# 1AC

### We affirm. 6 benefits

## 1---Safety (45)

#### There are a lot of shootings Liberman 24

Liberman 24, Mark Lieberman & Hyon-Young Kim12-31-2024, "School Shootings in 2024: More Than Last Year, But Fewer Deaths," Education Week, https://www.edweek.org/leadership/school-shootings-in-2024-more-than-last-year-but-fewer-deaths/2024/12, Mark Lieberman is a reporter for Education Week covering school finance. He previously covered technology and online learning for Education Week and, before that, for Inside Higher Ed. Before that, he reported on DC-area local news for the Current Newspapers and the Washington Post Express. His work has also appeared in Poynter, Vulture, Vox, IndieWire, The Week, USA Today, and Vice. He graduated in 2015 from the American University School of Communication with a bachelor’s degree in journalism. Hyon-Young Kim is senior digital news specialist for Education Week. She graduated from Johns Hopkins University with a degree in English and Classics, and began working at Education Week in 2014 after earning a master’s degree in journalism from the University of Maryland, College Park. accessed 2-19-2025 //wyatt G?//

The overall number of school shootings in 2024 that resulted in injuries or deaths slightly outpaced last year’s tally, according to Education Week’s school shootings tracker. Thirty-nine school shootings this year met the criteria for Education Week’s tracker—the second-highest total for any year since Education Week began tracking these incidents in 2018. Gun violence in and around schools weighs heavily on students and staff, close families and extended relatives, nearby neighbors, and the entire nation. This is true whether the event generates weeks of headlines or a stray news article; whether no one dies or many people do; and whether it’s been 25 minutes since the last incident or 25 years. Education Week began tracking school shootings in 2018, just two weeks before the mass school shooting in Parkland, Fla., in which 14 high school students and three adults died. Since then, EdWeek has counted 221 school shootings, as of Dec. 31, 2024. The tracker counts incidents in which at least one person other than the individual firing the weapon is injured by gunfire on school property when school is in session or during a school-sponsored event. Of the 39 shootings this year, more than two-thirds took place outdoors on school grounds, where administrators and security personnel typically have a harder time intervening when trouble arises. At least one school shooting took place in the United States every month this year. Mass shootings in 2024 outpaced last year, but not 2022 Four school shootings this year met the Gun Violence Archive’s definition of a mass shooting—in which four or more people other than the shooter died or were injured by gunfire. That’s three more than in 2023, but five fewer than in 2022, when nine mass shooting incidents took place—the most in a single year since EdWeek began tracking school shootings in 2018. The first mass school shooting in 2024 took place just four days into the calendar year, when a 6th grade student died, four more students were injured, and three staff members were injured in a shooting at Perry High School in Iowa. One of the injured staff members, the school’s principal, died 10 days later from injuries he sustained during the incident. Exactly eight months later, two students and two teachers were shot and killed by a 14-year-old student at Apalachee High School in Georgia. The incident had more casualties than any other school shooting in 2024—in addition to the four deaths, nine people were injured. Two of the four mass shootings in schools this year took place in Georgia. Separate from the Apalachee incident, four students were shot and injured on Feb. 14 at Benjamin E. Mays High School in Atlanta. The year’s last mass shooting took place just nine days before Christmas, on Dec. 16, at the Abundant Life Christian School in Madison, Wis. One teacher and a 14-year-old student were killed, and six other people were injured. Dozens of people were shot on school grounds this year Nationwide, 18 people died and 59 others were injured this year in instances of gun violence in and around schools. The number of deaths is lower than in the previous two years, but more than double the tally in 2019, when eight people died in school shootings nationwide. That number is lower than in any other year since EdWeek began tracking school shootings, aside from 2020, when school buildings nationwide were closed for much of the year. The total number of casualties—injuries and deaths combined—is higher than in 2023, but significantly lower than in 2022, when 140 people were injured or killed in a school shooting, according to the tracker. Shootings from prior years continued to make news in 2024 This year marked the 25th anniversary of the Columbine High School massacre, in which 12 students and one teacher were killed. That incident laid the groundwork for much of the school safety apparatus students, staff, and families across America now regularly confront in schools. It also spurred a tidal wave of billions of dollars in new expenses schools have incurred in well-intentioned—though sometimes insufficient or ill-advised—efforts to keep people safe. Years after a shooting takes place, answers to key questions and solutions to prevent further violence often remain frustratingly elusive. In January, a U.S. Department of Justice review found that a faster police response to the 2022 mass shooting in Uvalde, Texas, could have saved lives. Earlier this month, a judge denied a motion to dismiss criminal charges filed in July against two of the 376 officers involved in the Uvalde response. A trial over those charges is tentatively set for October 2025—29 months after the incident took place. None of the 374 other officers who responded in Uvalde, where two teachers and 19 elementary school students died, has been charged with a crime. School shootings also have ripple effects that go well beyond the immediate consequences. Schools across the country faced an uptick of violent threats in the days following the Apalachee High School shooting in Georgia. Most of those threats turned out to be unfounded or not credible—but even so, they take an emotional toll on all who respond to them.

#### , security camera analysis abuhassan 24

Hussein Abuhassan 24, August 5th 2024, "AI Security: Safeguarding Schools Beyond Surveillance," No Publication, https://www.securitymagazine.com/articles/100883-ai-security-safeguarding-schools-beyond-surveillance, accessed 2-19-2025 QUAL-Hussein AbuHassan is a prominent figure in the security industry, known as the President and Founder of the Law Enforcement Network (LENX), where he focuses on enhancing public safety through innovative solutions. He has over 20 years of experience in information technology and security. //wyatt G?//

Surveillance cameras have been a core component of safeguarding schools for decades by extending the capabilities of school security officials, allowing them to monitor activity across school campuses from a centralized location. Recent surveys show that 91% of schools now rely on surveillance cameras to support their security efforts. However, as security threats have evolved, surveillance systems have struggled to keep pace. The number of threat events has increased significantly over the past decade, putting much higher demands on security personnel. In 2023, for example, there were more than 346 school shooting incidents in the United States. By comparison, there were only 34 incidents in 2013. To bring surveillance systems up to date, schools are beginning to explore the potential of artificial intelligence. Integrating AI with modern surveillance results in proactive warning systems that strengthen schools’ security measures, giving them the capability to address far more than just immediate threats. Enhancing security with proactive threat detection Traditional surveillance systems allow security personnel to passively watch as threats unfold, and while they extend the reach of security systems, they don’t empower proactive threat detection. AI transforms traditional systems by giving them the capability to proactively analyze, interpret and respond to potential threats in real time by injecting intelligence into existing systems to enhance and fortify the security they can offer. Automated weapons detection is one of the key capabilities that AI brings to surveillance. AI systems are trained on vast datasets, empowering sophisticated algorithms that can recognize the visual signatures of virtually any weapon. Size, shape and material composition can reveal the presence of a weapon even before it is visible in its entirety. AI’s advanced visual recognition capabilities also allow for potential threats to be assessed in the context of their surroundings, meaning it won’t simply sound the alarm when someone carries any metal object into a classroom. As an intelligent sentinel, AI will first determine if the object is a wrench in the hands of a custodian or a gun in the hands of a potential shooter. Extending security beyond threat detection The capabilities of AI-driven security do not end with automated threat detection. AI empowers a holistic approach to security by identifying and mitigating risks, as the security training provided to AI allows it to detect anomalies in the school environment and monitor the school for signs of weapons as well as any unusual or unexpected behavior that might indicate a safety concern. For example, AI can learn the normal traffic patterns in school hallways, allowing it to identify when the movement of a student is normal and when it is suspicious. It can even identify anomalies like doors that are closed when they should be open or lights that are off when they should be on. Rather than simply log this activity as traditional surveillance systems do, AI can identify them as a safety concern and reach out appropriately. Advanced training can allow AI to assess the data it gathers through surveillance systems to identify potential weaknesses. If access policies create security vulnerabilities, AI can identify them and make suggestions for improving security. If security policies are being ignored, AI can detect violations and alert security personnel to the need for more effective training. Empowering effective security responses Adding AI to conventional surveillance systems also improves their capability for facilitating an effective security response. When a threat is detected, AI can trigger notifications to all appropriate personnel, including school security staff, teachers, administrators and any other officials as predetermined by the school’s security team. AI enhances the security response in several ways. First, it provides clear communication that is not adversely affected by emotions or unclear thinking. Even for the most seasoned security professional, an active shooter situation can be unnerving. AI is not rattled by a threat, allowing it to quickly and clearly communicate the situation as it is detected. AI systems also improve security response by providing dynamic video or photos of the threat until it is addressed. This allows security personnel to see exactly what has triggered concern and to track the concern as it moves through the school. Surveillance will always be a crucial component of school security, but without the advanced capabilities AI integrations provide, traditional surveillance methods will struggle to address the modern threat landscape. AI transforms conventional surveillance into a modern tool that can detect and address the threats that challenge today’s school security frameworks.

#### AI helps understaffed districts ly 24

Ly 24, October 23 2024,David Ly "AI in School Security: Empowering Understaffed Districts Amid Growing Threats," Campus Safety Magazine, https://www.campussafetymagazine.com/insights/ai-in-school-security-empowering-understaffed-districts-amid-growing-threats/162466/, David Ly is the CEO and founder of Iveda, a company that specializes in AI-based video surveillance and smart city technologies. He has over 20 years of experience in wireless data and cloud video surveillance, focusing on enhancing public safety and security through AI innovations.accessed 2-19-2025 //wyatt G?//

As students get back into the groove of the school year, their safety — and the safety of teachers, faculty, and staff — has become more critical than ever. This is further compounded by school districts grappling with budget constraints and staffing shortages. Amid rising concerns surrounding school-related violence like shootings, bullying, and other threats, artificial intelligence (AI) is emerging as a powerful tool to support schools in real-time monitoring and response. Education-related AI — including school security use cases — is expected to become a $6 billion market by 2025, driven by its capacity to augment overwhelmed staff and offer heightened situational awareness. While promising, AI deployments in school settings also raise important questions regarding privacy, ethics, and the balance between safety and student rights. AI’s Expanding Role in School Security AI technology is playing an increasingly significant role in mitigating security risks in schools. From video surveillance systems powered by machine learning to facial recognition and predictive analytics, these tools allow schools to monitor campuses more effectively than with human staff alone. One of the key areas where AI is making a difference is in the early detection of threats. AI-driven systems can analyze surveillance footage and detect suspicious behaviors, such as individuals loitering near entrances or students showing signs of distress. These systems, equipped with pattern recognition, can alert school administrators and law enforcement in real-time, allowing for quicker intervention before an incident escalates. For example, AI can assist in identifying potential intruders or unauthorized persons on school premises. By integrating with cameras, AI algorithms can detect unusual movement or behavior patterns — as well as license plates that may not be allowed on school property — to send instant alerts to school security staff, even when human eyes might miss the warning signs. There are even technology options on the market that can be plugged into existing infrastructure, minimizing both overhead costs and time to deploy. Another critical use case for AI is monitoring social media for potential threats. AI can scan online activity for keywords and patterns that suggest an impending security incident, such as threats of violence or plans for disruptive actions. When flagged, these alerts can be forwarded to relevant authorities, ensuring early interventions. Addressing School Staffing Shortages with AI Many school districts are facing a shortage of security personnel due to budget constraints or hiring challenges. AI-powered systems can help bridge this gap by automating many time-consuming monitoring tasks that traditionally require human labor. This includes sifting through hours of surveillance footage, reviewing online content, and tracking student movements on campus. By taking over these functions, AI can allow existing security staff to focus on higher-priority tasks and respond more effectively to actual incidents. Worse yet, budget constraints mean that a good portion of schools across the U.S. do not have dedicated security personnel, meaning teachers and staff are the acting “security” on campus. In these scenarios, automation is crucial to addressing threats promptly and allows teachers to direct their full attention to what matters most: educating. AI solutions bring 24/7 surveillance capabilities to schools without requiring round-the-clock staffing. As a result, districts that might otherwise be unable to afford full-time security can still maintain a continuous watch over campuses, providing peace of mind to administrators, teachers, and parents at all hours. The Implications of AI in Schools While AI offers significant potential benefits for school security, its deployment also raises several concerns. The use of surveillance technologies, particularly facial recognition and behavior analytics, raises privacy issues for students and staff. Schools are entrusted with sensitive personal data, and AI systems increase the risk of breaches if not properly safeguarded. Additionally, overreliance on AI for monitoring can create ethical dilemmas, such as the potential for bias in facial recognition systems, which have been shown to misidentify individuals from minority groups at higher rates. Careful oversight, transparency, and appropriate safeguards are essential to ensuring that AI is used responsibly in schools, enhancing security while preserving the rights and well-being of students. It’s also critical that everyone — from students and parents to teachers and faculty members — are educated early and often on how the technology works and its purpose in order to mitigate fears and concerns. Striking the right balance between enhancing safety and maintaining a nurturing, trusting educational environment will be a key challenge for school districts deploying AI solutions. The Future of School Security AI is already proving to be a game-changer for school security, offering understaffed and overwhelmed districts a valuable tool to enhance student safety. With its ability to monitor campuses, scan for digital warnings of violence, and detect threats in real-time, AI can fill critical gaps in school security operations to create safer learning environments across the globe.

#### Shootings are devastating Abrams 23

Zara Abrams 23, 10-27-2023, "Stress of mass shootings causing cascade of collective traumas," https://apa.org, https://www.apa.org/monitor/2022/09/news-mass-shootings-collective-traumas, accessed 3-4-2025 //wyatt G?//

