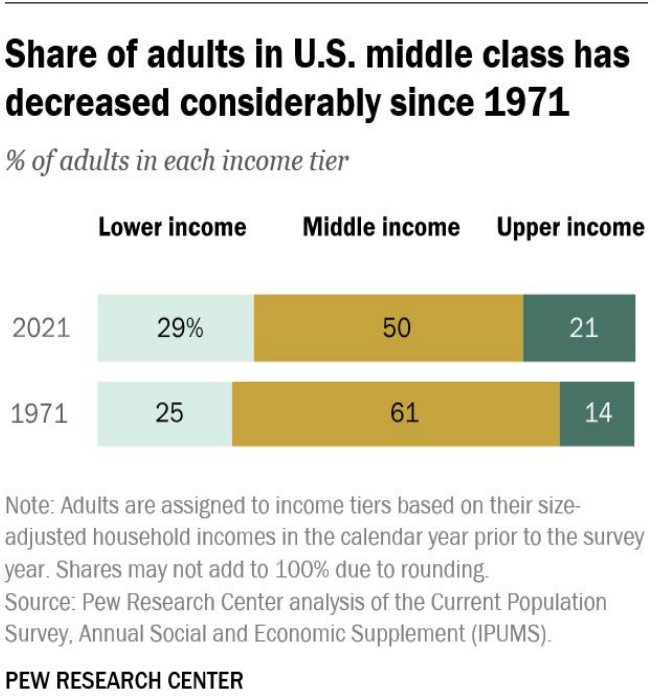
www.rodsoto.net

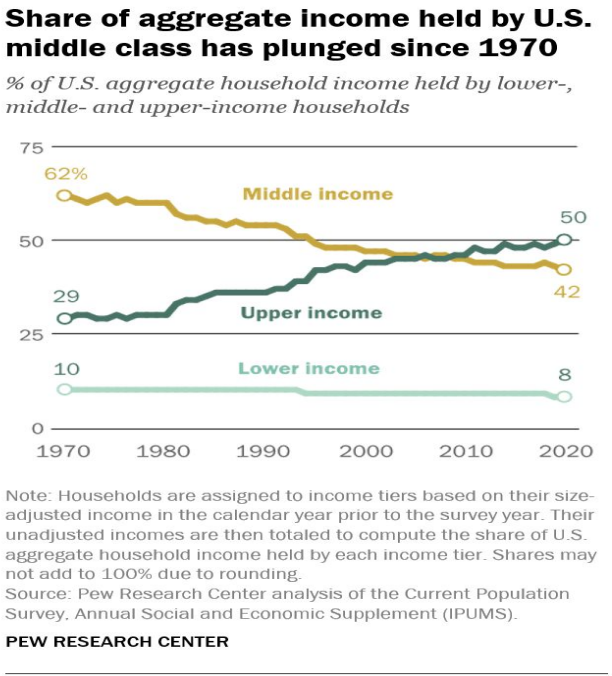
AI already transforming industry

Chatgpt (November 2022)

- The global cybersecurity workforce growth has stalled, with only a 0.1% increase from 2023 to 2024, reaching about 5.5 million professionals.
- Layoffs in the cybersecurity industry seem to be part of a broader trend in the tech sector, with over 130,000 tech employees laid off across 398 companies in 2023.
- Notable Cyber security layoffs
    - Rapid7 laid off 18% of its workforce (about 470 jobs)[3]
    - HackerOne cut up to 12% of its workforce[3]
    - NCC Group laid off 7% of its staff[3]
    - Bishop Fox laid off 13% of its workforce (about 50 employees)[5]
    - Sophos laid off 10% of its global workforce (about 450 employees)

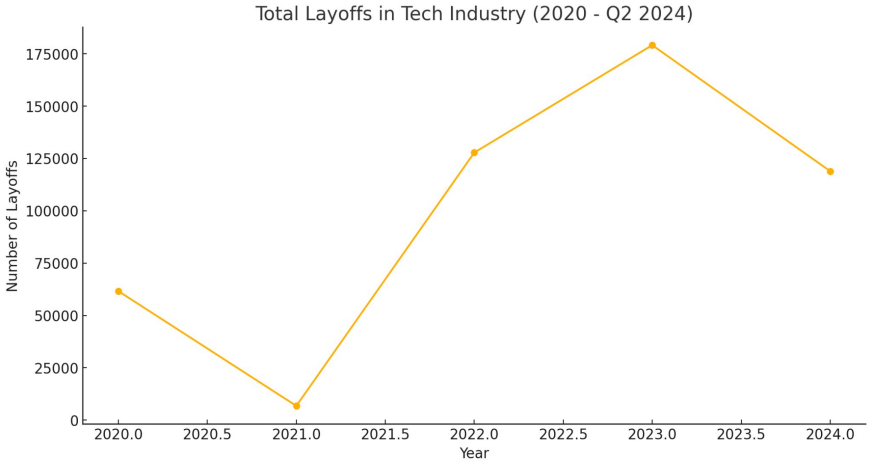
AI may increase wealth gap or shrink it… (yeah no)