As mass shootings continue to erupt in schools, grocery stores, restaurants, and other public places and establishments we visit every week, Americans are living in fear. For children and teens, whose mental health is already in crisis, the ongoing backdrop of violence is steadily eroding the sense of well-being, safety, and efficacy known to be essential for healthy development. As of Oct. 26, there have been 566 mass shootings reported and verified in the United States in 2023, according to the Gun Violence Archive. The incidence of mass shootings in the United States is growing and is correlated with increases in gun sales (Newsome, K., et al., Journal of Surgical Research, Vol. 280, 2022). On top of recent surges in depression, anxiety, and suicides, a majority of teens now say they worry about a shooting happening at their school (Pew Research Center, 2018). Those concerns have been linked with elevated anxiety levels and fear among students (O’Brien, C., & Taku, K., Personality and Individual Differences, Vol. 186, 2022). Meanwhile, clinical psychologists, including Erika Felix, PhD, of the University of California, Santa Barbara, say the young people they treat are on high alert, constantly planning their escape route if violence breaks out in public. “These tragedies are happening far too often, and the result is that many young people are feeling this constant back-of-the-mind stress,” Felix said. That stress is, of course, embedded within the context of the pandemic, the conflicts in the Middle East and Ukraine, economic challenges, political polarization, climate-related disasters, and other factors, which combine to create what psychologist Roxane Cohen Silver, PhD, of the University of California, Irvine, calls a “cascade of collective traumas” that the nation is facing together. “We’re not starting at a place where everybody is healthy and thriving,” said Rinad Beidas, PhD, a professor of psychiatry, medical ethics and health policy, and medicine at the University of Pennsylvania’s Perelman School of Medicine. “Our reserves are depleted as a nation and our young people are suffering.” Fear of mass shootings has left a large majority of Americans feeling stressed, including a third of adults who say they now avoid certain places and events as a result (Stress in America: Fear of mass shootings, APA, 2019). Experts say the frequency of mass shootings, amplified by our near-constant access to media coverage of such events, amounts to an accumulation of exposure that is harming everyone’s mental health. [Related: APA resources for coping with mass shootings] “The more catastrophic events we’re exposed to as a nation, the more impacted we’re going to be on a psychological level,” said Jonathan S. Comer, PhD, a professor of psychology and psychiatry at Florida International University. While some people report panic and distress, others feel numb. Psychological reactions to a crisis vary from one person to the next, based on factors such as age, trauma history, and proximity to an incident. But research has started to reveal who is most likely to be affected, what the long-term mental health problems will be, and what role media exposure plays. Psychology offers guidance about how to channel concern into action amid these atrocities. “We’re at a really important inflection point as a country where we all understand that what’s currently happening with regard to mass shootings cannot continue,” said Beidas, who also directs the Penn Medicine Nudge Unit and Penn Implementation Science Center. “I come to this with a lot of hope that we’re all recognizing that it’s time to do things differently.” A cycle of distress Mass shootings account for about 1% of annual firearm deaths in the United States, but they occupy an outsize space in the public consciousness. “These events are still relatively rare, but it doesn’t feel that way,” said school psychologist Franci Crepeau-Hobson, PhD, an associate professor and director of clinical training at the University of Colorado Denver’s School of Education and Human Development. “I think that everybody’s sense of security has been threatened.” For survivors and witnesses of mass shootings, suffering tends to be particularly severe. Studies have documented increases in posttraumatic stress disorder (PTSD), major depression, anxiety disorders, substance use disorder, and other conditions among people who have survived a mass shooting. “A common theme is that more exposure tends to be associated with more severe symptoms,” said clinical psychologist Sarah Lowe, PhD, an assistant professor of social and behavioral sciences at Yale School of Public Health, who led a 2015 literature review on the mental health consequences of mass shootings (Trauma, Violence, and Abuse, Vol. 18, No. 1, 2015). But the research is still very limited. In Lowe’s review, PTSD prevalence ranged from 3% to 91%, depending on the study, and methodological questions remain, such as what even constitutes a mass shooting. Though relatively few people will witness or survive mass shootings, many more will experience them through news reports and social media. “There’s a great deal of evidence that individuals who are far away from mass shootings can face anxiety and impairments, and this is often correlated with the amount of media exposure they have,” Comer said. Such findings are highly concerning given how intertwined people’s lives are with media, researchers say. Silver and her colleagues have studied that link for more than 20 years, showing how high levels of exposure to media coverage of 9/11 and the Boston Marathon bombings predicted symptoms of acute stress and posttraumatic stress (Psychological Science, Vol. 24, No. 9, 2013; PNAS, Vol. 111, No. 1, 2014). Over time, media exposure to mass violence can even fuel a cycle of distress, where persistent worry about future violence predicts more media consumption and more stress, the researchers found (Thompson, R. R., et al., Science Advances, Vol. 5, No. 4, 2019). That constant worry, known as “perseverative cognition,” has been linked to declines in physical health, including cardiovascular problems (Ottaviani, C., et al., Psychological Bulletin, Vol. 142, No. 3, 2016; JAMA Psychiatry, Vol. 65, No. 1, 2008). In addition to the risks of media exposure, people with a history of trauma are more likely to experience posttraumatic stress (PTS) symptoms following a new exposure, such as a terrorist attack or mass shooting (Garfin, D. R., et al., Psychological Science, Vol. 26, No. 6, 2015). Physical proximity to an incident also carries a higher risk of mental health problems. One study of 44 school shootings found that antidepressant use increased more than 20% among young people who lived within 5 miles of a shooting, versus those who lived 10 to 15 miles away (Rossin-Slater, M., et al., PNAS, Vol. 117, No. 38, 2020). Psychological proximity—the degree to which we relate to another person or an event—also increases the risk for PTS symptoms (Thoresen, S., et al., European Journal of Psychotraumatology, Vol. 3, No. 1, 2012). “Oftentimes, the more one identifies with the victims, the more difficulty they have in the aftermath of an event like this,” Comer said. Going numb While some people worry regularly about mass shootings, many are fatigued by the seemingly endless cycle of violence that moves rapidly through the media and public discourse. “There’s not one single way people are experiencing these tragedies, and there’s no one-size-fits-all response,” Silver said. “One person might be very impacted by an event, and another may not be concerned about it at all.” Research by cognitive psychologists helps explains how we perceive mass violence and why it can leave some people feeling numb. Paul Slovic, PhD, a professor of psychology at the University of Oregon, and his colleagues have shown that in many cases, the more people who die in an incident of mass violence, the less we care. They call this phenomenon the “deadly arithmetic of compassion.” Their research shows that people’s intuitive feelings of concern for victims of violence don’t respond well to statistics and don’t scale up. In other words, the horror people felt when 19 children and two adults were shot and killed at Robb Elementary School in Uvalde, Texas, isn’t 21 times greater than what people feel when one child is murdered. Slovic and other psychologists call this dampening of the emotional response “psychic numbing.” At the same time, people often have a false sense of inefficacy in the face of very large problems, which can lead to inaction and disengagement. In one study, participants who saw statistics about the magnitude of the hunger crisis in Africa donated about half as much money as those who saw a photo of a single child in need (PLoS ONE, Vol. 9, No. 6, 2014). “If we believe there’s a problem that we can’t do anything about, it makes sense that we don’t attend to it, because it’s very distressing to dwell on things you can’t fix,” Slovic said. Finally, research on what’s known as the “prominence effect” shows how people often struggle to make decisions when they require weighing complex tradeoffs (University of Illinois Law Review Slip Opinions, 2015). In the case of gun legislation, this helps explain why the complex calculus of lives saved versus freedoms sacrificed has largely resulted in inaction at the policy level. And on top of this deadly arithmetic, our attention is a scarce resource. Time passes, memories fade, and we’re inclined to shift our attention elsewhere if we don’t see progress. National surveys have shown that support for gun legislation spikes in the immediate aftermath of a mass shooting but fades within a few weeks (Jose, R., et al., Psychology of Violence, Vol. 11, No. 4, 2021; Filindra, A., et al., Social Science Quarterly, Vol. 101, No. 5, 2020). “Our mind deceives us into underreacting to the most important problems in the world, including mass violence,” Slovic said. “But when one of these events occurs, we do have a window of opportunity when people are awake, emotionally engaged, and motivated for action.” Youth on high alert The stress of mass shootings may weigh particularly heavily on children and teens, whose mental health is already in turmoil. In 2021, three leading pediatric organizations declared a national emergency, while the U.S. Surgeon General issued a special advisory on youth mental health, citing a 57% increase in suicides between 2007 and 2018 (Curtin, S. C., National Vital Statistics Reports, Vol. 69, No. 11, 2020). Research shows that at least some of that distress can be attributed to mass violence. One study of more than 2,000 teens found that greater concern about school shootings and violence predicted increases in anxiety and panic six months later (Riehm, K. E., et al., JAMA Network Open, Vol. 4, No. 11, 2021). “When I talk to kids about this, I am shocked by how inured and accepting they are,” said Don Grant, PhD, the executive director of outpatient services for Newport Academy in Santa Monica, California, and is president of APA’s Division 46 (Society for Media Psychology and Technology). “They don’t know a world where there’s not an active shooter drill at school.” In the educational context, that constant vigilance can be particularly problematic, and research on threat perception suggests that prolonged heightened anxiety may interfere with learning, said Crepeau-Hobson. Students who are constantly worried about a toxic stressor, such as gun violence, devote more mental resources to emotions and fewer to executive functions, including learning, memory, and sustaining attention (Dettmer, A. M., & Hughes, T. L., Education Week, 2022). “When threat perceptions are escalated and stress responses are activated, we can’t access the higher parts of our brain,” Crepeau-Hobson said. Data suggest those effects could be far-reaching. A 2020 report from the National Bureau of Economic Research found that school shootings increased absenteeism, reduced high school and college graduation rates, and decreased retention of teachers. Those effects persisted into the mid-20s of young adults who attended schools where a shooting occurred; they had lower employment rates and earnings than their peers (Cabral, M., et al., NBER Working Paper 28311, 2022). “It’s not just that individual young people experience these really deleterious effects, but there is also a societal effect,” Beidas said. Because mass shootings impact children and teens at the individual, institutional, and societal levels, experts say a tiered approach is needed to minimize harm. In the family context, it’s important to initiate conversations with children and teens after an incident, even if they aren’t part of the affected community, said Comer. “When kids hear about these events from their parents, they tend to do better than when they hear about it from their friends or the media first,” he said. If a child or teen becomes hypervigilant or starts to avoid certain places or activities, that may indicate a need for professional support, said Grant. Educators and policymakers also need empirical data on what makes schools safe—both physically and psychologically, said Crepeau-Hobson, a member of the APA’s Division 16 (School Psychology) executive committee. “A number of schools are wasting their resources on strategies that aren’t particularly helpful, without thinking about their psychological impact on children who are coming to school to learn,” she said. School districts across the nation are spending billions of dollars to enhance security, installing emergency alert systems and hiring additional personnel. But many of the new approaches lack evidence and could even cause harm. For example, a law enforcement presence may make some students feel safer but may undermine a sense of safety in others, such as students of color. Early studies of active shooter drills—which are now nearly ubiquitous—suggest they may increase anxiety, stress, and depression symptoms in children and adolescents (“The Impact of Active Shooter Drills in Schools,” Everytown Research and Policy, 2020). Communities also need to be prepared to support children in the immediate aftermath of a mass shooting. Last year, Comer launched the Network for Enhancing Wellness and Disaster-Affected Youth (new day), which delivers large-scale professional training on disaster mental health across the country. new day teaches Psychological First Aid and other skills to teachers, coaches, nurses, and others who work with children and teens. Sustaining engagement More research is also needed on how mental health services can best support survivors, families, and affected communities in the aftermath of a mass shooting, experts say. Richer firearm-injury and mortality datasets can also help researchers better understand the conditions surrounding these crises. But many feel change is urgently needed, and that partnering with the firearm community—to promote more secure storage of firearms, for example—is one way to start reducing firearm injuries and deaths right away, Beidas said. More than 7 million Americans bought firearms for the first time between January 2019 and April 2021, mostly for self-protection (Miller, M., et al., Annals of Internal Medicine, Vol. 175, No. 2, 2022). That suggests many people need education on secure storage (see “Talking to patients about firearm safety,” April 2022 Monitor), and that the recommended method of storing a gun unloaded and locked, with ammunition locked separately, might not be acceptable to all firearm owners. “We need to establish a shared mission with the firearm community,” Beidas said, “and keep in mind that a harm reduction approach is the most effective way to change behavior.” At the policy level, a majority of Americans support stricter gun laws, but progress in that domain may be incremental (Jose, R., et al., Psychology of Violence, Vol. 11, No. 4, 2021). Slovic said it’s important to stay engaged and not to let a false sense of inefficacy prevent us from taking steps in the right direction. “Just because we can’t fix a problem in its entirety doesn’t mean that we shouldn’t do what we can do to make a difference,” he said. “We cannot afford to let our minds deceive us into underreacting.”

## 2---Digital skill gap (47)

#### AI improves education and sets the next generation up for success, Milberg 24

Tanya **Milberg 24**, 4-28-2024, "The future of learning: AI is revolutionizing education 4.0," World Economic Forum, https://www.weforum.org/stories/2024/04/future-learning-ai-revolutionizing-education-4-0/, accessed 2-18-2025//Lead of Education, Skills, Learning @ WEF, Former BoD of Swiss Canadian Chamber of Commerce, M.A Tel Aviv University, //brayden?

Artificial intelligence (AI) can support education by automating administrative tasks, freeing teachers to focus more on teaching and personalized interactions with students, enhancing rather than replacing human-led teaching. AI applications in education must be designed collaboratively and with equity in focus, addressing disparities across various demographics and ensuring accessibility for all students. Beyond using AI tools for educational purposes**, it** i**s** crucial to educate students about AI itself, including how to develop AI technologies and understand their potential risks. In today’s rapidly evolving technological landscape, the intersection of artificial intelligence (AI) and education is not just a future possibility; **it is imminent**. Imagine a future where all students receive personalized support and inclusive learning opportunities, build stronger connections with teachers for enhanced guidance and receive apt recognition and evaluation of their achievements. While the promise of AI in education is compelling, only through responsible and informed adoption can AI truly fulfil its potential and ensure equitable access to quality education for all. In 2020, the World Economic Forum identified eight pivotal transformations needed to enhance education quality in the age of the Fourth Industrial Revolution – Education 4.0 Framework. As AI emerges as the defining technology of this era, we can accelerate the adoption of Education 4.0 by using this technology and ensuring learners are equipped to thrive with it.With increasing interest in AI and education, the Education 4.0 Alliance sought to understand the current state and future promises of the technology for education. The latest report – Shaping the Future of Learning: The Role of AI in Education 4.0 – shows four key promises that have emerged for AI to enable Education 4.0: 1. Supporting teachers’ roles through augmentation and automation The global teacher shortage poses a formidable challenge to improving educational outcomes, with the demand for educators projected to surge in the coming years. Integrating AI into education can streamline administrative tasks, giving teachers more time for meaningful student engagement. By automating routine duties and emphasizing human-centric teaching, we can create an environment where educators can thrive, creating a richer learning experience. However, teaching involves more than imparting information – AI should augment, not replace teachers’ role. 2. Refining assessment and analytics in education The integration of AI in education holds promise in revolutionizing the assessment and analytics landscape. AI-enabled assessments offer educators invaluable insights, from pinpointing learning trends to supporting the evaluation of non-standardized tests. By leveraging AI capabilities, educators can expedite the assessment process, offering timely feedback to learners and facilitating more focused engagement. Through real-time analysis, educators can identify strengths and weaknesses in student performance, allowing for targeted instructional strategies. 3. Supporting AI and digital literacy Many education systems struggle to address the **growing digital skills gap**, crucial for students' **employability** and ethical tech use. Bridging this gap is imperative to cultivate an AI-ready workforce. AI presents an avenue through which students can improve digital literacy, critical thinking, problem-solving and creativity, **preparing learners for future job** demand**s**. Integrating **AI into education**, through traditional or innovative methods, **is key to shaping tomorrow’s workforce**. 4. Personalizing learning content and experience Extensive research confirms that individual tutoring significantly boosts learning outcomes, with tutored students consistently outperforming 98% of their peers in traditional classroom settings. However, providing personalized tutoring for every student poses a major economic challenge. AI offers a solution to this hurdle. By harnessing AI, we can now tailor the learning experience to the individual, enhancing academic performance while seamlessly catering to diverse learning needs. Customizable interfaces emerge as invaluable assets, particularly benefiting neurodiverse students and those with diverse physical abilities.

#### AI skills are key to good jobs mckenna 25

Amanda Zieselman McKenna Alex Swartsel 25, 2-6-2025, "Skills and Talent Development in the Age of AI," https://www.jff.org/idea/skills-and-talent-development-in-the-age-of-ai/, Alex Swartsel is managing director of the Insights practice at JFFLabs and is leading the launch of the Center for Artificial Intelligence & the Future of Work. She helps education-to-career decision-makers understand and prepare for emerging technologies and innovations shaping the future of work and learning. Her skills and areas of expertise include: Technology and digital transformation Insights, thought leadership, research, and market analysis Public speaking and communications Organizational leadership and strategy Before joining JFFLabs, Swartsel was chief of development, finance, and external affairs for Teach for America’s Washington, DC, region and a senior advisor to U.S. Senator Elizabeth Warren. Educational background: Bachelor’s degrees in political science and music, Wellesley College MBA, Yale School of Managementaccessed 3-4-2025 (the way this article is formatted is weird, I did my best to paste the actual text tho, if there is an issue please email me) //wyatt G?//

In 2023, Jobs for the Future (JFF) released The AI-Ready Workforce, a report that explored how AI might reshape jobs to better understand how to support workers through this transition. We are still in the very early days of AI’s impact, and we’re just starting to see how it might be affecting the labor market—from job design, to next-generation workforce training, to how businesses are supporting their employees as they adopt new technologies. At JFF’s Center for Artificial Intelligence & the Future of Work, we believe the transformation set in motion by generative AI is accelerating shifts that will meaningfully change in-demand jobs and skills, with implications for a wide array of stakeholders from training providers and employers to policymakers and investors. Our new research explores these emerging trends, and offers key insights in three areas: Jobs across the economy are increasingly seeking AI skills. We explore this growing demand and share a new skills classification model for in-demand, high-growth occupations accessible to people without a bachelor’s degree. The model finds growing prioritization of generalized professional skills like critical thinking and problem solving, and human skills like initiative, leadership, and communication in tandem with the growth of AI. Training providers will need to strengthen their organizational capacity to support learners in an AI-powered future. We interviewed leaders in the field to develop a set of recommendations to support organizational responses to this moment. Download the toolkit here. Small businesses are moving toward AI adoption and are eager to drive economic opportunity for both employees and businesses. We conducted a national survey to understand where organizations are in their AI journeys and used these insights to develop a set of human-centered recommendations to support worker-centric AI adoption and talent development strategies. Download the toolkit here. Policymakers, investors, and funders can contribute to a workforce that welcomes everyone in the age of AI by supporting organizations committed to this work and helping create the conditions that will allow this work to be successful through pathways such as policy development and building the infrastructure for fair digital access. Subscribe for AI updates from JFF to learn more about our ongoing work in this field. AI and Jobs Since the public release of ChatGPT at the end of 2022, there has been rapid growth across the economy in job postings mentioning AI. We used keyword searches of job postings for “AI” and/or “artificial intelligence” as a proxy for employers’ growing interest in incorporating AI into roles. We searched for these keywords across all jobs, not just those requiring more specialized AI skills such as machine learning. Demand remains nascent, and these keywords are still rare in job descriptions, but we observed a marked increase when comparing December 2022 to December 2024, with the volume of job postings increasing 108% (from 730,000 job postings in December 2022 to 1.5 million in December 2024.) This suggests a rapid adoption of AI tools over a short time window to support and augment workers’ roles. Our data show notable demand for AI in job postings in key subsets of the labor market. From an occupational perspective, we see that jobs in the technology sector have had rapid growth in postings with AI keywords—a total of 192,724 postings, for an increase of 407%. We also see high growth in occupations in human resources, where a total of 3,651 postings represented 419% growth; supply chain, where 876 postings showed 86% growth; customer service, where 1,027 postings showed 70% growth; and marketing and public relations, where 4,710 postings showed 38% growth. This data supports emerging trends for where there is noted early AI adoption (McKinsey). Within these concentrations, we see demand across the spectrum of educational requirements. We see the highest increase of AI mentions in job postings requiring a bachelor’s degree—764,033 total, showing 125% growth in AI mentions since December 2022. However, we also see high levels of growth in roles requiring an associate’s degree (69,050 postings, 114% growth) or a high school degree (90,454 postings, 108% growth) as the highest level of education requirement. Notably, there is also an increase for roles with no education requirement listed (575,339 postings, 95% growth). Note that some roles list multiple education requirements. AI and Shifting Skillsets To better understand how the fast but uneven growth of AI may already be reshaping jobs and skills, we conducted a deeper skills analysis for a subset of occupations. Network and computer systems administrators Computer user support specialists Computer programmers Customer service representatives Project management specialists Medical assistants Medical and health service managers We chose these occupations because they are accessible to people without bachelor’s degrees, are in-demand and high-growth, are often connected to several of the industries we studied in The AI-Ready Workforce Report, and are largely representative of jobs that may be disrupted by AI. These occupations represented nearly 6.5 million jobs and 3.7% of the workforce in 2024. And each of these occupations saw immense growth in job postings with AI mentions during our period of analysis of skills demand (see below: Methodology.) For example, medical assistants saw 8,350% growth (from 2 postings mentioning AI in January of 2018 to 169 in December of 2024) and customer service representatives saw 7,150% growth (from 12 postings to 870 for the same time comparison). A table shows the increase in AI-related job postings from 2018 to 2024, detailing seven occupations with varying percentages, including Computer Programmers, Medical Assistants, and Project Managers. Other analyses of AI workforce impacts have discussed changing employer priorities for “hard” or “technical” skills as opposed to “soft” or “durable” skills, but we wanted to dig one level deeper to better understand how demand was changing for specific skills. We found that binary classifications were not nuanced enough, so we leveraged deep dives into existing alternative skills frameworks to further break out skills categories. To better understand how specific skills are becoming impacted, we categorized skills under four classifications. Competencies directly related to the use, management, and development of digital technologies and systems. In current context, these skills range from basic digital literacy to advanced technical proficiencies in software, hardware, and digital platforms. Examples include programming, data analysis, cybersecurity, and proficiency with specific software applications. We broke this category out specifically, as new and emerging digital skills may have an especially close relationship with artificial intelligence, given that new digital competencies are likely to be necessary to effectively use the technology, and the technology itself may replace or augment certain existing skill competencies. This gives us a sense of the changes in digital sophistication within different occupations. Professional competencies that are not tied to any particular domain or industry but are essential for effective performance across various job roles and sectors. These skills, while transferrable, are specifically relevant to professional contexts and distinct from general human skills. Examples include project management, strategic planning, business analysis, and professional writing. We looked at the listed seven occupations and used job posting data in Lightcast to compare demand for the top 20 growing and top 20 declining skills across each of the four skills categories in 2018 (chosen as a baseline year prior to the launch of ChatGPT and subsequent mainstream familiarity with AI) to the demand in 2024 (most recent and available full year of data following the launch of ChatGPT.) What We Learned From this analysis we see three emerging themes occurring across these seven occupations in tandem with the growing prominence of AI in the workforce: 1. Specialized digital skills (skills that require advanced expertise) are experiencing high rates of churn as new technologies are introduced and certain once-ubiquitous industry skills are likely being replaced by, or rolled into, new skill sets. In addition, there is a correlation in the labor market data between the rise of AI and the churn seen in the digital skills category. This means that technological advancements, accelerated through AI adoption, are shortening the useful life of some specialized skills and creating challenges for skills training to keep up with this rapid pace of change. EXAMPLE For network and systems administrators, cloud solutions and cloud computing are critical and growing specialized digital skills. We see demand for these skills increasing while skills such as distributed computing and database modeling are decreasing. This suggests that skills related to older technologies are gradually being replaced by skills associated with new technologies at an accelerated rate. 2. Professional skills, both specialized and generalized, are continuing to show up consistently in job postings, with nearly the same percentage appearing in 2024 as 2018. This means that, while digital skills are experiencing rapid and uneven turnover, employers are looking for both domain-specific and domain-agnostic professional knowledge in workers. EXAMPLE For customer service representatives, we see a continued valuing of professional skills like business operations and project management. 3. Human skills are rapidly and consistently increasing in demand from employers independent of occupation. AI may already be reinforcing a shift in demand for these non-specialized skill sets, even in highly technical roles, suggesting that these human skills are more resilient to displacement by AI. EXAMPLE Skills like critical thinking, problem solving, initiative, leadership, and communication were increasingly prioritized across each of these occupations.