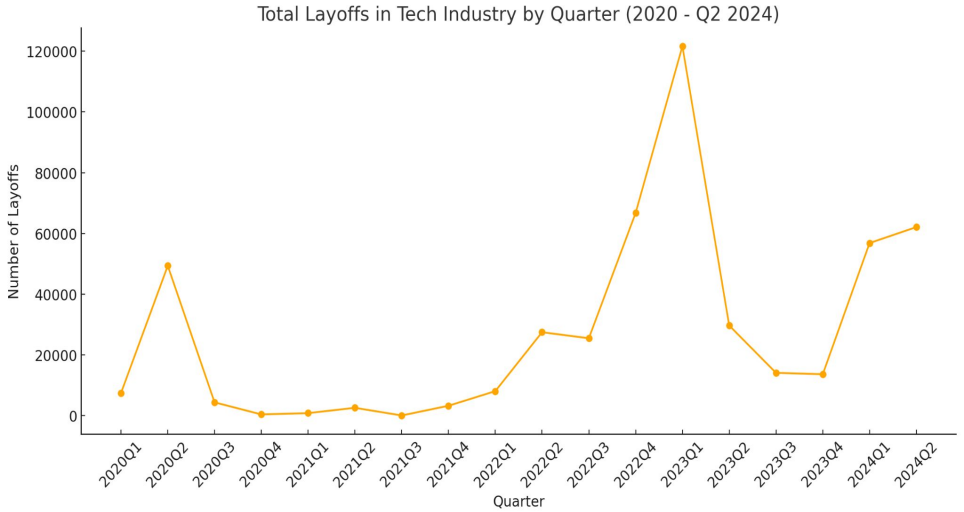


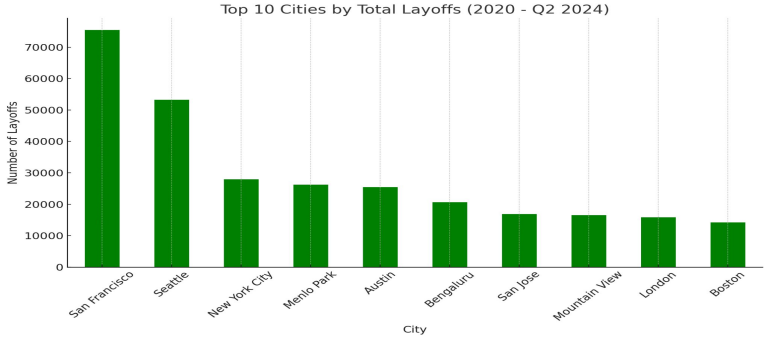


https://www.pewresearch.org/short-reads/2022/04/20/how-the-american-middle-class-has-changed-in-the-past-five-decades/

Tech Layoffs 2020 - Q2 2024 (Chagpt Nov 2022)