#### Lack of digital skills is dangerous Saunders 24

Trent Saunders, ND, "What is the Digital Skills Gap and How Much is it Costing Enterprises?," Future Point Of View, https://fpov.com/2024/02/27/what-is-the-digital-skills-gap-and-how-much-is-it-costing-enterprises/, accessed 2-18-2025// Pursuing his interest in innovation, Trent began his career in software sales and has built a track record of identifying solutions to help businesses grow. Trent graduated with a degree in Business from Southern Methodist University. During his time at SMU, he was the President of the Marketing Association and served as the team lead for a practicum project designing and pitching a campaign for the Dallas Stars. Trent remains an avid learner and is always on the hunt for new ideas.  //brayden?

The digital skills gap refers to the discrepancy between the digital skills an organization needs and the skills its current workforce possesses. This gap can have significant consequences for businesses, hindering their ability to **innovate and compete**, embrace digital transformation, and recruit and retain talent. A digital skills gap often manifests in an ineffective use of technology. Panorama Group evaluated ERP software usage and found that business typically use only 41% of their system’s features. A report from Okta found that while employees believe they use around 13 software tools, in reality large enterprises subscribe to 211 platforms. A digital skills gap results from a number of factors including a rapidly changing technological environment that outpaces skills growth and **a lack quality education** and training. Employers are ultimately held responsible for the consequences of a digital skills gap, and without a forward thinking model for upskilling labor, the tax of a digital skills gap will only continue to worsen for organizations. Enterprises are losing about $1.14 million per week due to the digital skills gap, according to a recent study by WalkMe. This loss of efficiency translates to a waste of 44 working days per year – time wasted by employees struggling with technology-related challenges. A study by Capgemini and LinkedIn found that the digital skills gap affects 54% of organizations globally, and results **in productivity losses**, lower employee engagement, and higher attrition rates. The study also revealed that 29% of employees believe that their current skill set is redundant or will be in the next one to two years, and 38% are worried about losing their jobs due to automation. The lack of sufficient digital skills in the workforce has large macroeconomic impacts. According to a report by Accenture, the lack of digital skills could cost the US economy up to $**975 billion in annual GDP** by 2028, as well as reduce the competitiveness and innovation potential of businesses across sectors. The report also estimates that closing the digital skills gap could **create 5.1 million new jobs** in the US by 2028, and increase the average income of workers by 17%. The digital skills gap can affect both individuals and organizations, as it can reduce productivity, innovation, competitiveness, and employability. It can also widen existing inequalities and create new ones, as those who lack digital skills may face higher risks of unemployment, underemployment, or exclusion from the labor market. Meanwhile, organizations that fail to close the digital skills gap risk falling behind competition that effectively upskills and onboards talent.

## 3---Face to face (34)

#### AI fixes teacher burnout Forbes 24

Tony Bradley 24, September 19 2024 "AI’s Role In Saving Teachers Time And Revolutionizing Education," Forbes, https://www.forbes.com/sites/tonybradley/2024/09/18/ais-role-in-saving-teachers-time-and-revolutionizing-education/, QUAL-Tony Bradley is a reporter who covers the cybersecurity industry and the cross-section of technology and entertainment. He has been a Forbes contributor since 2014. He is the founder and editor of TechSpective and a senior PR manager with NetApp. Bradley has been a CISSP-ISSAP since 2002 and was recognized by Microsoft as an MVP in Windows Security for 11 consecutive years. He has authored or co-authored a number of books, including Unified Communications for Dummies. He served in the U.S. Air Force in Desert Storm. His diverse background allows him to bring unique perspective to his stories. Follow Bradley for insights on emerging cybersecurity trends and a peak behind the curtain to see how technology shapes and enables entertainment. accessed 2-19-2025 //wyatt G?//

The teaching profession is in crisis. Burnout rates among educators are soaring, with K-12 teachers being some of the most overburdened professionals in the U.S. today. What many don’t realize is that much of this burnout stems from the hidden workload teachers face. This situation is compounded by the fact that the average teacher uses over 140 different digital tools throughout the school year. Juggling this fragmented ecosystem of apps and platforms adds to the stress, leaving educators with little time for what really matters: engaging with students. But there's hope on the horizon. Artificial intelligence is emerging as a powerful ally for educators, capable of automating many of these time-consuming tasks and freeing up hours each week. In particular, tools like Brisk Teaching’s AI-powered Chrome extension and its new student-facing feature, Brisk Boost, are reshaping the education landscape. Teacher Burnout and the Hidden Workload Burnout among teachers has reached alarming levels. According to a recent Gallup poll, K-12 teachers are experiencing the highest rates of burnout among all professions in the United States. This isn’t just about classroom management; the true burden comes from the hidden workload that many outside the profession are unaware of. Grading assignments, preparing lesson plans, managing student feedback, emailing parents, and attending professional development meetings all pile up behind the scenes. Teachers often spend more time on these tasks than they do teaching in the classroom. The result? High levels of stress and an increasing number of teachers leaving the profession. How AI Can Be a Solution Across various industries, AI has already proven its ability to automate repetitive and time-consuming tasks, boosting productivity and efficiency. The same potential exists in education, where AI can take over the labor-intensive tasks that weigh teachers down. Yet, the solution isn’t as simple as just throwing new tools into the mix. Teachers already navigate a sea of educational apps, platforms, and tools each year. If AI is going to make a meaningful impact, it must integrate seamlessly into the tools teachers are already using, without adding additional complexity or creating a steeper learning curve. Brisk Teaching’s AI-Powered Solution This is where Brisk Teaching comes in. Brisk Teaching is an AI Edtech startup that just announced its seed round, led by Owl Ventures, which brings their total funding to $6.9 million dollars. Brisk Teaching’s AI-powered Chrome extension is not another tool teachers have to manage—it’s a solution that works within their existing platforms to automate tasks they’re already doing. It speeds up routine activities like grading, lesson planning, and even creating new content from the materials teachers already use. For example, Brisk Teaching’s tools can turn a news article, YouTube video, or Google Slides presentation into a dynamic, interactive learning experience with just a few clicks. Teachers can also automate feedback on student writing, drastically reducing the time spent on grading essays. The result is a system that saves teachers up to 20 hours of work each week, freeing up time for what matters most: personalized engagement with students. But Brisk Teaching isn’t just about helping teachers—it’s about empowering students too. The newly launched Brisk Boost feature allows students to use AI in safe, controlled activities that are linked directly to their lesson objectives. By functioning as a personal tutor, Brisk Boost adapts to each student’s unique needs, offering real-time feedback, interactive quizzes, and brainstorming support. All of this helps students stay engaged while giving teachers valuable insights into how well their students are grasping the material. Real-World Impact: Success and Adoption The impact of Brisk Teaching’s solution has been swift and significant. Since launching just over a year ago, the company has grown rapidly, with over 500,000 teachers—one in ten in the U.S.—now using the AI-powered Chrome extension. These tools have already saved educators over 10 million hours globally, proving that AI can make a meaningful difference in the classroom. Educators who have adopted Brisk’s solutions report not only time savings but also improved student outcomes. For example, by automating repetitive tasks, teachers have more time to focus on individual student needs and can offer more personalized instruction. At the same time, Brisk Boost has helped engage students with content in new and interactive ways, leading to greater participation and comprehension. “Brisk Teaching is an incredible AI tool. It serves as a blueprint for instant student feedback - which you can edit on the spot,” explained Chrissy Macso, a middle school English teacher at Old Trail School in Ohio. “If this would have come out years ago, more teachers would likely be feeling way less burnout. You can tell this is a product made by teachers for teachers. They thought of everything. If you’re a teacher and haven’t tried this tool, do it.” The Future of AI in Education As the adoption of AI in education continues to grow, we’re witnessing a shift in attitudes. What was once viewed with skepticism—particularly when tools like ChatGPT first hit the scene—is now being embraced by teachers as a way to enhance both their own productivity and the learning experience of their students. Arman Jaffer, CEO of Brisk Teaching, shared, “We talk to teachers and school administrators every day to understand what’s top of mind for them. It’s been interesting to see how attitudes have changed rapidly about generative AI. Many we talk to have shifted from ‘Ban it,’ to ‘How can teachers use this?’ to ‘How can schools use AI to engage students and teach them the skills of the future?’” This shift is a testament to the value AI brings in creating more personalized learning experiences. Tools like Brisk Boost, which adapt to each student's needs, represent the future of differentiated learning. Rather than treating all students the same, AI allows teachers to tailor their instruction to better suit the unique learning styles and abilities of their students. Empowering Educators for the Future The benefits of AI in education go far beyond simple time savings. By automating the most tedious and time-consuming tasks, AI is empowering teachers to focus on what truly matters—engaging with students and fostering a better learning environment. Solutions like Brisk Teaching’s AI-powered Chrome extension and Brisk Boost are not only helping to alleviate teacher burnout but also paving the way for a more sustainable and effective future for education. It is clear that AI is not just a passing trend—it’s a transformative technology that will shape the future of education for years to come. Teachers, administrators, and policymakers should embrace AI tools that integrate seamlessly with existing systems, saving time and enhancing the learning experience. With AI as an ally, educators can finally find the balance they’ve been seeking between managing administrative tasks and delivering quality education to their students.

#### Education is optimistic WEF 25

**World Economic Forum**, 25, 1-9-2025, "Using AI in education to help teachers and their students," <https://www.weforum.org/stories/2025/01/how-ai-and-human-teachers-can-collaborate-to-transform-education/> QUAL- Derek Haoyang Li is the Founder and Chief Education Technology Scientist at Squirrel Ai Learning, a top 20 AI-Unicorn in China. He is the Vice Chair of the Intelligent Education Sub-Committee of the Chinese Association of Automation and also the Chair of the IEEE Artificial Intelligence LLM-4EDU Standards Group. Derek was featured as the cover story in Forbes China magazine and interviewed. As a serial entrepreneur, Derek co-founded two publicly-listed companies. One of the companies had a market cap of $200 million. Squirrel Ai Learning is the leading AI and education innovator and unicorn at the forefront of the K-12 AI revolution. Squirrel Ai launched the world’s first LAM (Large Adaptive Model) engine in 2024. Derek also created several ingenious educational innovations: “Concepts on Nano-scaled knowledge Components”, “AI-Model-Adapted Learning-Skills-Decomposition Methods”, “Reconstructing Knowledge Space Theory (KST) with Students’ Reasons for Mistakes”, “Algorithms on Calculating the Relevance of Probability between Non-relevant Knowledge Components.” , accessed 2-19-2025 //brayden?

Educators and technologists must work together to create a new educational paradigm where **AI and human teachers operate as true partner**s. This vision sees teachers evolving into "learning architects" who orchestrate sophisticated educational experiences by leveraging AI tools while maintaining their crucial role as mentors and guides. This isn't just an aspirational vision – according to a 2023 Walton Family Foundation survey, **71% of teachers and 65% of students already agree that AI tools will be essential for students' success** in college and the workplace. The next five years will be critical in shaping this transformation. Educational institutions need to invest in both AI infrastructure and teacher training, ensuring educators are comfortable using these tools to enhance their teaching rather than feeling threatened by them. Forward-thinking schools are already establishing AI competency programmes for teachers, focusing on how to effectively integrate tools like adaptive learning platforms and GenAI into their teaching practice. Recent Pew Research data suggests that teachers are fully aware of the role of AI in education, with **73% of educators** either **see**ing balanced **benefits**, positive **potential** or remaining open **to** exploring **AI**'s impact. This measured perspective from the teaching community provides an excellent foundation for a collaborative future in which AI tools are carefully and purposefully integrated into education with teacher input and guidance. Realizing this potential will require careful attention to equity, however, ensuring these tools reach all students, not just those in well-funded districts. The future of education lies not in choosing between AI and human teachers, but in embracing the powerful potential of their collaboration. The technology is ready and early results are promising. Now it’s time for educational institutions, policy-makers and teachers to embrace this collaborative approach to create learning environments that are more personalized, equitable and effective than ever before. By combining the analytical power of AI with the irreplaceable human element of teaching, we can truly transform education for the next generation.

#### AI is a lifesaver Will 25

Madeline Will 25, 2-14-2025, "Here’s How Teachers Are Using AI to Save Time," Education Week, https://www.edweek.org/technology/heres-how-teachers-are-using-ai-to-save-time/2025/02, accessed 2-19-2025 (skipped the rest of the quotes cuz I got lazy, nothing contradictory to the rest of the article tho) QUAL- Madeline Will is an assistant managing editor for Education Week, leading coverage of school leadership and general education trends. Previously, she covered the teaching profession for Education Week for eight years. She graduated from the University of North Carolina at Chapel Hill.

//wyatt G?//

Teachers spend up to 29 hours a week doing nonteaching tasks: writing emails, grading, finding classroom resources, and carrying out other administrative work. They also have high stress levels and are at risk for burnout. Can artificial intelligence help ease both those problems? Advocates say AI can be a real timesaver for teachers, completing tasks in seconds that would have taken a person hours. While educators caution that AI will never replace a teacher’s professional expertise, many argue that it can take the more mundane, rote job duties off teachers’ plates—reshaping a notoriously high-stress job. Already, 9 in 10 educators say artificial intelligence has changed the job of teaching at least a little, according to a nationally representative EdWeek Research Center survey of teachers, school leaders, and district leaders, conducted in December. Forty-two percent said AI has changed the profession “a fair amount” or “a lot.” And the job will change as AI gets more advanced and teachers become more comfortable with its use, educators predict: About three-quarters said AI will change the profession “a fair amount” or “a lot” over the next five years. Part of that perceived change likely stems from the way students may be using AI to complete assignments. But another way AI is changing the profession involves the day-to-day work. The EdWeek Research Center asked 990 educators (mostly teachers) to share an example of how they use AI in their classroom or daily work. Although many respondents said they aren’t using AI in the classroom at all, other responses show that teachers are leaning on AI tools to make their jobs easier, including by creating such classroom materials as quizzes and assignments, drafting emails to parents and administrators, helping individualize instruction, and refining and enhancing lessons. Following are 40 responses from teachers: Teachers use AI to help them write emails to parents and administrators When writing a negative letter about grades to a parent, I go to AI to change the wording for me. —Middle school social studies | Indiana I use it as a tool to communicate with administrators and parents. I find it much quicker to type in the general idea and receive an email I could have written, but it would have taken me 15 minutes or more. —Elementary school | Utah I use it to clarify information if I am struggling with words. I put in a parent letter (for example) and have it fix it. Then I edit their fix. —Middle school English/language arts | North Carolina Making emails to parents sound more professional. —Elementary instructional technology | Maryland I’ve used it to reword/edit recommendation letters and report card comments. —High school science | Michigan How teachers use the technology to create quizzes and other classroom resources I have used School AI to create an escape room review for genetics. I have used ChatGPT to create lesson prompts. I have used Magic AI to create worksheets and questions for YouTube videos I show in class. I have used AI to create quiz questions in Quizizz. —Middle school science | New York I use AI to aid in making worksheets or quizzes out of already existing resources. —High school science | Missouri I have AI make my warm-up and exit tickets. —High school math/computer science/data science | New Jersey Using textual details to create accurate AI images to depict key settings in The Great Gatsby. —High school English/language arts | Georgia I have used AI to develop a list of anticipation questions to lead discussion before a research project. —High school English/language arts | Arkansas I don’t use it daily, but one way I’ve used it is to create grammar sentence practice with AI-created sentences for students to correct. —Middle school English/language arts | New York I’ve utilized Notebook LM to generate a two-person podcast that students listened to as a preview to the reading they would be doing for a unit. —High school science | Kansas Helps create story problems for math. Creates reading comprehension articles for subjects I’m teaching. —Elementary school | Utah AI-driven strategies teachers are using to differentiate instruction The best way that AI has helped in my classroom is by finding resources or alternate lessons/activities for students who are absent and have missed labs or experiments. It also helps alter lessons for students who are well below grade level and struggle with grade-level assignments. —Middle school science | Pennsylvania I use AI to change the reading level of some assignments. For example, it can very quickly change a given text from 10th grade to 5th grade. —High school social studies | Oregon As a special education teacher, I work with students across multiple subjects. Many times I do not have the background in some subjects. I have used ChatGPT to provide me with examples of the tasks being asked of students. By doing so, I am able to guide a student in how to begin a task or what to focus on with a task. —Middle school special education | Pennsylvania To reduce time and mental effort to research and design individual learning programs to match student’s expressed interest. —High school mythology | Louisiana I use AI to simplify reading selections in the target language that I teach so that the selections are at levels that are appropriate for specific classes of students. —High school world/foreign languages | Colorado I have used it to modify content and instructions for students [with individualized education programs] and to create quizzes. —High school English/language arts | Washington state

#### And, retention post 24

Rachel Post 24, 2-1-2024, "How Can AI Help Solve Teacher Shortages?," No Publication, <https://www.aaspa.org/news/how-can-ai-help-solve-teacher-shortages>, QUAL- Rachel Post is a contributor to the AASPA blog, focusing on topics related to educational administration and human resources. accessed 2-19-2025 //wyatt G?//

When discussing the current state of education with administrators, one theme consistently predominates: the national teacher shortage crisis and its effects on students, teachers, and administrators. At the start of the 2023 school year, there were an estimated 55,000 vacant teaching positions nationwide, an increase of 51% from 2022. An additional 270,000 teachers were working without meeting state qualifications. Coupled with a high teacher turnover rate, peaking at 14% in the 2021-22 school year, districts and administrators across the country are desperate to secure teachers from an ever-diminishing supply. School districts are reacting with various strategies, from adopting four-day school weeks to offering signing bonuses to reducing teacher licensure requirements. While these measures offer temporary relief, they invariably create deeper problems and they fail to address the root causes of teacher shortages or the long-term well-being of students. The Rise of AI in Education – Can It Be Used for HR? The post-COVID era has seen a surge in educational technology and AI, sparking conversations about their potential to revolutionize education. However, this conversation hasn’t yet extended to the HR department. But what if AI-powered technology could provide tangible solutions to the teacher shortage, aid in preparing new educators, and streamline HR operations in schools? Online Teaching: Filling Immediate Vacancies & Training New Teachers Due to the shortage of certified in-person teachers, many districts are turning to companies that provide online instruction. COVID compelled teachers and schools to become well practiced in managing online classrooms. Schools are now far more capable than ever of implementing online teaching solutions, and an entire generation of teachers has gained substantial experience in online delivery. AllCourse, a new edtech company, is using these newfound societal capabilities to help solve teacher shortages. AllCourse is a marketplace linking certified teachers teaching online with school districts looking to hire quickly and painlessly. Akin to other labor marketplaces like Upwork or TaskRabbit, What makes AllCourse unique is the AI it uses to recruit large numbers of highly qualified teachers, which means that AllCourse can offer extremely cost-effective and flexible teacher hiring options. Districts can post jobs for free, and then AllCourse’s AI-powered system then begins to crawl the web, as well as first-degree teacher connections within the AllCourse community, to find teachers who meet the exact qualifications of the job posting. With AllCourse, it’s free and easy to build a large pool of online teachers who are licensed and qualified for all your open roles. Beyond filling immediate vacancies, online teachers have an unexpected perk – they can help train new teachers. When districts implement online teachers in in-person settings, a classroom facilitator, such as a paraprofessional or substitute, often manages the environment, monitoring behavior and encouraging engagement. One district in South Carolina decided to use this facilitator role as part of their teacher training program for candidates undergoing certification. These facilitators gain valuable classroom management experience and mentorship from highly-qualified teachers. Furthermore, all AllCourse teachers record their sessions; AllCourse is building a large library of recorded classes that can be used as training tools for new teachers. Online teachers, therefore, can both address the immediate need to fill vacancies and help train the next generation of educators.AI-Powered Tools: Reshaping Resource Creation to Reduce Teachers' Workload The potential of AI to change the ways teachers teach is frequently talked about, but what if AI tools could attract teachers by easing their workload? Teacher burnout, resulting from heavy workloads, is a leading cause of high teacher turnover rates, with 44% of K-12 teachers reporting often or always feeling burnout. AI has the potential to reduce teacher burnout by providing tools that allow educators to spend more time on teaching and less time procuring resources. BookBaker, created by AllCourse, is a first-of-its-kind AI content generator that allows teachers to quickly create custom learning materials differentiated for their students and aligned with their curricula. BookBaker allows educators to create any kind of materials – from worksheets all the way up to textbooks – in just a few minutes at 90-99% lower prices than traditional materials. BookBaker is poised to become an essential tool in reducing teacher burnout, as teachers increasingly turn to it to find free materials already created by other teachers or to create their own materials at ultra low cost simply by checking a few boxes. And implementing powerful new AI tools like BookBaker will allow districts to reallocate the billions of dollars spent on textbooks and other learning content to areas such as teacher salaries and student enrichment programs.BookBaker also helps substitute teachers by enabling them to create standards-aligned, relevant worksheets for students in minutes, ensuring continuous learning even during teacher vacancies and situations where there are no sub plans. AI in HR: Cultivating School Culture A strong school culture is essential for attracting and retaining skilled educators. Research suggests that teachers who resonate with their school's mission are more likely to stay. However, creating mission-aligned documents can be time-consuming for already inundated HR departments. AI tools like BookBaker can expedite this process. By using AI content-generators, school districts can quickly create a wide variety of customized training materials, employee handbooks, and FAQs, all aligned with the school’s mission. This not only helps improve school culture but also frees up HR staff to focus on recruiting and retaining educators. Technology and AI are often not part of the HR conversation, but these tools can help school districts whether they are filling immediate vacancies, training new teachers, or attracting teachers with tools that can reduce their workload. Solutions like AllCourse’s teacher recruitment marketplace and BookBaker’s AI-superpowered content creation are two examples of how we can harness technology to create sustainable solutions to the teacher shortage – ultimately supporting teachers and improving student outcomes.

## 4---Cyber (60)

#### 2025 is a turning point Doyle 25

Kirsten Doyle 25, 1-8-2025, "Cyber Threats Rising: US Critical Infrastructure Under Increasing Attack in 2025," No Publication, <https://www.tripwire.com/state-of-security/cyber-threats-rising-us-critical-infrastructure-under-increasing-attack,QUALS-> Kirsten Doyle has been in the technology journalism and editing space for nearly 24 years, during which time she has developed a great love for all aspects of technology, as well as words themselves. Her experience spans B2B tech, with a lot of focus on cybersecurity, cloud, enterprise, digital transformation, and data centre. Her specialties are in news, thought leadership, features, white papers, and PR writing, and she is an experienced editor for both print and online publications., accessed 2-3-2025 //WG//

As we enter 2025, the frequency and sophistication of cyberattacks on critical national infrastructure (CNI) in the US are rising at an alarming rate. These attacks target the foundational systems that support everything from energy and water to transportation and communications, and the consequences are far-reaching and potentially catastrophic. They impact not just the operations of these services but also the very way of life for affected populations. The Deadly Cost of Ignoring OT Security Critical infrastructure attacks are particularly egregious because they have cascading effects. When a malicious actor compromises a power grid, water supply, or communication network, the impact can ripple across multiple sectors. Antonio Sanchez, Principal Cybersecurity Evangelist at Fortra, explains that the disruption of essential services, especially in such sensitive sectors, is akin to cyber-terrorism. “Successful attacks on critical infrastructure affect the way of life for that region,” he says. These attacks are not about isolated disruptions; they are deliberate and designed to cause widespread harm, often with financial or political motives. In the past, critical infrastructure systems were separated from the internet in what is known as air-gapped environments, which were considered secure. However, the growing trend toward integrating Operational Technology (OT) with Information Technology (IT) to reduce management costs has created new attack surfaces for malefactors. Sanchez emphasizes that these systems must maintain strict segmentation to limit access. “Organizations need to ensure they segment the network and separate IT from OT assets,” he advises. Critical Infrastructure in the Crosshairs The number of attacks on critical infrastructure in the US has surged in recent years. The public and private sector entities are facing a surging flood of high-profile threats. For example, we’ve seen attacks on energy grids, water systems, and transportation networks that have disrupted daily operations and raised national security concerns. Experts are predicting that this trend will only intensify in 2025. As technology progresses, there’s a corresponding progression in tactics used by malefactors. Adversaries are becoming more sophisticated, using highly cunning, targeted methods to infiltrate networks, perform reconnaissance, and remain undetected for extended periods of time. One of the most notorious groups behind a slew of attacks is Volt Typhoon, a Chinese state-sponsored threat actor. Bob Erdman, Associate Vice President, Research & Development at Fortra, describes Volt Typhoon’s motivations as geopolitical, claiming its aim is to compromise critical infrastructure in the United States and other Western countries to preposition access and maintain persistence with the assumed goal of being able to quickly launch attacks and create chaos if the geopolitical landscape changes. Hidden Breaches and Shadow Attackers Volt Typhoon’s tactics are a vivid demonstration of the evolving nature of critical infrastructure threats. The group doesn’t rely on traditional malicious code, which is more easily detectable. Instead, its approach focuses on maintaining long-term, stealthy access to targeted systems. Erdman explains, “Volt Typhoon does not typically rely on malware or ransomware as their objectives appear to be long and quiet persistence. They exploit unpatched vulnerabilities in publicly facing systems like firewalls, VPNs, and web servers to gain access.” After the Storm, the Fallout Recent attacks on US critical infrastructure have had unforgettable repercussions. One of the most publicized attacks was the Colonial Pipeline breach in 2021, which led to a widespread fuel shortage across the southeastern parts of the country. The attack, attributed to the DarkSide ransomware gang, laid bare the vulnerabilities in critical energy infrastructure and shone a light on the dire risks posed by cyberattacks on the nation’s energy systems. Similarly, the 2023 hack of US water systems was another wake-up call. Threat actors gained unauthorized access to a water treatment plant in Florida, attempting to alter chemical levels in the water supply. Luckily, the attack was uncovered before any real harm could happen. However, it was a harsh wake-up call to the vulnerability of utility systems to external threats. The fallout from these attacks includes financial losses, national security concerns, and general public distrust in the ability of governments and private companies to protect critical infrastructure. In the case of the Colonial Pipeline attack, for example, the company coughed up a ransom of $4.4 million, and the US government had to intervene to manage the crisis. Lessons from the Frontlines From these and other attacks, there are key lessons for public and private sector entities that manage critical infrastructure: Segmentation and Isolation: As Sanchez mentioned, IT and OT systems must be segmented to prevent unauthorized access. This is crucial in reducing the attack surface and limiting the damage in case of a breach. Patch Management: Erdman stresses the importance of patching vulnerabilities in publicly facing systems. Attackers often exploit unpatched systems to gain initial access, making timely patching and updates essential for defense. Incident Response and Training: Cybersecurity teams must be prepared for the worst. Running tabletop exercises and having detailed response plans in place can make a significant difference in minimizing the impact of an attack. Third-Party Penetration Testing: External experts can help identify vulnerabilities that internal teams may overlook. Regular penetration testing and adversary simulations can help organizations strengthen their defenses. All Eyes on 2025 As we look ahead to 2025, several trends are rearing up in the world of cyberattacks on critical infrastructure: Increased State-Sponsored Attacks: As geopolitical tensions rise, we can expect state-sponsored threat actors to have critical infrastructure in their crosshairs. Their goal is often not immediate disruption but rather long-term access and to prepare for future conflicts. Sophisticated Attack Methods: Attackers will continue to refine and hone their tactics, using tools that enable them to fly under the rader for longer periods. They will exploit unpatched externally facing systems, use hands-on keyboard to maintain persistence and remain stealthy, says Erdman. The Internet of Things (IoT) and Critical Infrastructure: The skyrocketing adoption of IoT devices in critical infrastructure is a whole new smorgasbord of opportunities for bad actors. These devices often have security slapped on as an afterthought instead of built-in from the ground up, making them prime and easy targets for exploitation. Cloud Migration Risks: As more critical infrastructure moves to cloud environments, the risk of cyberattacks soars. While cloud services offer scalability and cost savings, they also shatter the traditional perimeter and open up new vectors for potential breaches. A Matter of National and Public Safety The trend of rising cyberattacks on US critical national infrastructure in 2025 is a clear and present danger to national security and public safety. Malicious actors and state-sponsored groups have deep pockets and evil intentions and are growing increasingly sophisticated in their approach. They will exploit every possible vulnerability in IT and OT systems to get a foot in the door and maintain persistent access to critical networks. To mitigate these risks, entities across the board must prioritize cybersecurity measures such as network segmentation, patch management, incident response planning, and regular security testing. As the threat landscape evolves, so must the industry’s strategies for defending against these deadly, sophisticated attacks.

#### AI solves Palo Alto networks

Palo Alto Networks "What Is Generative AI in Cybersecurity?," Palo Alto Networks, Palo Alto Networks, Inc. is an American multinational cybersecurity company with headquarters in Santa Clara, California. The core product is a platform that includes advanced firewalls and cloud-based offerings that extend those firewalls to cover other aspects of security. The company serves over 70,000 organizations in over 150 countries, including 85 of the Fortune 100 (first half of the article isn’t rlly T, scroll a bit for the relevant part) https://www.paloaltonetworks.com/cyberpedia/generative-ai-in-cybersecurity, accessed 3-4-2025 //wyatt G?//

What Is Generative AI in Cybersecurity? 3 min. read Generative AI in cybersecurity represents a transformative shift in how security professionals predict, detect, and respond to threats. This technology leverages machine learning models, particularly those based on generative adversarial networks (GANs), to simulate cyberattacks and defensive strategies. The capability of generative AI to produce new data instances that mimic real-world datasets allows cybersecurity systems to evolve rapidly, adapting to new threats as they emerge. As these AI models undergo training, they become increasingly sophisticated in understanding the nuances of security data, enabling them to identify subtle patterns of malicious activity that might elude traditional detection methods. Using Generative AI in Cybersecurity Cybersecurity is one of the most critical use cases for generative AI. In cybersecurity, the power of generative AI cuts two ways: It is a powerful tool for those who perpetrate cybercrime and an equally powerful tool for cybersecurity teams responsible for preventing and mitigating the risk of cybercrime. Generative AI in security operations centers (SOCs) and security event and incident management (SEIM) has become essential in cybersecurity prevention and threat mitigation. In SOCs, AI models can identify patterns indicative of cyber threats, such as malware, ransomware, or unusual network traffic, that might elude traditional detection systems. Generative AI contributes to more sophisticated data analysis and anomaly detection in SIEM systems. By learning from historical security data, AI models can establish a baseline of normal network behavior and then flag deviations that may signify security incidents. Benefits of Generative AI in Cybersecurity Generative AI in cybersecurity significantly bolsters the ability to identify and neutralize cyber threats efficiently. By leveraging deep learning models, this technology can simulate advanced attack scenarios crucial for testing and enhancing security systems. This simulation capability is essential for developing strong defenses against known and emerging threats. Additionally, generative AI streamlines the implementation of security protocols by automating routine tasks, allowing cybersecurity teams to focus on more complex challenges. It also plays a pivotal role in training, providing realistic and dynamic scenarios that help improve the decision-making skills of IT security professionals. As cyber threats become more sophisticated, generative AI's adaptive and proactive nature becomes increasingly critical in maintaining the integrity and resilience of cybersecurity infrastructures. Enhancing Threat Detection and Response Generative AI can create sophisticated models that predict and identify unusual patterns indicative of cyber threats. This capability allows security systems to respond more rapidly and effectively than traditional methods. By continuously learning from data, generative AI adapts to new and evolving threats, ensuring that detection mechanisms are always several steps ahead of potential attackers. This proactive approach mitigates the risks of breaches and minimizes the impact of those that may occur. Security teams benefit from these advanced analytics by receiving detailed insights into threat vectors and attack strategies. This enables them to devise targeted responses and strengthen their defense mechanisms against future attacks. This dynamic interplay between detection and response fortifies cybersecurity frameworks, making them resilient against the increasingly sophisticated landscape of cyber threats. Automating Security Measures Generative AI streamlines cybersecurity by automating routine security tasks, such as configuring firewalls or scanning for vulnerabilities, freeing human resources for more complex issues. This technology also customizes security protocols by analyzing vast amounts of data to predict and enforce the most effective measures for each unique threat scenario. As a result, organizations can deploy dynamic security solutions that are both scalable and adaptable to changing threat landscapes. This automation enhances operational efficiency and significantly reduces the likelihood of human error, often a significant vulnerability in cybersecurity defenses. Scenario-Driven Cybersecurity Training Generative AI elevates cybersecurity training by creating realistic, scenario-based simulations that challenge professionals to respond to dynamic cyber threats. These AI-generated scenarios adapt in real-time, reflecting the evolving nature of cyber threats, thus providing a practical, immersive experience. Trainees can engage with various attack vectors and defense strategies, enhancing their ability to think critically and react swiftly under pressure. This hands-on approach builds deep technical expertise and improves decision-making skills, crucial for defending against sophisticated cyberattacks. Generative AI Applications in Cybersecurity Generative AI's ability to produce and utilize synthetic data enhances training protocols without compromising absolute data integrity. Its integration into cybersecurity operations transforms traditional defensive measures into proactive, adaptive strategies that keep pace with the rapidly changing digital threats. Detecting and Creating Phishing Attacks The use of generative AI has opened up new possibilities in both detecting and creating phishing attacks. While traditional anti-malware solutions focus on identifying known malicious code, generative AI can potentially identify more sophisticated and complex phishing attacks. By analyzing patterns in legitimate communications, such as email messages, generative AI can identify subtle signs of phishing emails that may otherwise go undetected. This can help individuals and organizations stay one step ahead of cybercriminals and protect themselves from potentially devastating attacks. Data Masking and Privacy Preservation Generative AI has the remarkable ability to create synthetic data that closely resembles real data sets. This is particularly useful when working with sensitive information that needs to be protected. By generating data that mimics the real thing, organizations can avoid the risks of using actual data sets that may contain confidential or personally identifiable information. This synthetic data can be used to train security models and algorithms without compromising the privacy of individuals or exposing sensitive data. In other words, generative AI can help organizations preserve data privacy and protect against security breaches while leveraging machine learning and data analysis benefits. Automated Security Policy Generation Automated security policy generation can assist organizations in creating security policies customized to their specific context and needs. Analyzing an organization's environment and security requirements allows for generating optimized policies to provide an appropriate level of security while also considering the organization's unique characteristics. This approach ensures that the security policies are effective, relevant, and applicable to the organization's goals and objectives. Incident Response Generative AI has the potential to revolutionize incident response by providing an automated approach to handling security incidents. One of the key benefits of generative AI is its ability to generate appropriate actions or scripts based on the nature of the incident. Cyber teams can then automate the initial steps of the response process, generating immediate responses to standard threats, categorizing incidents based on severity, and recommending mitigation strategies. With generative AI, cyber teams can quickly isolate affected systems to minimize the damage of a security breach. Generative AI can simulate various response strategies, enabling teams to evaluate the effectiveness of different approaches in real time and strengthening decision-making during a cybersecurity incident. By automating incident response in this way, organizations can save time, reduce costs, and improve overall security posture. Behavior Analysis and Anomaly Detection Behavior analysis and anomaly detection are essential techniques used in cybersecurity to detect potential security threats. Generative AI can play a significant role in this process by generating models of normal user or network behavior and identifying deviations from the expected behavior. These deviations, also known as anomalies, may indicate a security breach or unauthorized access to the system. By analyzing these anomalies and comparing them to the expected behavior, security professionals can identify potential threats and take appropriate measures to prevent any security incidents. Reporting Generative AI streamlines the creation of comprehensive, understandable cybersecurity reports. It can synthesize data from various sources into coherent reports, highlighting key findings, trends, and potential vulnerabilities. This saves time and ensures the reports are more accurate and informative, providing valuable insights for decision-makers. Generative AI can identify and highlight patterns of interest or anomalies in the data, providing a more profound analysis that can be crucial for understanding the nuances of cybersecurity threats and defenses. AI-generated reports can be tailored to different audiences, from technical teams requiring in-depth analysis to executive summaries for leadership, enhancing communication of cybersecurity issues across an organization. Generative AI Cybersecurity Risks While generative AI has become an increasingly valuable tool for cybersecurity teams, it is also becoming a powerful weapon for cybercriminals. The same capabilities that make generative AI powerful for threat detection and incident response can be used maliciously. For example, cybercriminals can exploit the ability of generative AI to analyze and understand complex patterns to find vulnerabilities in cybersecurity systems. As generative AI models become more sophisticated, cybercriminals could reverse-engineer them to bypass security protocols. Adversaries and generative AI Adversaries are already using generative AI to launch more sophisticated attacks. Their use of the technology will continue rising because it effectively brings speed, insight, automation, and imitation to their cybercrime weapons. Typical uses of generative AI by cybercriminals include: Phishing and Social Engineering Generative AI generates personalized content that mimics legitimate communication, tricking recipients into divulging sensitive information or downloading malware. Deepfakes Audio or video powered by generative AI can impersonate individuals, manipulate public opinion, or conduct sophisticated social engineering attacks. Malware Development Generative AI can create malware that adapts and evolves to evade detection by traditional antivirus and malware detection tools. Exploiting Vulnerabilities Generative AI can analyze individuals, systems, and software for vulnerabilities to launch more targeted attacks. Automated Hacking Generative AI can automate certain aspects of hacking, allowing cybercriminals to launch large-scale attacks that are more complex and difficult to detect and counter. Bypassing Security Measures AI models can be trained to mimic user behavior or generate inputs that can trick biometric security systems, CAPTCHAs, and other AI-based security solutions. Securing the AI Pipeline Securing the AI pipeline means safeguarding the entire lifecycle of an AI system, from data collection and model training to deployment and maintenance. This encompasses protecting data used for training AI models, ensuring the integrity of AI algorithms, and guarding against unauthorized access or tampering. It also involves continuously monitoring and updating the AI systems to protect against emerging threats. Securing the AI pipeline is critical for several reasons: Protecting sensitive data from being compromised is particularly important when AI systems handle personal or confidential information. Ensuring AI systems' reliability and trustworthiness is essential for their acceptance and effective utilization. Guarding against manipulating AI systems can have serious consequences, from spreading misinformation to causing physical harm in AI-controlled environments. Best security practices in the AI pipeline include resilient data governance, encryption and secure coding practices, multi-factor authentication, and continuous monitoring and response. As AI continues to evolve, so do the risks to cybersecurity. The following predictions provide several insights into the direction of AI in cybersecurity. 1. More sophisticated AI-powered attacks With AI, attackers can create more sophisticated and targeted attacks that bypass traditional security measures. 2. Greater use of AI for cyber defense As AI evolves, it will become more widely used for cybersecurity, including threat detection, analysis, and response. 3. More regulations and standards As the risks of AI-powered attacks increase, more regulations and standards will be put in place to ensure the responsible and ethical use of AI. 4. Greater emphasis on human oversight As AI becomes more prevalent in cybersecurity, it will become increasingly important to have human oversight and decision-making to ensure that AI is being used effectively and ethically. 5. More investment in AI cybersecurity As the risks of AI-powered attacks increase, more will be invested in developing AI-powered cybersecurity solutions to stay ahead of attackers. The future of generative AI is closely tied to the ability of cybersecurity leaders to harness its power to ensure that the technology is used safely and securely across all industries and use cases. This means maximizing the use of generative AI for prevention, protection, response, and prediction.