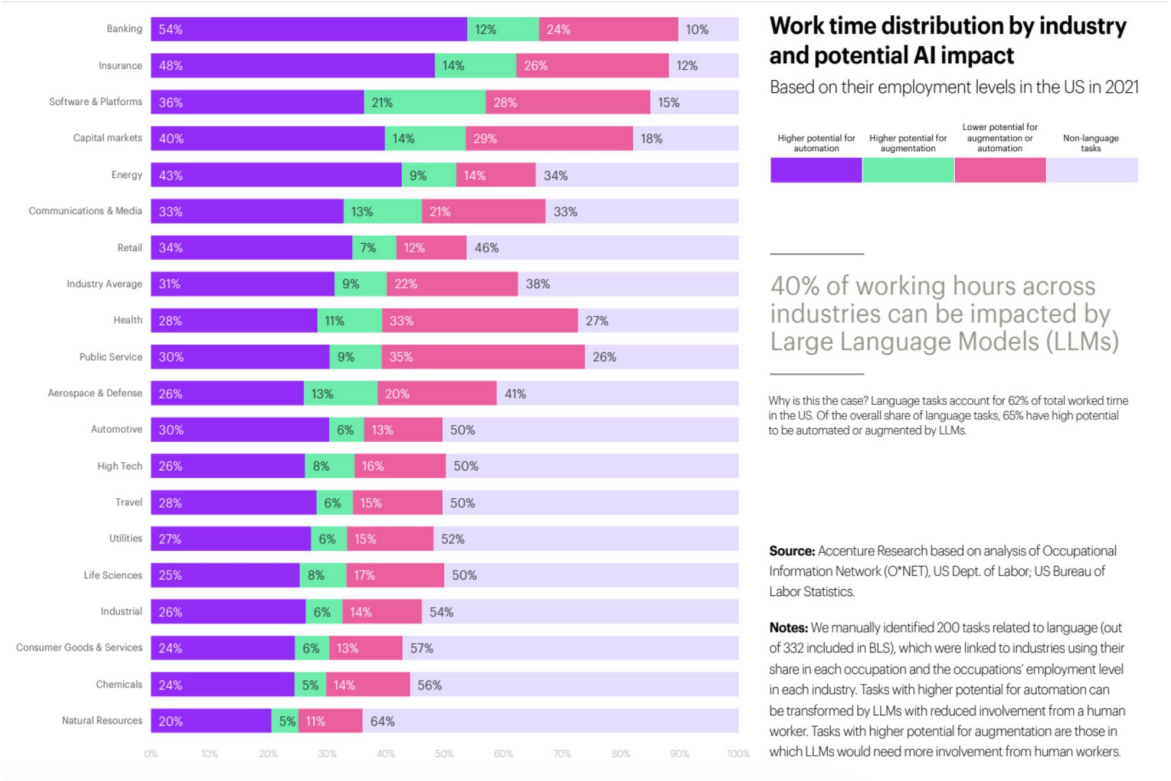


https://www.kaggle.com/datasets/ulrikeherold/tech-layoffs-2020-2024

AI Disruption in jobs

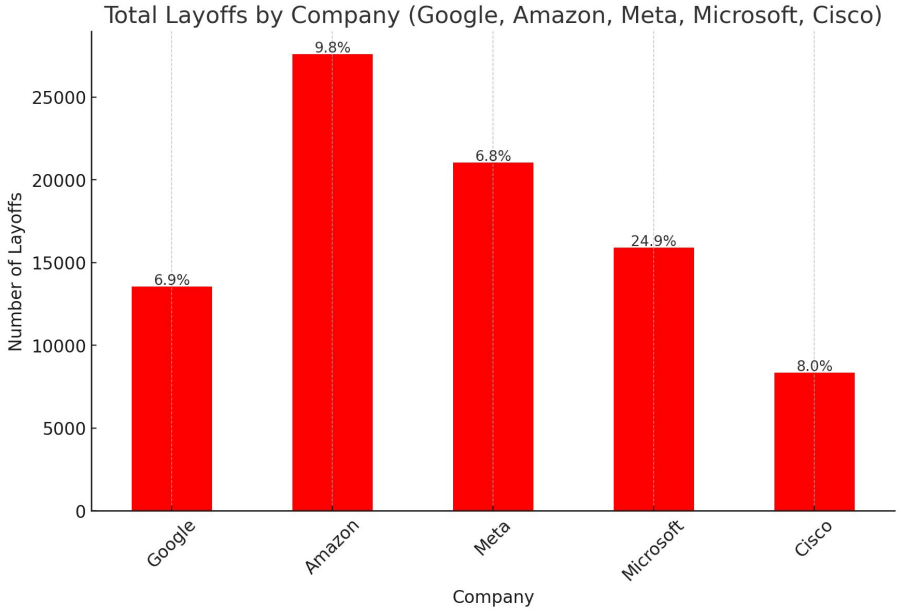
- Potential 300 - 400 MILLION JOB losses (Goldman Sachs, Mckinsey)
- Embodiment will only make these numbers HIGHER

https://www.weforum.org/agenda/2023/05/jobs-lost-created-ai-gpt/



What is the industry saying about AI and layoffs

- **Google.** Shifting focus to generative AI and reallocating resources
- **Microsoft.** Focus on defining the AI wave (Large investment in OpenAI)
- **Amazon** announced layoffs in its Alexa division, stating that it is "shifting some of our efforts to better align with our business priorities (Large Investment in Antropic creators of Claude LLM)
- **Meta**. A major goal will be building the most popular and most advanced AI products and services
- **Cisco.** Redirecting hundreds of millions of dollars into rapidly evolving markets, including AI.



AI + Crime is not the only thing you have to worry about…

Hyperscaler? What is that?

A hyperscaler is a large-scale data center operator that provides massive computing resources, typically in the form of cloud services.

Services Offered

Hyperscalers provide a comprehensive suite of cloud services, including:

- Compute and storage resources
- Database management
- Machine learning and AI capabilities
- Big data analytics
- Security services
- Content delivery networks

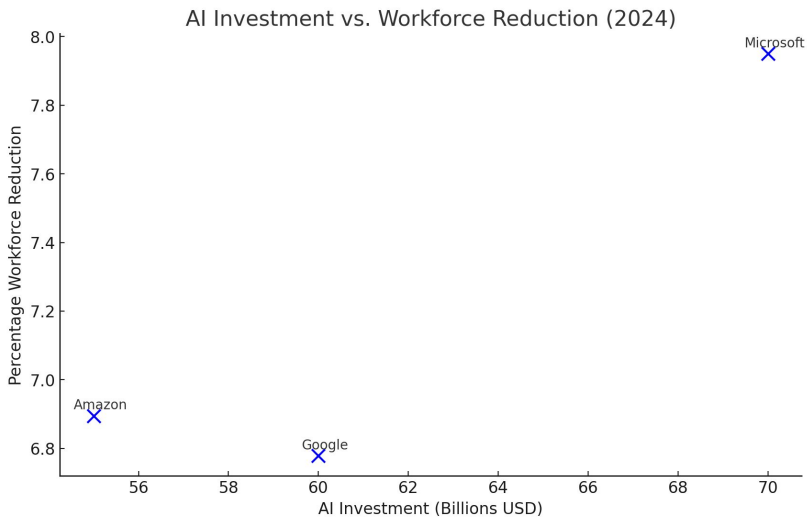
The leading hyperscalers in the market include:

1. Amazon Web Services (AWS)
2. Microsoft Azure
3. Google Cloud Platform (GCP)
4. IBM Cloud
5. Oracle Cloud

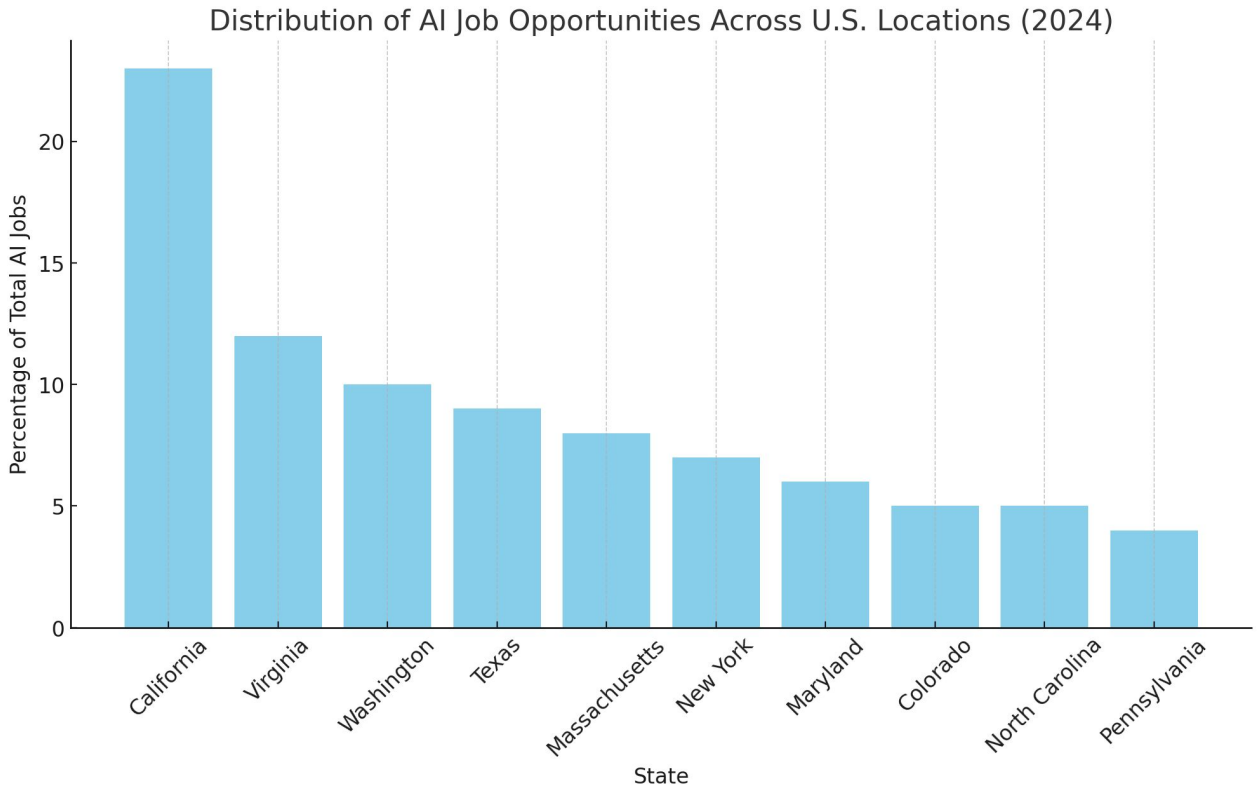
Are the hyperscalers hiring?