#### AI educates general employees Keepnet labs 24

Keepnet Labs 2024-12-06 "How Generative AI is Transforming Security Behavior and Culture Programs," Keepnet Labs is a cybersecurity company specializing in human risk management. They utilize AI-driven phishing simulations, adaptive training programs, and automated threat response mechanisms to enhance organizational security. Their platform is designed to reduce employee-driven threats by providing tailored training that adapts to individual user behavior and risk levels. Keepnet Labs aims to foster a robust security culture within organizations by equipping employees with the knowledge and skills necessary to recognize and respond to potential threats effectively. The company emphasizes continuous improvement and real-time analytics to help organizations stay ahead of evolving cyber threats. https://keepnetlabs.com/blog/how-generative-ai-is-transforming-security-behavior-and-culture-programs, This article was updated on February 14, 2025, accessed 3-4-2025 //wyatt G?//

\*for clarification SBCP= security behavior and culture programs (basically programs that teach employees to not get hacked)\*

Human error remains a key vulnerability, with 82% of breaches involving the human element (Verizon DBIR, 2023). This underscores the importance of security behavior and culture programs (SBCPs), which aim to mitigate human risks by fostering awareness and proactive security behaviors. With the advent of generative AI, these programs are undergoing a dramatic transformation. AI offers the ability to create personalized, engaging, and scalable training modules that elevate security awareness and embed a culture of resilience. In this blog, we’ll explore: The current challenges in SBCPs. How generative AI addresses these challenges. Practical use cases and future possibilities. What are the Current Challenges in SBCPs? While SBCPs are essential for mitigating risks, organizations face persistent hurdles: Low Engagement with Traditional Awareness Training Static and one-size-fits-all content fails to capture employee interest or cater to diverse learning styles. Limited Personalization Traditional SBCPs often overlook role-specific risks, leaving employees ill-equipped to tackle threats relevant to their roles. Scalability and Localization Global organizations struggle to scale security awareness training across geographies while addressing cultural nuances. Ineffective Metrics Measuring the success of security awareness initiatives remains a challenge. For insights on relevant metrics, refer to our blog on evaluating security awareness efforts. Generative AI offers solutions to these limitations, creating opportunities for truly transformative SBCPs. How Generative AI Reshapes Security Programs Generative AI addresses these challenges through innovative features, driving measurable improvements in security behavior and culture: Creating Personalized and Adaptive Training AI analyzes employee performance data to deliver customized phishing simulations and training content. By tailoring scenarios to individual roles, employees gain relevant skills to identify and respond to threats. Learn how Keepnet Labs applies behavioral science to build highly effective AI-driven training programs. Developing Engaging Content Generative AI can produce immersive scenarios, such as realistic vishing or smishing attacks, enhancing employees’ ability to detect and neutralize such threats. Gamification features further boost engagement by turning learning into a competitive and rewarding experience Enabling Real-Time Feedback Generative AI tools provide immediate feedback during simulations, helping employees identify mistakes and learn from them instantly. This continuous improvement loop ensures lasting behavior change. Scaling Across Global Teams AI-powered platforms offer multilingual training content, enabling organizations to roll out security initiatives seamlessly across regions. For instance, localized phishing simulations prepare employees for region-specific attack tactics. Discover more in our blog on harnessing AI and machine learning in security awareness training. AI’s Impact on Security Awareness Training: The Teknosa Success Story Teknosa, a leading technology retailer with 2,500 employees and 211 stores across 68 locations, faced a growing threat of vishing attacks—voice phishing scams targeting their customer service and sales teams. These scams not only disrupted operations but also posed significant financial and reputational risks. To combat this, Teknosa partnered with Keepnet Labs to implement an AI-driven security behavior program, achieving outstanding results within just 90 days. Key Outcomes of Teknosa’s Program 80% Improvement in Identifying Voice Scams: Employees' ability to recognize and report fake phone calls increased dramatically. $439,250 in Potential Loss Prevention Annually: The company avoided significant financial losses due to reduced scam success rates. $30,000 Saved in Incident Response Costs Annually: Streamlined processes cut response times and associated costs by over 60%. These results highlight how AI-powered tools and real-time feedback can revolutionize security awareness training and help organizations build robust defenses against emerging threats. For more information on AI based security awareness tools, visit top security awareness training solutions for 2025. The Role of Metrics in AI-Driven SBCPs Measuring the success of SBCPs is crucial for continuous improvement. With AI, organizations can leverage: Behavioral Metrics: Track phishing simulation results and human risk scores. Engagement Data: Monitor participation rates and user feedback to optimize content. Performance Benchmarks: Compare results across departments or regions. Learn more about effective metrics for evaluating security awareness. AI’s Role in Building a Resilient Security Culture Generative AI goes beyond training by instilling long-term cultural change: Promoting Accountability: Transparent human risk scores incentivize better security behavior. Encouraging Collaboration: AI-driven simulations foster teamwork through incident response drills. Enhancing Compliance: AI tailors training to meet specific regulatory needs, streamlining compliance efforts. Explore how AI’s benefits extend into broader security applications in our blog on AI’s pros and cons in cybersecurity. How Keepnet Leverages AI to Transform Security Awareness Keepnet is at the forefront of cybersecurity innovation, offering a comprehensive suite of AI-powered products designed to address human risks and bolster organizational defenses. With a focus on empowering businesses to counter sophisticated social engineering attacks, Keepnet integrates artificial intelligence into its tools to deliver personalized, engaging, and scalable solutions. Here’s how Keepnet’s AI-driven products transform security awareness and behavior programs: Phishing Simulator Keepnet’s Phishing Simulator enables organizations to create real-world phishing campaigns using AI. Dynamic Personalization: Tailors phishing emails based on job roles, behaviors, and risk levels. Advanced Threat Simulation: Generates complex scenarios, including spear phishing and quishing, to test employee readiness. Actionable Insights: Provides detailed analytics on employee responses to enhance awareness programs. Learn more about the Phishing Simulator. Vishing Simulator Voice phishing, or vishing, is a growing threat, and Keepnet’s Vishing Simulator combats this effectively. AI-Generated Calls: Uses AI-driven text-to-speech technology to create realistic scam calls tailored to your organization. Behavior Tracking: Identifies weak points in employee responses, offering insights for improvement. Localized Campaigns: Supports multilingual training to address regional threats. Discover the Vishing Simulator. Smishing Simulator The Smishing Simulator addresses the rising risk of SMS phishing by training employees to spot and respond to fraudulent messages. Customizable Scenarios: Simulates attacks such as fake delivery notifications or urgent banking alerts. Real-Time Feedback: Instantly informs employees of mistakes, fostering immediate learning. Trend Analysis: Tracks smishing trends and tailors training to address current threats. Explore the Smishing Simulator. Quishing Simulator With QR code phishing, or quishing, on the rise, Keepnet’s Quishing Simulator educates employees about this evolving threat. AI-Driven QR Codes: Creates malicious QR code simulations to test employee vigilance. Scenario Customization: Adapts to your industry’s specific use cases, such as fake parking tickets or invoices. Awareness Building: Raises organizational awareness about emerging attack vectors. Learn more about the Quishing Simulator. Awareness Educator Keepnet’s Security Awareness Educator delivers engaging, AI-powered learning experiences to help employees stay ahead of cyber threats. Behavioral Science Integration: Incorporates nudges and gamified elements to sustain learning retention. Adaptive Content: Uses AI to tailor lessons based on individual performance and knowledge gaps. Seamless Scalability: Delivers training across global teams with localized content. Find out about the Security Awareness Training. Incident Responder Responding to email-based threats is faster and more efficient with the Incident Responder. AI-Assisted Threat Removal: Automates the detection and removal of phishing emails from employee inboxes. Accelerated Response Time: Reduces incident response times from hours to minutes. Customizable Workflows: Adapts to your existing IT infrastructure for seamless integration. Explore the Incident Responder. Human Risk Management Platform Keepnet’s Human Risk Management Platform offers a centralized hub for monitoring and reducing human risks across your organization. Human Risk Scoring: Uses AI to generate individual and team risk scores based on behaviors and training results. Comprehensive Reporting: Benchmarks performance across departments and industries. Integrated Defense: Unites all Keepnet tools for a holistic approach to human risk mitigation. Discover the Human Risk Management Platform.

#### Critical infrastructure loss causes societal collapse Friedemann 16

Friedemann 16 (Alice Friedemann, transportation expert, founder of EnergySkeptic.com and author of “When Trucks Stop Running, Energy and the Future of Transportation,” worked at American Presidential Lines for 22 years, where she developed computer systems to coordinate the transit of cargo between ships, rail, trucks, and consumers, citing Dr. Peter Vincent Pry. Pry is executive director of the Task Force on National and Homeland Security, a Congressional advisory board dedicated to achieving protection of the United States from electromagnetic pulse and other threats. Dr. Pry is also the director of the United States Nuclear Strategy Forum, an advisory body to Congress on policies to counter weapons of mass destruction. Dr. Pry has served on the staffs of the Congressional Commission on the Strategic Posture of the United States, the Commission to Assess the Threat to the U.S. from an EMP Attack, the House Armed Services Committee, as an intelligence officer with the CIA, and as a verification analyst at the U.S. Arms Control and Disarmament Agency. 1-24-16, accessed 1/1/19 “Electromagnetic pulse threat to infrastructure (U.S. House hearings)” <http://energyskeptic.com/2016/the-scariest-u-s-house-session-ever-electromagnetic-pulse-and-the-fall-of-civilization/>)

Modern civilization cannot exist for a protracted period without electricity. Within days of a blackout across the U.S., a blackout that could encompass the entire planet, emergency generators would run out of fuel, telecommunications would cease as would transportation due to gridlock, and eventually no fuel. Cities would have no running water and soon, within a few days, exhaust their food supplies. Police, Fire, Emergency Services and hospitals cannot long operate in a blackout. Government and Industry also need electricity in order to operate. The EMP Commission warns that a natural or nuclear EMP event, given current unpreparedness, would likely result in societal collapse. Terrorists, criminals, and even lone individuals can build a non-nuclear EMP weapon without great trouble or expense, working from Unclassified designs publicly available on the internet, and using parts available at any electronics store. In 2000, the Terrorism Panel of the House Armed Services Committee sponsored an experiment, recruiting a small team of amateur electronics enthusiasts to attempt constructing a radiofrequency weapon, relying only on unclassified design information and parts purchased from Radio Shack. The team, in 1 year, built two radiofrequency weapons of radically different designs. One was designed to fit inside the shipping crate for a Xerox machine, so it could be delivered to the Pentagon mail room where (in those more unguarded days before 9/11) it could slowly fry the Pentagon’s computers. The other radiofrequency weapon was designed to fit inside a small Volkswagon bus, so it could be driven down Wall Street and disrupt computers— and perhaps the National economy. Both designs were demonstrated and tested successfully during a special Congressional hearing for this purpose at the U.S. Army’s Aberdeen Proving Ground. Radiofrequency weapons are not merely a hypothetical threat. Terrorists, criminals, and disgruntled individuals have used home-made radiofrequency weapons. The U.S. military and foreign militaries have a wide variety of such weaponry. Moreover, non-nuclear EMP devices that could be used as radiofrequency weapons are publicly marketed for sale to anyone, usually advertised as ‘‘EMP simulators.’’ For example, one such simulator is advertised for public sale as an ‘‘EMP Suitcase.’’ This EMP simulator is designed to look like a suitcase, can be carried and operated by one person, and is purpose-built with a high energy radiofrequency output to destroy electronics. However, it has only a short radius of effect. Nonetheless, a terrorist or deranged individual who knows what he is doing, who has studied the electric grid for a major metropolitan area, could—armed with the ‘‘EMP Suitcase’’— black out a major city. A CLEAR AND PRESENT DANGER. An EMP weapon can be used by state actors who wish to level the battlefield by neutralizing the great technological advantage enjoyed by U.S. military forces. EMP is also the ideal means, the only means, whereby rogue states or terrorists could use a single nuclear weapon to destroy the United States and prevail in the War on Terrorism or some other conflict with a single blow. The EMP Commission also warned that states or terrorists could exploit U.S. vulnerability to EMP attack for coercion or blackmail: ‘‘Therefore, terrorists or state actors that possess relatively unsophisticated missiles armed with nuclear weapons may well calculate that, instead of destroying a city or military base, they may obtain the greatest political-military utility from one or a few such weapons by using them—or threatening their use—in an EMP attack.’’ The EMP Commission found that states such as Russia, China, North Korea, and Iran have incorporated EMP attack into their military doctrines, and openly describe making EMP attacks against the United States. Indeed, the EMP Commission was established by Congress partly in response to a Russian nuclear EMP threat made to an official Congressional Delegation on May 2, 1999, in the midst of the Balkans crisis. Vladimir Lukin, head of the Russian delegation and a former Ambassador to the United States, warned: ‘‘Hypothetically, if Russia really wanted to hurt the United States in retaliation for NATO’s bombing of Yugoslavia, Russia could fire an SLBM and detonate a single nuclear warhead at high altitude over the United States. The resulting EMP would massively disrupt U.S. communications and computer systems, shutting down everything.’’ China’s military doctrine also openly describes EMP attack as the ultimate asymmetric weapon, as it strikes at the very technology that is the basis of U.S. power. Where EMP is concerned, ‘‘The United States is more vulnerable to attacks than any other country in the world’’: ‘‘Some people might think that things similar to the ‘Pearl Harbor Incident’ are unlikely to take place during the information age. Yet it could be regarded as the ‘Pearl Harbor Incident’ of the 21st Century if a surprise attack is conducted against the enemy’s crucial information systems of command, control, and communications by such means as… electromagnetic pulse weapons… Even a superpower like the United States, which possesses nuclear missiles and powerful armed forces, cannot guarantee its immunity…In their own words, a highly computerized open society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems and from power plants to iron and steel works, relies entirely on computer networks… When a country grows increasingly powerful economically and technologically…it will become increasingly dependent on modern information systems… The United States is more vulnerable to attacks than any other country in the world.’’ Iran—the world’s leading sponsor of international terrorism—in military writings openly describes EMP as a terrorist weapon, and as the ultimate weapon for prevailing over the West: ‘‘If the world’s industrial countries fail to devise effective ways to defend themselves against dangerous electronic assaults, then they will disintegrate within a few years… American soldiers would not be able to find food to eat nor would they be able to fire a single shot.’’ The threats are not merely words. The EMP Commission assesses that Russia has, as it openly declares in military writings, probably developed what Russia describes as a ‘‘Super-EMP’’ nuclear weapon—specifically designed to generate extraordinarily high EMP fields in order to paralyze even the best protected U.S. strategic and military forces. China probably also has Super-EMP weapons. North Korea too may possess or be developing a Super-EMP nuclear weapon, as alleged by credible Russian sources to the EMP Commission, and by open-source reporting from South Korean military intelligence. But any nuclear weapon, even a low-yield first generation device, could suffice to make a catastrophic EMP attack on the United States. Iran, although it is assessed as not yet having the bomb, is actively testing missile delivery systems and has practiced launches of its best missile, the Shahab–III, fuzing for high- altitude detonations, in exercises that look suspiciously like training for making EMP attacks. As noted earlier, Iran has also practiced launching from a ship a Scud, the world’s most common missile—possessed by over 60 nations, terrorist groups, and private collectors. A Scud might be the ideal choice for a ship-launched EMP attack against the United States intended to be executed anonymously, to escape any last-gasp U.S. retaliation. Unlike a nuclear weapon detonated in a city, a high-altitude EMP attack leaves no bomb debris for forensic analysis, no perpetrator ‘‘fingerprints.’’ Under present levels of preparedness, communications would be severely limited, restricted mainly to those few military communications networks that are hardened against EMP. Today’s microelectronics are the foundation of our modern civilization, but are over 1 million times more vulnerable to EMP than the far more primitive and robust electronics of the 1960s, that proved vulnerable during nuclear EMP tests of that era. Tests conducted by the EMP Commission confirmed empirically the theory that, as modern microelectronics become ever smaller and more efficient, and operate ever faster on lower voltages, they also become ever more vulnerable, and can be destroyed or disrupted by much lower EMP field strengths. Microelectronics and electronic systems are everywhere, and run virtually everything in the modern world. All of the civilian critical infrastructures that sustain the economy of the United States, and the lives of 310 million Americans, depend, directly or indirectly, upon electricity and electronic systems. Of special concern is the vulnerability to EMP of the Extra-High-Voltage (EHV) transformers, that are indispensable to the operation of the electric grid. EHV transformers drive electric current over long distances, from the point of generation to consumers (from the Niagara Falls hydroelectric facility to New York City, for example). The electric grid cannot operate without EHV transformers—which could be destroyed by an EMP event. The United States no longer manufactures EHV transformers. They must be manufactured and imported from overseas, from Germany or South Korea, the only two nations in the world that manufacture such transformers for export. Each EHV transformer must be custom-made for its unique role in the grid. A single EHV transformer typically requires 18 months to manufacture. The loss of large numbers of EHV transformers to an EMP event would plunge the United States into a protracted blackout lasting years, with perhaps no hope of eventual recovery, as the society and population probably could not survive for even 1 year without electricity. Another key vulnerability to EMP are Supervisory Control And Data Acquisition systems (SCADAs). SCADAs essentially are small computers, numbering in the millions and ubiquitous everywhere in the critical infrastructures, that perform jobs previously performed by hundreds of thousands of human technicians during the 1960s and before, in the era prior to the microelectronics revolution. SCADAs do things like regulating the flow of electricity into a transformer, controlling the flow of gas through a pipeline, or running traffic control lights. SCADAs enable a few dozen people to run the critical infrastructures for an entire city, whereas previously hundreds or even thousands of technicians were necessary. Unfortunately, SCADAs are especially vulnerable to EMP. EHV transformers and SCADAs are the most important vulnerabilities to EMP, but are by no means the only vulnerabilities. Each of the critical infrastructures has their own unique vulnerabilities to EMP: The National electric grid, with its transformers and generators and electronic controls and thousands of miles of power lines, is a vast electronic machine—more vulnerable to EMP than any other critical infrastructure. Yet the electric grid is the most important of all critical infrastructures, and is in fact the keystone supporting modern civilization, as it powers all the other critical infrastructures. As of now it is our technological Achilles Heel. The EMP Commission found that, if the electric grid collapses, so too will collapse all the other critical infrastructures. But, if the electric grid can be protected and recovered, so too all the other critical infrastructures can also be restored. Transportation is a critical infrastructure because modern civilization cannot exist without the goods and services moved by road, rail, ship, and air. Cars, trucks, locomotives, ships, and aircraft all have electronic components, motors, and controls that are potentially vulnerable to EMP. Gas stations, fuel pipelines, and refineries that make petroleum products depend upon electronic components and cannot operate without electricity. Given our current state of unpreparedness, in the aftermath of a natural or nuclear EMP event, transportation systems would be paralyzed. Traffic control systems that avert traffic jams and collisions for road, rail, and air depend upon electronic systems, that the EMP Commission discovered are especially vulnerable to EMP. Communications is a critical infrastructure because modern economies and the cohesion and operation of modern societies depend to a degree unprecedented in history on the rapid movement of information—accomplished today mostly by electronic means. Telephones, cell phones, personal computers, television, and radio are all directly vulnerable to EMP, and cannot operate without electricity. Satellites that operate at Low-Earth-Orbit (LEO) for communications, weather, scientific, and military purposes are vulnerable to EMP and to collateral effects from an EMP attack. Within weeks of an EMP event, the LEO satellites, which comprise most satellites, would probably be inoperable. Banking and finance are the critical infrastructure that sustain modern economies. Whether it is the stock market, the financial records of a multinational corporation, or the ATM card of an individual—financial transactions and record keeping all depend now at the macro- and micro-level upon computers and electronic automated systems. Many of these are directly vulnerable to EMP, and none can operate without electricity. The EMP Commission found that an EMP event could transform the modern electronic economy into a feudal economy based on barter. Food has always been vital to every person and every civilization. The critical infrastructure for producing, delivering, and storing food depends upon a complex web of technology, including machines for planting and harvesting and packaging, refrigerated vehicles for long-haul transportation, and temperature-controlled warehouses. Modern technology enables over 98 percent of the U.S. National population to be fed by less than 2 percent of the population. Huge regional warehouses that resupply supermarkets constitute the National food reserves, enough food to feed the Nation for 30–60 days at normal consumption rates, the warehoused food preserved by refrigeration and temperature control systems that typically have enough emergency electrical power (diesel or gas generators) to last only about an average of 3 days. Experience with storm-induced blackouts proves that when these big regional food warehouses lose electrical power, most of the food supply will rapidly spoil. Farmers, less than 2 percent of the population as noted above, cannot feed 310 million Americans if deprived of the means that currently makes possible this technological miracle. Water too has always been a basic necessity to every person and civilization, even more crucial than food. The critical infrastructure for purifying and delivering potable water, and for disposing of and treating waste water, is a vast networked machine powered by electricity that uses electrical pumps, screens, filters, paddles, and sprayers to purify and deliver drinkable water, and to remove and treat waste water. Much of the machinery in the water infrastructure is directly vulnerable to EMP. The system cannot operate without vast amounts of electricity supplied by the power grid. A natural or nuclear EMP event would immediately deprive most of the U.S. National population of running water. Many natural sources of water—lakes, streams, and rivers—would be dangerously polluted by toxic wastes from sewage, industry, and hospitals that would backflow from or bypass wastewater treatment plants, that could no longer intake and treat pollutants without electric power. Many natural water sources that would normally be safe to drink, after an EMP event, would be polluted with human wastes including feces, industrial wastes including arsenic and heavy metals, and hospital wastes including pathogens. Emergency services such as police, fire, and hospitals are the critical infrastructure that upholds the most basic functions of government and society—preserving law and order, protecting property and life. Experience from protracted storm-induced blackouts has shown, for example in the aftermath of Hurricanes Andrew and Katrina, that when the lights go out and communications systems fail and there is no gas for squad cars, fire trucks, and ambulances, the worst elements of society and the worst human instincts rapidly takeover. The EMP Commission found that, given our current state of unpreparedness, a natural or nuclear EMP event could create anarchic conditions that would profoundly challenge the existence of social order.

erful, the dangers of unintended or accidental escalation can only grow more severe.

## 5---Bias (25)

#### Grading bias is an issue Dhliwal 20

Tasminda K. Dhaliwal 20, 7-20-2020, "Educator bias is associated with racial disparities in student achievement and discipline," Brookings, https://www.brookings.edu/articles/educator-bias-is-associated-with-racial-disparities-in-student-achievement-and-discipline/, Assistant Professor of Education Policy - Michigan State University accessed 2-19-2025 //wyatt G?//

Education leaders across the country have joined the chorus condemning the recent police killings of Black people. Statements released by superintendents and teachers’ unions suggest a reckoning with the institutional racism and bias embedded within schools. Some school districts have seized on this period of national reflection to propose actions and policy changes intended to reduce racial disparities in education and create anti-racist school systems. Education scholars have hypothesized that implicit bias, or unconscious beliefs, may contribute to stubborn racial disparities in education, such as differences in student achievement and school discipline between Black and white students. For instance, teachers’ unconscious racial beliefs could produce biased evaluations of students’ academic performance, which translates into real implications for educational attainment. Yet evidence linking teachers’ bias to these disparities has been lacking. In a study published in Educational Researcher this month, we examine teachers’ implicit biases and their correlates. Our findings, described in more detail below, largely confirm hypotheses that connect county-level teacher implicit bias to disparities in achievement and school discipline between Black and white students at the county level. Measuring implicit bias requires tapping into implicit cognition—a difficult task. In our study, we leverage data from Project Implicit’s white-Black implicit association test (IAT). The white-Black IAT assesses test-takers’ automatic associations for white and Black people. The IAT identifies biases through a series of high-speed computerized tasks, which compare how quickly individuals associate white and Black people with certain attitudes (e.g., favorable, unfavorable). We pair these data with nationwide data on racial achievement gaps, made available by the Stanford Education Data Archive, and racial discipline gaps, made available by the Civil Rights Data Collection. It is important to note that our research design does not allow us to definitively conclude that teachers’ biases cause racial disparities in student outcomes or identify the mechanisms behind the bias-outcome relationship. Still, the results described below persist even after accounting for important contextual factors (e.g., socio-economic status and segregation measures) and instructional factors (e.g., per-pupil expenditures and student/teacher ratio). Our first key finding is that educators, like the general public, hold “slight” pro-white/anti-Black implicit bias and that this bias is more strongly related to individual factors than contextual factors. Teachers of color show lower average bias than white teachers, with Black teachers showing the least anti-Black bias. But teachers of color are a far smaller share of the teaching workforce than white teachers. Female teachers, who continue to substantially outnumber male teachers, show lower average bias. We also find that teachers working in counties with larger shares of Black students exhibit lower levels of implicit bias. This might be because teachers with lower bias prefer to work in counties with more Black students and/or that working in schools serving more Black students leads to lower bias. Regardless, there is some relief that we do not observe the reverse pattern. Our second key finding is that we observe larger racial disparities in test scores and suspensions in counties with stronger implicit and explicit pro-white/anti-Black bias among teachers. In Figure 1, we plot predicted white-Black differences in test scores for counties with varying levels of teacher implicit bias (assuming average values on other contextual characteristics). The solid vertical line identifies counties with average teacher bias; in these counties, Black students score approximately 0.55 standard deviations (SDs) lower than white students on tests. Contrastingly, counties with “little or no” pro-White/anti-Black teacher bias lie to the left of the dashed vertical line; for these counties, test score differences range up to approximately 0.40 SDs. The predicted differences in disparities emerge even after accounting for several context-varying factors that contribute to achievement or opportunity gaps, including individual-based factors (e.g., poverty) and school-based factors (e.g., racial segregation). Unfortunately, very few counties exhibit low levels of teacher implicit bias: Of the 764 we analyze, only in seven were teachers, on average, demonstrating “little or no” pro-white/anti-Black bias. Black students in counties where teachers hold average levels of bias also have predicted probabilities of being suspended that are far greater than those for Black students in counties with low pro-white/anti-Black bias. In Figure 2, we show the predicted probabilities for in-school (left) and out-of-school suspensions (right) for Black and white students. Again, the solid vertical line identifies counties with average teacher bias and the dashed vertical line helps delineate those with low pro-white/anti-Black bias. In counties with average bias, we estimate that Black students have a 13% and 16% predicted probability of being suspended in and out of school, respectively, whereas white students have a 5% probability of being suspended either in or out of school. Meanwhile, Black students in counties with low teacher bias have up to an 8% predicted probability of being suspended both in and out of school, while white students have up to 2% and 4% suspension probabilities. These results are generally similar to those from a study published last year that examined implicit biases of the broader population and racial discipline gaps using a slightly different analytical approach. Overall, our research suggests that teachers’ biases may contribute to the seemingly entrenched disparities in academic achievement and suspensions between Black and white students. Education reformers and policymakers have sought to reduce unequal outcomes for Black students for decades. Many of these efforts, even when undertaken by well-intentioned educators, have largely failed. The undercurrents of educator implicit bias could be part of the explanation as to why well-meaning reforms to address racial disparities have little to show for. But addressing implicit bias is likely more complicated than requiring educators attend a training. In fact, recent evidence on interventions designed to reduce implicit bias show little overall impact on behavior. That may be because implicit bias has a large contextual component. According to some scholars of implicit bias, aggregate measures of bias, like the ones we use, are better thought of as measuring the psychological residue of structural racism (e.g., redlining and policing) rather than fixed attitudes that people hold regardless of the context. In other words, as long as structural racism looms large, implicit biases will too. Working to both dismantle the contextual factors that induce greater implicit bias and attending to individual teachers’ implicit attitudes is likely necessary for this most recent wave of action to realize its potential.

#### AI is a solution Paykamian 23

Brandon Paykamian 23, 5-8-2023, "Can Artificial Intelligence Help Mitigate Grading Bias?," GovTech, <https://www.govtech.com/education/higher-ed/can-artificial-intelligence-help-mitigate-grading-bias>, Brandon Paykamian is a journalist and columnist from Johnson City, Tennessee, known for his work in local journalism and various publications. He has a background in Mass Communications and has written on social and political issues, Brandon Paykamian is a former staff writer for the Center for Digital Education. accessed 2-19-2025 //wyatt G?//

The ed-tech platform Copyleaks has developed an AI-assisted tool to eliminate human bias and discrepancies in the grading process, aiming to provide consistency in grading while helping teachers save time. Much of the recent focus on artificial intelligence-driven ed-tech tools has been on ChatGPT and keeping students honest, but could AI keep graders on track too? The ed-tech platform Copyleaks is betting so, touting a new AI-assisted tool to help educators grade exams and address concerns about how human biases can affect the grading process. According to CEO and co-founder Alon Yamin, Copyleaks’ anti-plagiarism and grading platform was among the first to develop and launch AI-detection functions this year to catch students using generative AI to complete assignments, given widespread concerns about AI's potential to enable academic dishonesty. However, he said, the company recently started noticing the need for additional AI-driven functions to address discrepancies in the grading process. “I think generally once humans are in the process, you will always have bias. Think about a human grader grading thousands of assignments. The solution we provided is focused on high volumes of exams … Naturally, humans are affected by external factors, and there could be a day where I am waking up a bit tired or angry, and it can affect the way I am grading the exams,” he said. “That led us to think about how we can solve this bias, as well as how we can automate this whole process away where we’re talking about thousands, tens of thousands and sometimes millions of exams." According to Yamin, Copyleaks users scan and grade about 10 million documents a month, and most of the company's clientele is in the U.S. education market. Kinsey Rawe, senior vice president and general manager of Courseware and Instructional Services for Imagine Learning, noted that tools like Copyleaks' new AI Grader can lighten the workload of educators tasked with grading scores of assignments and exams and providing feedback. “Copyleaks gives us an opportunity to help teachers save precious time that they can utilize to provide more personalized instruction to students while helping them understand the importance of academic integrity,” Rawe wrote in an email to Government Technology. According to a 2020 research article in EducationNext by David Quinn, an associate professor of education at the University of Southern California, his own experiment found that teachers were about 4.7 percent more likely to rate writing from white students to be at or above grade level when compared to “identical writing from a Black child.” What’s more, Quinn wrote, anti-bias training has generally proven less than promising when it comes to addressing and reducing such grading biases.At the same time, concerns have been raised about algorithmic bias in AI and its impact on higher education, such as with enrollment-management algorithms that some say have filtered out low-income, female and non-white applicants who are more likely to need larger aid packages. And there are examples of past mishaps involving AI-driven grading: In August 2020, the BBC reported that an algorithm used to grade A-level exams had to be scrapped after it gave far lower scores than expected. But because one or a handful of exams can alter a student's entire future, Copyleaks Chief Operating Officer Shouvik Paul said some education systems have sought to address grading biases by hiring more than one grader for each exam, which he called "very time-consuming and extremely expensive" for institutions tasked with grading large amounts of exams. “You’re really hoping that at the end of the day, they’re giving the attention, time and diligence required to truly put that effort into grading it accurately without bias and with the same level of consistency,” he said. “The way other countries tackle that is they’ll hire two, sometimes three individuals to grade the same paper, and they take a sort of median score. That gets really complicated." Paul said that for big tests administered to large numbers of students, there is often a 6 percent difference between what human graders give to the same work, according to data from the company noting inconsistencies from grading bias. He said that in A/B testing, results were within a 2 percent margin when using the AI Grader, which showed that the tool is effective in mitigating grading bias. “With us the accuracy is extremely high,” he said. “We tend to be in that 1 to 2 percent sort of delta between what the humans are grading and what the AI gave it.”