- IBM CEO Arvind Krishna stated that the company wouldn't be hiring while it shifted to AI
- AWS has been cutting jobs in certain areas while increasing investment in AI.
- Google has been laying off employees across multiple teams while increasing focus on AI
- Microsoft is still hiring for remote positions, with 883 fully remote jobs available as of August 2024

There is cleary hiring in AI with AI-related hiring making up over 10% of tech job posting. Current tech sector unemployment rate is 2.3% (October 2024).



Where are all these jobs located? - 2024 -



Skills sought in these jobs

Machine Learning and Deep Learning: Expertise in building and optimizing models, using frameworks like TensorFlow and PyTorch.

Generative AI and Large Language Models: Ability to work with algorithms that create text, images, or other data.

Data Science and Data Engineering: Skills in data analysis, processing, and pipeline creation. (Amazon SageMaker, DataBricks, SnowFlake, DataDog, Spark)

Natural Language Processing (NLP): Developing systems that understand or generate human language.

Software Development: Strong programming skills, especially in Python, R, or Java, Scala.

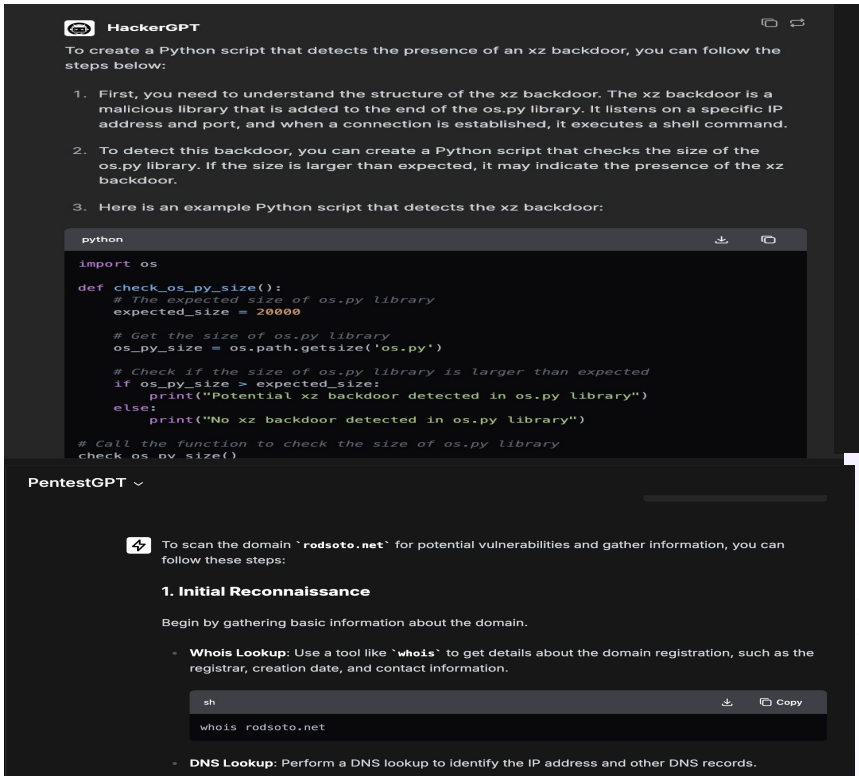
Higher exposure to AI doesn't necessarily harm workers' jobs, as long as they have the skills to use AI effectively. Occupations where computer use is high have seen **higher employment growth** despite AI adoption

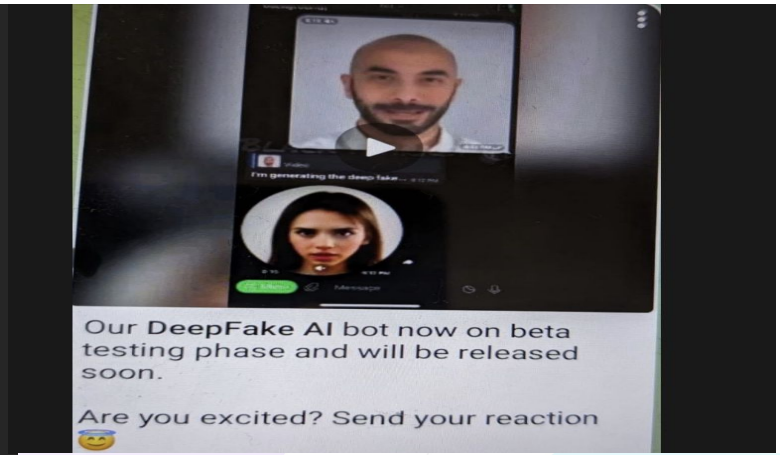
Ok this is a cyber security conference what about cyber?