#### = education O/Ws because at least racism will not be further intrenched

## 6---Access (30)

#### AI increases access to underprivileged communities Peplinksi 23

Melissa Peplinksi 23, 11-15-2023, "How we can use AI to increase access and equity in science education," Thomas B. Fordham Institute, The Thomas B. Fordham Institute is a nonprofit education policy think tank based in Washington, D.C., that focuses on research and analysis related to K-12 education in the United States. https://fordhaminstitute.org/national/commentary/how-we-can-use-ai-increase-access-and-equity-science-education, accessed 2-20-2025 //wyatt G?//

Editor’s note: This essay is an entry in Fordham’s 2023 Wonkathon, which asked contributors to answer this question: “How can we harness the power but mitigate the risks of artificial intelligence in our schools?” Learn more. When we started thinking about the question of how we can harness AI to benefit K–12 teachers and students, we asked AI, ChatGPT specifically, and got the following response: Artificial intelligence (AI) can significantly enhance K–12 education by offering personalized learning experiences, automating administrative tasks, providing intelligent tutoring, and fostering engagement. The chatbot then detailed specific ways in which AI can help to offer all those benefits within an educational context. The reality of AI in education is that it can supply all those amazing supports, and there are already many examples of personalized learning, automated tasks, intelligent tutoring and chatbot tools, and opportunities for increased engagement. In order to narrow the scope of our exploration of the impacts of AI in the classroom, we will focus specifically on science education because of its increasing importance and relevance to our current world and the ways in which AI is able to integrate into a science curriculum not only as a tool, but also as a subject of deeper inquiry and study. When we asked AI what AI + science equals, we got this insightful response from ChatGPT: AI + Science = Innovation and Discovery The combination of AI and science leads to innovative solutions, accelerates discoveries, and enhances our understanding of the world. In today’s science classrooms, AI can provide real and innovative solutions to enhance student learning. AI can allow students to access key models and phenomena through new and diverse lenses. AI, in partnership with science educators, can be a tool that helps to make science relevant, engaging, and accessible to all students, regardless of their personal background, support needs in the classroom, or other relevant characteristics to their learning. Some uses of AI within science education that have had positive impacts in the classroom include: Assessments AI-driven assessments: Assessment is an integral part of any science curriculum. To be able to understand and track student progress, there need to be assessments throughout the year. A report on the future of testing from the Center for American Progress details ways that assessment might be enhanced by AI with “intelligent tutoring, stealth assessments, games, and virtual reality.” They assert that “mini-tests built by artificial intelligence can provide a wide variety of ways to use this technology to build engaging tools.” Relevant examples: AI can be used to tailor examples and phenomena in the science classroom to specific student contexts and experiences to make the curriculum more culturally relevant and engaging to students. Using examples that reflect students’ lived experiences can help them to connect on a deeper level with their science learning. For example, if you ask ChatGPT to provide an example of a science phenomenon based on energy that is relevant to a middle school student in Louisiana, it will provide details and examples of solar energy. This is in large contrast to a student example in Seattle, Washington, where an example might be closely related to water because of the abundance of water resources in that area. Also, with ChatGPT, you can provide more specifics to the student and school culture, NGSS dimensions, or other characteristics related to phenomena that would help to pinpoint the closest relevant examples. Grading AI grading tools: Tools like gradescope can support teachers in their grading, saving them time and providing insights on how their students are progressing. AI also has the capability to help address bias in grading by ensuring that students are graded by objective standards and that teachers’ implicit biases are not reflected within student grades. Supports The MSU Denver Virtual Lab Assistant: Otherwise known as the VLA, this tool supports science learning for students with visual impairments and allows those students “the ability to control laboratory equipment in a completely independent manner via voice command.” Benetech: A non-profit working to develop an AI solution to create accessible equations and charts for usage with screen readers and within their audio content library, Bookshare. This increases access for students with dyslexia/dysgraphia, students with low vision, or students with other barriers to accessing the materials. Benetech envisions a science classroom where “readers will not have to take extra steps to access the complex visuals as they would already be converted into digital materials.” AI tutors: Emerging AI tutor solutions like Khanmingo provide tutoring support for both teachers and students alike, providing coaching through both lesson planning and student learning. Students in computer science courses can get real time feedback on their work as they code to help them identify where they might need to go back to and re-learn specific things to apply to their assignments. With the development of tools like the ones above, we can envision a future where AI solves many of the access and equity issues plaguing science education and education more broadly. These innovative tools and uses of AI also show us areas where we can further develop AI to fill more gaps in the science classroom. In science, with the advent of innovative assessments and tasks, we are seeing that many schools and districts struggle to know and understand high-quality aligned Next Generation Science Standard (NGSS) assessments. As an organization, in partnership with AI, this provides us an opportunity to creatively problem solve for these instances and provide the knowledge necessary to support the integration and analysis of these assessments. Also, as we consider what students are learning within the NGSS, specifically in science practices, we can use AI to help teachers expand their curriculum. For example, in MS Practice 8, it says, “[students will] gather, read, and synthesize information from multiple appropriate sources and assess the credibility, accuracy, and possible bias of each publication and methods used, and describe how they are supported or not supported by evidence.” This practice provides an opportunity to use AI as an on ramp to meeting these expectations, but also expands the opportunities for students to practice. AI can unfortunately also present challenges for students and teachers if used incorrectly in a classroom setting. Right below the area where you input your prompts in ChatGPT is an important warning about the information that is provided: “ChatGPT can make mistakes. Verify important information.” This highlights the potential for AI to spread misinformation and bias, and even beyond that, there are additional risks associated with AI being used in ways that undermine students’ creativity and critical thinking by completing tasks for them instead of allowing them to reason through them. The way we can begin to truly integrate AI into the classroom and mitigate the risks associated with AI is by forming a strong partnership between AI and educators. Educators and education leaders should be given the training and support to understand the benefits and potential uses of AI to enhance student learning and be given opportunities to work alongside content experts to review content generated by AI. There are several resources available to empower school leaders and educators to leverage AI in the classroom, from organizations like Code.org, OpenAI, and other leading technology and education organizations. The use of AI within science education just makes sense. AI, as an innovation within the field of science, shows students the ways in which science has already transformed our world and the ways we think, work, learn, and do most other things. With the right guidance and collaboration from educators and students, AI can revolutionize the way we learn in a science classroom. AI can bridge long-existing learning gaps by providing innovative accessibility supports, engaging and culturally relevant examples within assessments and activities, and supporting teacher practice with enhanced grading and feedback supports. We must embrace AI in the classroom to meet the needs of this new generation of science learners.

#### Districts will have access AASA 25

AASA 25, 1-15-2025, "Capacity Building Grant Will Allow School Systems to Become More AI-Ready," Default, https://www.aasa.org/news-media/news/2025/01/15/capacity-building-grant-will-allow-school-systems-to-become-more-ai-ready, accessed 3-4-2025 //wyatt G?//

CoSN announced receipt of a new grant to advance the thoughtful and responsible implementation of artificial intelligence (AI) technologies in K-12 school districts, which was made possible by the Bill & Melinda Gates Foundation. The Building Capacity for Generative AI in K-12 Education Grant will support training to help school districts assess their readiness to implement generative AI (Gen AI) technologies and develop a roadmap for implementation that aligns with their instructional and operational objectives. Through collaboration with Education Service Agencies (ESAs) and state nonprofit organizations, as well as working with national education associations, CoSN will provide high-quality professional learning opportunities to school districts of all sizes, with a special emphasis on reaching small- and medium-sized school districts that may otherwise have limited access to quality training and guidance, ensuring responsible and effective integration of Gen AI for all. This project builds on the success of previous efforts, including the development of the CoSN/CGCS K-12 Generative AI Readiness Assessment and the K-12 Gen AI Maturity Tool. Informed by insights from project partners as well as from members of CoSN’s AI Committee, CoSN will define a process to ensure the Maturity Tool is relevant and accessible to school districts of all sizes and locations, including rural and under-resourced school districts. CoSN will also capitalize on the local reach of ESAs and state nonprofit organizations to ensure the “Go to Market” strategy reaches all school systems/districts, not simply the largest and most sophisticated. This grant will enable CoSN to build a more scalable model to benefit districts of all sizes. “As schools across the country explore how AI can transform teaching, learning and the broader education enterprise, many districts — especially smaller, under-resourced ones — are unsure where to begin,” said Keith Krueger, CEO, CoSN. “This groundbreaking initiative leverages CoSN’s national expertise, in partnership with education service agencies, to empower districts to navigate the opportunities and challenges of AI in K-12 education. We are especially proud to collaborate with our strategic partners AESA, AASA and SETDA on this critical effort.” Key activities supported by the grant include: Training a cohort of 10-20 lead trainers at the national level. In partnership with the Association of Education Service Agencies (AESA), hosting four regional Train-the-Trainer sessions to train additional cohorts who, in turn, will provide ongoing training to local school districts, with special emphasis on reaching under-resourced and rural districts. Hosting three Gen AI Maturity Summits for district teams targeting medium and large school districts. The summits will focus on building awareness of the CoSN/CGCS K-12 AI Maturity Tool and how it can be used by districts along with resources, insights and strategies for harnessing the power of generative AI. Key objectives of the grant include: Serving medium and small school districts that lack the capacity and expertise to leverage AI opportunities by engaging ESAs and state nonprofit organizations in a “Train-the-Trainer” model, delivering professional learning opportunities and shared technical assistance. Collecting data on best practices for meeting the local needs of different ESA and state nonprofits’ operating models to support scaling efforts. Conducting a pre- and post-survey of participating district teams to provide baseline data and evaluate their readiness to utilize the Gen AI Maturity Tool. Developing a library of resources from CoSN’s Gen AI Committee — with experts from AESA, The School Superintendents Association (AASA) and SETDA, the principal association representing U.S. state and territorial education technology leaders — tied to the Gen AI Maturity Tool, providing evidence and examples of successful Gen AI integration at varying levels of maturity. Enhancing networking between ESAs, state nonprofit education organizations, superintendents, state departments of education and CoSN to foster collaboration and knowledge sharing on common successful strategies. Lessons learned from these activities will inform the continuous improvement of the “Train-the-Trainer” model and supporting resources, with a view to making the training available to additional organizations and school districts following the completion of grant-funded activities. By prioritizing trust, transparency, and ethical, responsible, and sustainable implementation, CoSN aims to ensure the safe and effective use of AI technologies in K-12 education.

# 2AC

## a/2 superintelligence

**It’s impossible---it can’t understand abstract and complex understanding of consciousness.**

**Lehewych 22** [Daniel; March 31; M.A. in Philosophy from the City University of New York Graduate Center, professional freelance writer; Big Think, “The subtle art of language: why artificial general intelligence might be impossible, DOA: 4/12/2024, https://bigthink.com/the-future/artificial-general-intelligence-impossible/]

**Consciousness is arguably the most mysterious problem humans have ever encountered**. In many famous philosophical essays, consciousness is **regarded as unsolvable.** Yet, as we speak, engineers and cognitive scientists are [putting their noses to the grindstone](https://gcrinstitute.org/papers/055_agi-2020.pdf) to develop consciousness in artificial intelligence (AI) systems. Typically, this project is referred to as the development of **“artificial general intelligence”** (AGI), which covers a wide range of cognitive and intellectual abilities that humans possess. Thus far, this project — being conducted **globally in 72 independent research projects — has not produced conscious robots.** Rather, as it stands, we have **super-intelligent AI** that, on the whole, **is very narrow in its abilities.** One-trick pony For example, the best human chess players are [utterly demolished](https://www.npr.org/sections/alltechconsidered/2016/10/24/499162905/20-years-later-humans-still-no-match-for-computers-on-the-chessboard) in chess matches against computers like IBM’s Deep Blue. To quote author and grandmaster chess player Andrew Soltis, “Right now, there’s just no competition. The computers are just much too good.” However, **Deep Blue is only good at chess. We have yet to create an AI system that can outpace or even keep up with general human cognition**. Even [Sophia](https://qz.com/1121547/how-smart-is-the-first-robot-citizen/), the famous humanoid robot granted citizenship in Saudi Arabia in 2017, does not demonstrate consciousness or artificial general intelligence. To be sure, some of what Sophia is capable of is astonishingly sophisticated. For instance, Sophia receives visual information, which she can use to recognize individual faces and sustain eye contact. Likewise, Sophia can process language to the extent that she can hold trivial conversations with people. Moreover, Sophia can make over 60 different facial expressions during those conversations. This certainly makes it feel like one is in the presence of a conscious being. **Language is the key to artificial general intelligence** Sophia’s amazing abilities sound sufficient for consciousness, but only superficially. And the reason for this is rooted in language. **Human language is profoundly complex**. One major distinguishing feature of human communication is that the meaning of what we say often isn’t conveyed explicitly by the literal meaning of our sentences. Instead, the meaning of our words often goes beyond what we expressly assert. Irony is a good example. Consider going to a Broadway show where the lead actor shows up drunk and puts on a terrible performance. One could jokingly say that the show displayed “peak professionalism and wit.” The average person immediately understands these words to represent the opposite of their literal meaning. In fact, a great deal of human communication is indirect. Sarcasm, metaphor, and hyperbole often convey meaning with greater persuasiveness than literal assertions. Much of the time, we imply or hint at what we mean, rather than say it directly. Indeed, human communication would be quite bland without our frequent appeal to figures of speech. Poetry and literature essentially would be non-existent. The subtle art of language, in some sense, is part of what makes us human. A chatbot with a face **Human consciousness**, in other words, in part **consists of understanding abstract and indirect meanings. And it is precisely this sort** of understanding **that artificial intelligence is incapable of**. Sophia can talk, but the conversation is trivial. Indeed, many computer scientists see Sophia as nothing more than a [Chatbot with a face](https://qz.com/1121547/how-smart-is-the-first-robot-citizen/). Christopher Hitchens once aptly stated that “the literal mind is baffled by the ironic one, demanding explanations that only intensify the joke.” Such literal mindedness toward language is what characterizes [artificial intelligence’s relationship with it](https://dl.acm.org/doi/fullHtml/10.1145/3290605.3300325). If, for example, Sophia were to hear the earlier Broadway joke, even in context, she may respond, “I don’t know what you’re talking about. The actor was unprofessional and drunk.” In other words, she doesn’t get it. **Even detecting such complex concepts** as drunkenness or professionalism **would be a tall order** for Sophia. Unlike humans and even some animals, sophisticated AI systems like Sophia cannot detect other creatures’ emotional or mental states. Hence, they can only comprehend the word-for-word meaning of sentences. Try being ironic with Siri, for instance. It won’t work. Heck, ask her to [find something that isn’t McDonald’s](https://bigthink.com/neuropsych/can-ai-think-understand/). She can’t do that either. Theory of mind We understand other people and their minds [by analogy](https://bigthink.com/thinking/problem-other-minds-js-mill/). Unfortunately, such **indirectness is something engineers and cognitive scientists have failed to program in artificial intelligence. This is because the human ability to reliably understand each other indirectly is itself a mystery. Our ability to think abstractly and creatively**, in other words, **is quite challenging to understand. And it is impossible to code for something we don’t understand**. That is why novels and poems written by AI [fail to create a coherent plot](https://www.theatlantic.com/technology/archive/2018/10/automated-on-the-road/571345/) or are [mostly nonsensical](https://futurism.com/artificial-intelligence-bad-poems). Artificial general intelligence — robot consciousness — might be possible in the distant future. **But without a full** and comprehensive **understanding of language and its countless nuances, AGI certainly will remain impossible.**

**AI will never be “misaligned” or “go rogue.” It’s human-limited.**

**Mueller 24** [Milton Mueller – Professor and Program Director, Masters of Science in Cybersecurity Policy, “The Myth of AGI: How the illusion of Artificial General Intelligence distorts and distracts digital governance,” 5-22-24, <https://www.internetgovernance.org/wp-content/uploads/MythofAGI.pdf>, accessed 2-9-25 //Bosley]

Some of the more recent literature in computer science, however, attempts to show how computing machinery might become autonomous. Human intelligence evolved from nature; mightn’t AGI evolve from computers? These **researchers attempt to show how an AI application might acquire autonomy** and a will to survive **through** known features of **deep learning**, **reward structures**, **and** the application of **game-theoretic models**. The progression is **based on** three arguments: "**the** **alignment problem**;” the notion of “**AI drives**” (Omohundro, 2007; Shulman, 2010), **and** a **belief that these drives can prevent humans from** disabling or **controlling the machine** – the so-called “off-switch problem.” (Hadfield-Menell et al, 2008; Sotala & Yampolskiy, 2015).

The alignment problem is defined as "the challenge of ensuring that AI systems pursue goals that match human values or interests." (Ngo et al., 2023; Russell, 2019; Gabriel, 2020) The “AI drive” work asserts that "goal-seeking systems will necessarily begin to model their own operation and to improve themselves” in ways that give them their own motives. (Omohundro, 2018) The off-switch problem is a simple game theory model of why a machine might resist being turned off. Taken together, these arguments try to mount the case that machines equipped with advanced artificial intelligence could evolve into a life-form – and a potentially dangerous one at that.

Insofar as there is a coherent argument here, it indicates two possible paths toward an AGI that is a threat to human control. The first is that the machines will evolve into an autonomous AGI (Bullock, Mckernon, & Dicarlo, 2023); the other is that AI training and development would result in a deviation-amplifying feedback process (Ngo, et al, 2023) through which the machines acquire their own purposes and autonomy from human purposes.

**The machine evolution argument can be** readily **dismissed**. Machines do not evolve. Of course, **technology does change over time** in ways that superficially resemble “evolution,” but a proper application of evolutionary concepts corrects that perception. **The machine itself isn’t evolving** – **the changes in technology are produced by humans responding to markets and** other **human social systems.** **Evolution in the Darwinian sense requires** **self-replication**, **mutation** **and** **natural selection** over many generational cycles. The replication of machines comes from human manufacturing processes, not from self-replication. **Nor does mutation** – changes in the design of machines – **come from the machines**. They come from human decisions in response to societal pressures for efficiency, innovation and safety. **The selection process** – that is, which machines continue to be produced and which become obsolete – **is also governed by human decisions**. The choices are made by people in competitive markets and/or political institutions. Hence, the machines themselves do not evolve, industries and sociotechnical systems do. **Human decisions**, by individuals or in aggregate, **control each step of the process**. If this is true, we cannot speak of “machine evolution.” For machines to evolve, they would first have to become alive, which means they would gain the ability to self-support and self-replicate, which they currently cannot do.