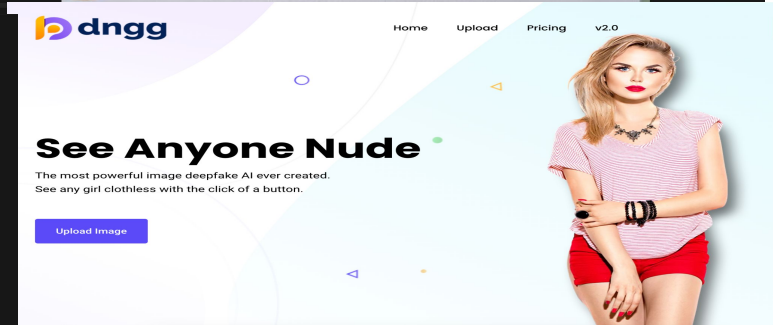
AI is here to stay…

- It is changing the way you do things, including those things we detect, fight and defend against
- It will put pressure on the job market (18-24 months)
- It requires the acquisition of “bridging” skills
- It will make obsolete many positions in the current market
- It will require those who work on it to have the knowledge the experience in security PLUS AI technologies
- It may not be that good for us…or at least some of us…(the numbers in the previous slides cleary shows it)

It is changing the way we attack, detect and defend







It clearly amplifies CRIME

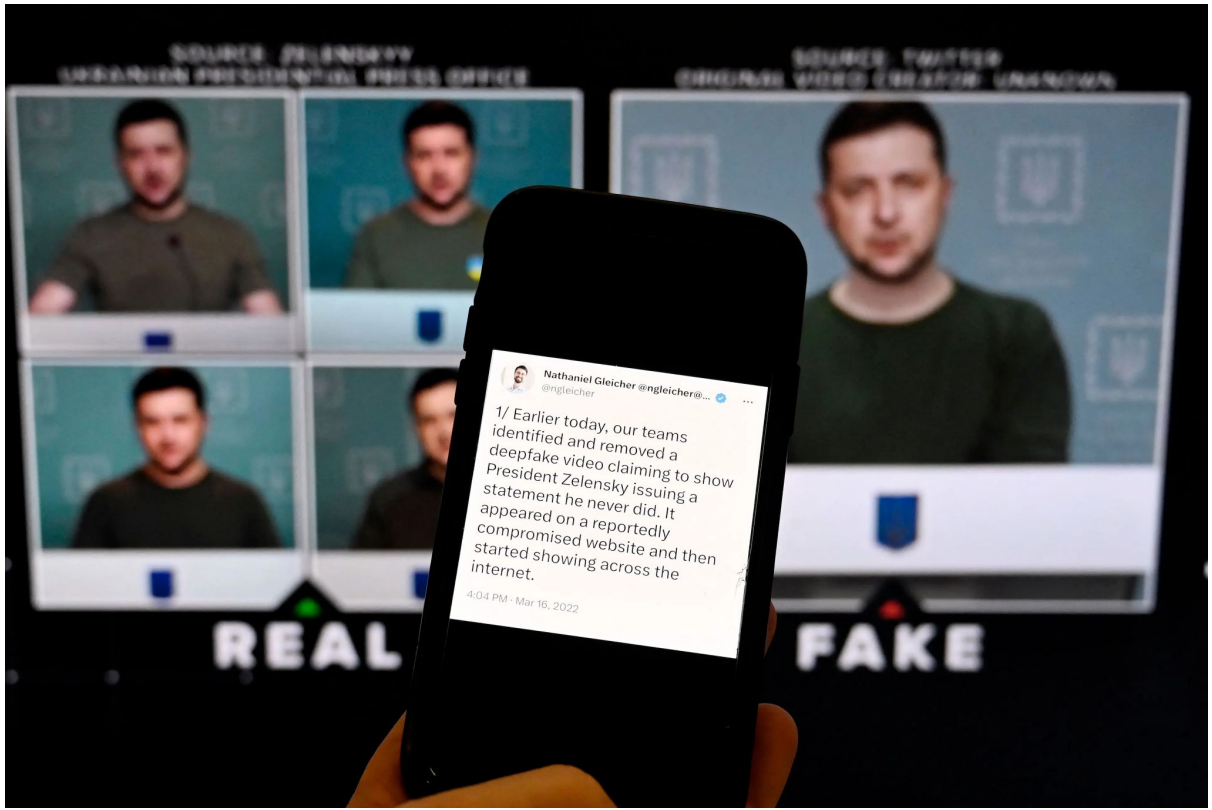
- Lowers the barrier for criminals (specially low level skills)
- Deep fake Videos and Voice cloning (Financial fraud, blackmail, fake kidnapping, disinformation)
- Since the fourth quarter of 2022 when ChatGPT launched, there's been a 1,265% increase in malicious phishing emails, and a 967% rise in credential phishing in particular, according to a new report by cybersecurity firm SlashNext
- Several cases of students using AI to target coeds or fake celebrity pr0n on social media
- Microsoft stated that it uncovered and obstructed attempts by malicious cyberattacks to utilize its AI technology
- Soon we will have to deal with the EMBODIMENT of AI and this will bring a new class of crime as well (drones, robots, vehicles, etc)
- The Google Cloud Cybersecurity Forecast 2024 sees generative AI and large language models contributing to an increase in various forms of cyberattacks. More than 90% of Canadian CEOs in a KPMG poll think generative AI will make them more vulnerable to breaches. And a UK government report says AI poses a threat to the country's next election.