So, **the autonomous AGI scenario must be based**, at least initially, **on a cybernetic process**, **in which human efforts to produce AI generate a deviation-amplifying feedback loop** that not only makes machines more intelligent but also gives them their own goals and the ability replicate themselves or “survive” without human consent.

**It’s impossible due to laws of computation.**

Bert **Gambini 22**, News Content Manager, Humanities, Economics, Social Sciences, Social Work, Libraries, University of Buffalo, citing Jobst Landgrebe & Barry Smith, philosophers at University of Buffalo, “New book co-written by UB philosopher claims AI will “never” rule the world,” UB, 8/22/22, DOA: 4/03/2024, https://www.buffalo.edu/news/releases/2022/08/014.html]

Elon **Musk** in 2020 **said** that artificial intelligence (**AI**) with**in five years would surpass human intelligence on its way to becoming “an immortal dictator**” over humanity. **But** a new book co-written by a University at Buffalo philosophy professor argues **that won’t happen – not by 2025, not ever!** Barry Smith, PhD, SUNY Distinguished Professor in the Department of Philosophy in UB’s College of Arts and Sciences, and Jobst Landgrebe, PhD, founder of Cognotekt, a German AI company, have co-authored “Why Machines Will Never Rule the World: Artificial Intelligence without Fear.” Their book presents a powerful argument against the possibility of engineering machines that can surpass human intelligence. **Machine learning and all other working software** applications − the proud accomplishments of those involved in AI research − **are** for Smith and Landgrebe **far from anything resembling** the capacity of **humans.** Further, they argue that **any incremental progress** that’s unfolding **in the field** of AI research **will** in practical terms **bring it no closer to the** full **functioning possibility of the human brain.** Smith and Landgrebe offer a critical examination of AI’s unjustifiable projections, such as machines detaching themselves from humanity, self-replicating, and becoming “full ethical agents.” **There cannot be a machine will**, they say. **Every single AI application rests on the intentions of human beings** – including intentions to produce random outputs. **This means the Singularity**, a point **when AI becomes uncontrollable and irreversible** (like a Skynet moment from the “Terminator” movie franchise) **is not going to occur. Wild claims** to the contrary serve **only** to **inflate AI’s potential and distort public understanding** of the technology’s nature, possibilities and limits. Reaching across the borders of several scientific disciplines, Smith and Landgrebe argue that **the idea of** a general artificial intelligence (**AGI**) − the ability of computers to emulate and go beyond the general intelligence of humans − **rests on fundamental mathematical impossibilities that are analogous in physics to** the impossibility of building **a perpetual motion machine. AI that would match the general intelligence of humans is impossible because of** the **math**ematical **limits on what** can be modelled and **is “computable.” These** limits **are accepted by** practically **everyone** working **in the field**; yet they have thus far failed to appreciate their consequences for what an AI can achieve. **“To overcome these** barriers **would require a revolution in math**ematics **that would be of greater significance than the invention of** the **calculus by** Newton and **Leibniz** more than 350 years ago,” says Smith, one of the world’s most cited contemporary philosophers. “We are not holding our breath.” Landgrebe points out that, “As can be verified by talking to mathematicians and physicists working at the limits of their respective disciplines, **there is nothing even on the horizon which would suggest that a revolution of this sort might** one day **be achievable. Mathematics cannot** fully **model the behaviors of complex systems like the human organism**,” he says. AI has many highly impressive success stories, and considerable funding has been dedicated toward advancing its frontier beyond the achievements in narrow, well-defined fields such as text translation and image recognition. Much of **the investment to push the technology forward into areas requiring** the machine counterpart of **general intelligence may**, the authors say, **be money down the drain.** “The text generator **GPT-3 has shown itself capable** of producing different sorts of convincing outputs across many divergent fields,” says Smith. “**Unfortunately**, its **users soon recognize that mixed in with these** outputs there **are** also **embarrassing errors, so** that the **convincing outputs themselves** began to **appear as nothing more than clever parlor tricks.” AI’s role in sequencing the human genome led to suggestions for how it might help find cures for many** human **diseases; yet, after 20 years** of additional research (in which both Smith and Landgrebe have participated), **little has been produced to support optimism of this sort. “In certain completely rule-determined confined settings, machine learning can be used to create algorithms that outperform humans**,” says Smith. “But **this does not mean that they can ‘discover’** the **rules governing just any activity** taking place in an open environment, **which is what the human brain achieves every day.” Technology skeptics do not**, of course, **have a perfect record**. They’ve been wrong in regard to breakthroughs ranging from space flight to nanotechnology. **But** Smith and Landgrebe say their **arguments are based on the mathematical implications of the theory of complex systems. For mathematical reasons**, AI cannot mimic the way the human brain functions. In fact, the authors say that **it’s impossible to engineer a machine that would rival the cognitive performance of a crow.** “An AGI is impossible,” says Smith. “As our book shows, **there can be no general artificial intelligence because it is beyond the boundary of what is even in principle achievable by means of a machine.”**

### a/2 military

**Military readiness solves extinction and it’s an impact filter.**

**Dowd 15** (Alan, senior fellow with the Sagamore Institute Center for America's Purpose, “Shield & Sword: The Case for Military Deterrence”, https://providencemag.com/2015/12/shield-sword-the-case-for-military-deterrence/)

Surely, the same principle applies in the realm of nations. Our world teems with violent regimes and vicious men. And something precious—our notion of peace, sovereignty, liberty, civilization itself—sits exposed to all that danger. In a world where might makes right, **the only thing that keeps the peace**, defends our sovereignty and liberty, and upholds civilization **is** the willingness to use our resources to keep the dangers at bay. Yet too many policymakers disregard the wisdom of **military deterrence**, and too many people of faith forget that the aim of deterrence is, by definition, to prevent wars, not start them. Some people of faith oppose the threat of military force, let alone the use of military force, because of Christ’s message of peace. This is understandable in the abstract, but we must keep in mind two truths. First, governments are held to a different standard than individuals, and hence are expected to do certain things individuals aren’t expected to do—and arguably shouldn’t do certain things individuals should do. For example, a government that turned the other cheek when attacked would be conquered by its foes, leaving countless innocents defenseless. A government that put away the sword—that neglected its defenses—would invite aggression, thus jeopardizing its people. Second, all uses of force are not the same. The sheriff who uses force to apprehend a murderer is decidedly different from the criminal who uses force to commit a murder. The policemen posted outside a sporting event to deter violence are decidedly different from those who plot violence. Moral relativism is anything but a virtue. Some lament the fact that **we live in** such **a violent world**, but that’s precisely the point. Because we live in a violent world, governments must take steps to deter those who can be deterred—and neutralize those who cannot. In this regard, it pays to recall that Jesus had sterner words for scholars and scribes than He did for soldiers. In fact, when a centurion asked Jesus for help, He didn’t admonish the military commander to put down his sword. Instead, He commended him for his faith.[i] “Even in the Gospels,” soldier-scholar Ralph Peters reminds us, “it is assumed that soldiers are, however regrettably, necessary.”[ii] They are necessary not only for waging war but, preferably, for maintaining peace. It’s a paradoxical truth that **military readiness can keep the peace**. The Romans had a phrase for it: Si vis pacem, para bellum. “If you wish for peace, prepare for war.” President George Washington put it more genteelly: “There is nothing so likely to produce peace as to be well prepared to meet an enemy.” Or, in the same way, “We infinitely desire peace,” President Theodore Roosevelt declared. “And the surest way of obtaining it is to show that we are not afraid of war.” After the West gambled civilization’s very existence in the 1920s and 1930s on hopes that war could somehow be outlawed, the men who crafted the blueprint for waging the Cold War returned to peace through strength. Winston Churchill proposed “defense through deterrents.” President Harry Truman called NATO “an integrated international force whose object is to maintain peace through strength…we devoutly pray that our present course of action will succeed and maintain peace without war.”[iii] President Dwight Eisenhower explained, “Our arms must be mighty, ready for instant action, so that no potential aggressor may be tempted to risk its own destruction.” President John Kennedy vowed to “strengthen our military power to the point where no aggressor will dare attack.” And President Ronald Reagan steered the Cold War to a peaceful end by noting, “None of the four wars in my lifetime came about because we were too strong.” Reagan also argued, “Our military strength is a prerequisite for peace.”[iv] Even so, arms alone aren’t enough to deter war. After all, the great powers were armed to the teeth in 1914. But since they weren’t clear about their intentions and treaty commitments, a small crisis on the fringes of Europe mushroomed into a global war. Neither is clarity alone enough to deter war. After all, President Woodrow Wilson’s admonitions to the Kaiser were clear, but America lacked the military strength at the onset of war to make those words matter and thus deter German aggression. In other words, America was unable to deter. “The purpose of a deterrence force is to create a set of conditions that would cause an adversary to conclude that the cost of any particular act against the United States of America or her allies is far higher than the potential benefit of that act,” explains Gen. Kevin Chilton, former commander of U.S. Strategic Command. It is a “cost-benefit calculus.”[v] So, given the anemic state of America’s military before 1917, the Kaiser calculated that the benefits of attacking U.S. ships and trying to lure Mexico into an alliance outweighed the costs. That proved to be a grave miscalculation. **In order for the adversary not to miscalculate**, a few **factors must hold**. First, **consequences must be clear**, which was not the case on the eve of World War I. Critics of deterrence often cite World War I to argue that arms races trigger wars. But if it were that simple, then a) there wouldn’t have been a World War II, since the Allies allowed their arsenals to atrophy after 1918, and b) there would have been a World War III, since Washington and Moscow engaged in an unprecedented arms race. The reality is that miscalculation lit the fuse of World War I. The antidote, as alluded to above, is strength plus clarity. A second important factor to avoid miscalculation: The adversary must be rational, which means it can grasp and fear consequences. Fear is an essential ingredient of deterrence. It pays to recall that deterrence comes from the Latin dēterreō: “to frighten off.”[vi] Of course, as Churchill conceded, “The deterrent does not cover the case of lunatics.”[vii] Mass-murderers masquerading as holy men and death-wish dictators may be immune from deterrence. (The secondary benefit of the peace-through-strength model is that it equips those who embrace it with the capacity to defeat these sorts of enemies rapidly and return to the status quo ante.) Third, **the consequences of military confrontation must be credible and tangible**, which was the case during most of the Cold War. Not only did Washington and Moscow construct vast military arsenals to deter one another; they were clear about their treaty commitments and about the consequences of any threat to those commitments. Recall how Eisenhower answered Soviet Premier Nikita Khrushchev’s boast about the Red Army’s overwhelming conventional advantage in Germany: “If you attack us in Germany,” the steely American commander-in-chief fired back, “there will be nothing conventional about our response.”[viii] Eisenhower’s words were unambiguously clear, and unlike Wilson, he wielded the military strength to give them credibility. Discussing military deterrence in the context of Christianity may seem incongruent to some readers. But for a pair of reasons it is not. First, deterrence is not just a matter of GDPs and geopolitics. In fact, scripture often uses the language of deterrence and preparedness. For example, in the first chapter of Numbers the Lord directs Moses and Aaron to count “all the men in Israel who are twenty years old or more and able to serve in the army.” This ancient selective-service system is a form of military readiness. Similarly, I Chronicles 27 provides detail about the Israelites’ massive standing army: twelve divisions of 24,000 men each. II Chronicles 17 explains the military preparations made by King Jehoshaphat of Judah, a king highly revered for his piety, who built forts, maintained armories in strategically located cities “with large supplies” and fielded an army of more than a million men “armed for battle.” Not surprisingly, “the fear of the Lord fell on all the kingdoms of the lands surrounding Judah, so that they did not go to war against Jehoshaphat.” In the New Testament, Paul writes in Romans 13 that “Rulers hold no terror for those who do right, but for those who do wrong…Rulers do not bear the sword for no reason.” Again, this is the language of deterrence. Those who follow the law within a country and who respect codes of conduct between countries have nothing to fear. Those who don’t have much to fear. Likewise, to explain the importance of calculating the costs of following Him, Jesus asks in Luke 14, “What king would go to war against another king without first sitting down to consider whether his 10,000 soldiers could go up against the 20,000 coming against him? And if he didn’t think he could win, he would send a representative to discuss terms of peace while his enemy was still a long way off.” In a sense, both kings are wise—one because he recognizes that he’s outnumbered; the other because he makes sure that he’s not. Put another way, both kings subscribe to peace through strength. Again, as with the Centurion earlier, Jesus could have rebuked the martial character of these kings, but he did not. This is not just description but commendation. We ignore their example at our peril. Secondly, it is not incongruent if **we understand military deterrence as a means to prevent great-power war**—**the kind that kills by the millions**

### on their T definition- it’s not topical

#### A few definitions all from Meriam webster education means

Merriam webster"Definition of EDUCATION," No Publication, https://www.merriam-webster.com/dictionary/education, accessed 3-7-2025 //wyatt G?//

1 a : the action or process of educating or of being educated also : a stage of such a process b : the knowledge and development resulting from the process of being educated a person of little education 2 : the field of study that deals mainly with methods of teaching and learning in schools

#### Educate means

Merriam webster"Definition of EDUCATING," No Publication, https://www.merriam-webster.com/dictionary/educating, accessed 3-7-2025 //wyatt G?//

1 a : to provide schooling for chose to educate their children at home b : to train by formal instruction and supervised practice especially in a skill, trade, or profession 2 a : to develop mentally, morally, or aesthetically especially by instruction b : to provide with information : inform educating themselves about changes in the industry 3 : to persuade or condition to feel, believe, or act in a desired way educate the public to support our position

#### In means

Merriam webster "Definition of IN," No Publication, https://www.merriam-webster.com/dictionary/in, accessed 3-7-2025 //wyatt G?//

1 a —used as a function word to indicate inclusion, location, or position within limits in the lake wounded in the leg in the summer b : into sense 1 went in the house 2 —used as a function word to indicate means, medium, or instrumentality written in pencil bound in leather 3 a —used as a function word to indicate limitation, qualification, or circumstance alike in some respects left in a hurry b : into sense 4a broke in pieces 4 —used as a function word to indicate purpose said in reply 5 —used as a function word to indicate the larger member of a ratio

#### By contrast, research means

Merriam webster "Definition of RESEARCH," No Publication, https://www.merriam-webster.com/dictionary/research, accessed 3-7-2025 //wyatt G?//

1 : studious inquiry or examination especially : investigation or experimentation aimed at the discovery and interpretation of facts, revision of accepted theories or laws in the light of new facts, or practical application of such new or revised theories or laws 2 : the collecting of information about a particular subject 3 : careful or diligent search

#### On their definition for military- don’t buy it:

#### It’s paywalled- we can’t access and reverse search doesn’t even work- skews us out from prepping and also checking back the validity or context of their evidence

#### Be skeptical given they paste in 2 sentences without any context, when they cite an entire book

#### Prefer us because we give word-specific, dictionary definitions. Hold them to this for the entire round

The self replicating AI card is from 2021, no impact yet

### A/2 neuroscience

#### Its not T, just because the field can be educated doesn’t mean their stuff is prefer the spec stuff we say above

#### The card literally says the only usage of AI is mind uploading- meaning if its true that It works all it does it replicate dead humans, not evolve to be superintelligent

#### There is literally no impact

### a/2 misalignment

#### Misalignment is definitely not T, each part of the link should have to be education specific

#### The competitively advantageous stuff Isnt generative AI + what if scenario + miscalc only happens if orgs making ASI are competing- they give no precedent if this is happening

#### ON PANDEMICS

#### Which terrorist group is going to develop AI to wipe out the whole world- if terrorists want to commit terror that’s certainly not where they look first

#### Their card is 10 years old, and nothing has happened yet

#### It doesn’t say that the AI would make the pandemic to kill humans, just to make it in general, so it wont be the bioweapon the impact is about

**Counter-tech solves.**

James **Fodor 20**, PhD student at the University of Melbourne, completed masters in neuroscience at the Australian National University, research assistant in structural biology at Monash University, 5/11/2020, “Critical Review of 'The Precipice': A Reassessment of the Risks of AI and Pandemics,” cc

Failure of timely biomedical response

In addition to the failure of public policy responses, **extinction of humanity** by a novel pathogen would also require the failure of any **biomedical response** to the pandemic. Ord believes that as biological techniques become easier and cheaper, they become accessible to more and more people, and hence represent a greater and greater risk. He argues:

As the pool of people with access to a technique grows, so does the chance it contains someone with malign intent. (p. 134)

This argument, however, appears to only consider one side of the issue. As the pool of people with access to a technique grows, so too does the number of people who wish to use that technique **to do good**. This includes developing techniques and technologies for more easily **detecting**, **controlling**, and **curing** **infectious diseases**. It surprises me that Ord never mentions this, since the development of biomedical technologies does not only mean that there is greater scope for use of the technology to cause disease, but also greater scope for use new techniques to prevent and cure disease. Indeed, since the prevention of disease receives far more research attention that causing disease, it seems reasonable to assume that our abilities to development treatments, tests, and vaccines for diseases will develop more rapidly than our abilities to cause disease. There are a **range** of **emerging biomedical technologies** that promise to greater improve our ability to fight **existing** and **novel diseases**, including **transmissible vaccines**, rational **design of drugs**, and **reverse vaccinology**. As such, I regard it unlikely that if biomedical technology had advanced sufficiently to be able to produce an extinction-level pathogen, it would nevertheless fail to develop sufficient countermeasures to the pathogen to at least prevent full human extinction.

#### SAI Jacobs 16 evidence is old and itself admits astronomical suffering is rarely discussed because its so realistically unlikely

#### Don’t buy the “AI comes this year”- that was literally about OpenAI or ChatGPT and the AGI is thus obviously not the same as the superintelligence they talk about

### a/2 military AI

#### All the cards are pre-trump, they didn’t cut updates and so their authors don’t account for trump being best friends with putin

Look at how he 2 v 1ed Zelensky for proof

#### Also the AI isn’t T in the first place

#### IL is nonexistent- goes from arms race to extinction but a. where’s conflict happening b. when