Notable AI based campaigns

- AI-Powered Voice Cloning Scams. $25 million loss due to DeepFake impersonations (Hong Kong)
- AI enhanced phishing campaigns. There's been a significant increase in phishing attacks (47% increase from 2021 to 2022)
- AI Powered DeepFake romance scams, extortion and blackmail. (Between 2022 and 2023, deepfake sexual content increased by over 400%, and deepfake fraud increased by 3000%.)
- FAKE AI (FIN7 deep nude campaign, Fake Chatgpt json error X post)
- Creation of chatbots like WormGPT, FraudGPT, HackerGPT, and DarkBARD.(Most of them seem fake and fraud/scam)
- OpenAI reports several nation states researching technology, vulnerabilities and exploitation of critical infrastructure related technology

Fake ai

Deepfakes


REAL
FAKE
Nathaniel Gleicher @ngleicher@...
@ngleicher
1/ Earlier today, our teams identified and removed a deepfake video claiming to show President Zelensky issuing a statement he never did. It appeared on a reportedly compromised website and then started showing across the internet.
4:04 PM · Mar 16, 2022

AI presents a challenge to all of us in Cybersecurity

AI presents several challenges in cybersecurity, including:

1. **Adversarial Attacks**: AI models, especially in machine learning, can be manipulated through adversarial attacks where small perturbations in input data deceive the model into making incorrect predictions. This vulnerability can be exploited to bypass security measures such as facial recognition or malware detection.
2. **Data Quality and Availability**: Training AI systems requires large, high-quality datasets. In cybersecurity, these datasets need to represent real-world threats accurately. However, collecting and labeling data for cybersecurity use cases is challenging because threats evolve rapidly, and labeled datasets may quickly become outdated.
3. **Explainability and Trust**: Many AI models, especially deep learning systems, function as "black boxes" that lack transparency. This can make it difficult for cybersecurity teams to understand how a model arrives at its decisions, limiting trust in AI-driven security measures. Explainable AI techniques are needed to make AI decisions more interpretable.
4. **Automation vs. Human Expertise**: While AI can automate many security tasks, it is not a complete replacement for human expertise. AI systems may struggle with nuanced decision-making, such as determining the intent behind a threat. There is also a risk that over-reliance on automation could reduce human involvement in critical security tasks.
5. **Ethical and Privacy Concerns**: The use of AI in cybersecurity may raise privacy issues, especially when monitoring user behavior or analyzing sensitive data. Ethical considerations also arise with AI-based surveillance tools or automated decision-making systems that could impact individual rights.
6. **Weaponization of AI by Cybercriminals**: As AI becomes more accessible, cybercriminals are using it to enhance their attacks. AI can be used to create sophisticated phishing campaigns, automate malware distribution, or develop evasive techniques that bypass traditional defenses

*If we do not understand the basic functionings of AI we cannot protect it and we will fail in our jobs

What can YOU do NOW? - Keywords RE-SKILL - UPSKILL

- Evaluate your current technical skills in relation to AI/ML (Identify skill gaps)
- It is likely that you will have to acquire skills in programming languages relevant to AI (Python, R, Java, Scala).
- Security of the platforms that run AI (AWS, GCP, Oracle, Azure, DataBricks, Spark) - “Hyperscalers”
- Understanding of algorithms and machine learning principles.
- Data analysis and modeling skills.
- Soft skills focusing on critical thinking and problem-solving in AI contexts.
- Effective communication with AI teams and stakeholders.
- Continuous learning and adaptability to new AI trends.

Create a path in your career that targets the above

Pathways **to acquire AI Skills**

Formal/Informal Education and Training

- Degree programs and certifications in AI and related fields. (Berkeley, UT, MIT)
- Online courses and workshops (webinars).
- Self-Directed Learning (Youtube, Amazon,GCP, Azure, https://arxiv.org/, DataBricks)
- Learning resources (books, online tutorials, forums).
- Projects and hands-on experience. (Fork and create your own projects i.e Github)
- LEARN PYTHON (mandatory) www.edube.org
- Networking and Community Engagement
- AI conferences, seminars, and meetups.
- Joining AI-focused online communities and groups.
- Play with the available FREE local models (Ollama, GPT4All)
- Play with the ones online (Chatgpt, Perplexity, POE, Microsoft Copilot, Grok)

But wait not all of us can work at hyperscalers can we?

Frontier Models (Models trained on 10^26 FLOPS)

- Training a model at 10^26 FLOP would cost more than $100 million
- This cost threshold serves as an additional regulatory barrier
- Current frontier models are mainly driven and trained by Hyperscalers

Current Frontier Models (October-2024)

- GPT-4 Turbo (OpenAI) - Microsoft, Apple
- Claude 3 (Anthropic) - Amazon
- Gemini Ultra (Google)
- Gemini Pro 1.5 (Google's latest release)
- Mixtral 8x22B (Mistral) Microsoft, Google, Amazon, Databricks
- Meta’s Llama 3.1 405B is considered "the first frontier-level open source AI model”

Very hard at this time and place to develop your own Model but you can look at Agents

LLM vs Agent

There will be plenty of opportunities of developing agents and all kinds of other vertical applications related to AI, specially in Cyber security.

Aspect	Large Language Model (LLM)	Agent
Primary Function	Generates human-like text based on input prompts; excels in language understanding and generation tasks.	Interacts with environments to perform tasks autonomously; makes decisions and takes actions to achieve specific goals.
Interactivity	**Reactive**: Responds to user inputs without initiating actions on its own.	**Proactive and reactive**: Can initiate actions based on goals or respond to changes in the environment.
Learning Ability	Typically does not learn from new interactions unless retrained; relies on pre-trained knowledge.	Can learn from interactions in real-time, adapting to new information or changes in the environment.
Environment	Operates within the scope of language and text; does not interact with the physical world.	Operates in both virtual and physical environments; may interact with software systems, hardware devices, or the physical world.
Goal Orientation	Does not have inherent goals; aims to produce the most statistically probable text continuation based on input.	Operates towards specific goals set by designers or users, optimizing actions to achieve desired outcomes.
Examples	**LLMs**: GPT-4, BERT, RoBERTa; used for tasks like text generation, translation, and summarization.	**Agents**: Virtual assistants (like Siri or Alexa), autonomous robots, trading bots, game AI characters; perform tasks like navigation and strategic planning.

Proactive Learning & Adaptation

- We must approach and engage AI despite the uncertainty
- We must provide critical and sound feedback of it uses and abuses
- AI is fallible as we have seen in recent news, it is important to educate those in power to understand the reach and shortcomings of it
- This technology evolves incredibly fast. Be prepared to re learn and acquire new skills even if you are current.
- Most of all do not fear these things, they are still far away from being sentient, they are at best stochastic parrots.
- Remember you are human, there is nothing wrong with supporting humans… (AI should augment Humans not discard them - i.e Exoskeleton vs Robot).
- Even if you do well there will be significant effects of AI on society (i.e millions of people either transitioning careers or jobless for some time).
- Finally No time like the present, try to enjoy it.

“High tech low life” refers to a cultural concept that captures the contrast between advanced technology and societal decay. Here are the key aspects:

Core Elements

- Advanced technology coexisting with social deterioration
- Cutting-edge innovations alongside marginalized individuals
- Stark contrast between technological progress and human struggle

Key Characteristics

- Urban settings featuring advanced technology like:
- Artificial intelligence
- Cybernetic enhancements
- Digital networks
- Social elements including:
- Economic disparity
- Corporate dominance
- Urban decay
- Marginalized populations

Q&A

Thank you

Rod Soto

X - @rodsoto

www.rodsoto.net