Expert Insights
PERSPECTIVE ON A TIMELY POLICY ISSUE

ASAD RAMZANALI, GANESH SITARAMAN

Toward a Grand Strategy for AI Resilience

March 2026

For more information on this publication, visit **www.rand.org/t/PEA4525-1**.

Published by the RAND Corporation, Santa Monica, Calif.

About This Paper

As the increasing adoption of artificial intelligence (AI) transforms society, policymakers should aim for resilience—the ability to withstand shocks, adapt, and recover—as the central goal of public policy. Drawing lessons from engineering, psychology, and ecology, we explore how resilience can guide policy choices as AI profoundly changes the economy, individuals and communities, and national security. Resilience stands in contrast to other approaches to policy approaches: An overarching do-nothing approach to social media and today's wait-and-see approach to AI have failed to strengthen people, institutions, and systems to withstand pressures from a technology whose impact has a wide variety of possibilities.

Center for the Geopolitics of Artificial General Intelligence

RAND Global and Emerging Risks is a division of RAND that delivers rigorous and objective public policy research on the most consequential challenges to civilization and global security. This work was commissioned by the division's Center for the Geopolitics of Artificial General Intelligence (AGI), which is committed to helping decisionmakers understand, anticipate, and prepare to navigate the national security and geopolitical implications of AGI. The center convenes leading technologists, strategists, economists, political scientists, and outside experts to consider the feasibility and effectiveness of prospective AGI-enabled capabilities; the domestic and international implications of their use; and the strategies and policies that governments, businesses, and civil society could adopt to respond to new realities.

For more information, visit www.rand.org/geopolitics-of-agi.

Funding

This effort was independently initiated and conducted within the Center for the Geopolitics of Artificial General Intelligence using income from operations and gifts from RAND supporters, including philanthropic gifts made or recommended by DALHAP Investments Ltd., Ergo Impact, Founders Pledge, Charlottes och Fredriks Stiftelse, Good Ventures, Longview, and Coefficient Giving. RAND donors and grantors have no influence over research findings or recommendations.

Contents

Toward a Grand Strategy for AI Resilience

Introduction

Leading experts have strong and diverging views about the future of artificial intelligence (AI), especially the speed of technological progress, the desirability of that speed, the risks of adoption, and appropriate public policy responses. But what is striking—and perhaps surprising—is that there is a near consensus at the heart of AI debates: Widespread adoption of AI will lead to significant societal changes. *Accelerationists*, whose views are typified by Marc Andreessen's "Techno-Optimist Manifesto," see society as "poised for an intelligence takeoff that will expand our capabilities to unimagined heights."[1] *Doomers*, who fear that AI "might eventually outnumber, outsmart, obsolete and replace us" and that it risks "loss of control of our civilization,"[2] see potential catastrophic risks manifesting in years or decades. *Pragmatists* view AI as a "normal technology"[3] and see a future of gradual but significant change over decades, mirroring the development of prior general-purpose technologies. *Populists* challenge "corporate consolidation, economic injustice, tech oligarchy, and rising authoritarianism,"[4] which they already see occurring.

Although the speed and the precise nature of the coming changes are unclear, AI optimists and pessimists alike seem to agree with the Greek philosopher Heraclitus: The only constant is change. However, change can be disruptive, causing short-term and long-term societal problems. With respect to AI, commenters have raised concerns about disruption in almost every domain: from the economic harms of job losses to the social harms of people reliant on companion-bots, the political challenges of deepfakes, and the national security harms of novel biological weapons.

Ideally, society would endure any coming changes without great suffering or deterioration of core societal values—and while reaping the benefits of new technologies. A successful process of widespread AI adoption would prevent and minimize negative effects, involve adaptation, and ensure that people and society rapidly bounce back from personal and social disruptions. This idea of enduring a challenge, adapting, and rebounding is known as resilience.

Our argument in this paper is that the widespread adoption of AI is likely to change society in positive and negative ways and that a strategy of resilience is the best proactive response.[5] In the next section, we describe the concept of resilience and AI policy with examples from three domains—engineering, psychology, and ecology—and we offer a basic framework for thinking about how to apply resilience ideas to public policy with respect to AI. In the following three sections, we go deeper, describing illustrative examples of foreseeable and likely disruptions in the economy, society, and national security.[6] Although we cannot predict the exact nature, timeline, or magnitude of these changes, the current push toward widespread adoption of AI gives us reasonable confidence that these changes will take place to some degree. These changes are significant, and they threaten to make society more fragile.

---

1 Andreessen, "The Techno-Optimist Manifesto."

2 Future of Life Institute, "Pause Giant AI Experiments."

3 Narayanan and Kapoor, *AI as Normal Technology*.

4 Brennan, Kak, and Myers West, *Artificial Power*.

5 For a discussion by one of us applying resilience to a broader set of issues, see Sitaraman, "A Grand Strategy of Resilience."

6 We do not assume or plan for scenarios of the more-extreme instances of a future imagined by *doomers*. If the end of civilization comes to pass in a couple years, resilience-type policies will not make a difference.

Each section then outlines how a resilience-based response might look. Some responses include adopting specific federal or state legislative proposals, while others call for broader cultural shifts that can be catalyzed by policymakers. This approach has some significant benefits: Most of its recommendations do not require predicting the speed or precise nature of technological change, and the recommendations would also help society endure other contemporary challenges successfully. In particular, a strategy for AI resilience would not take a do-nothing or wait-and-see approach focused on specific harms but instead would adopt proactive, structural policies that build a resilient economy, society, and national security system. Perhaps most notably, our resilience-based approach does not reject change: It seeks instead to shape change and to shape society's ability to respond to change.

Resilience and AI Policy

The ideal of resilience can be simply stated: It is the ability of a person, institution, or system to withstand shocks, adapt to them, and bounce back.[7] The more resilient the person, institution, or system, the better able it is to handle challenges. Resilience is based on the assessment that "while the optimal strategy is usually to prevent harm from occurring in the first place, often it is not possible or feasible to prevent a harmful event."[8] As legal scholars Gary E. Marchant and Yvonne A. Stevens observe, in such situations, "the focus must shift to minimizing the extent, duration of, and recovery from the harm."[9]

At a more technical level, the concept of resilience has emerged in multiple fields, with each emphasizing different aspects of the idea. Drawing on the leading literature review by academic experts Patrick Martin-Breen and J. Marty Anderies, we highlight three areas: engineering, psychology, and ecology.[10] These three areas emphasize different aspects of resilience that are relevant to how policymakers might respond to the challenges of AI in the domains of the economy, individuals and communities, and national security.

In engineering, resilience describes a property of a material when pressure or force is applied to it. Materials generally either bend or break in response to stress, and those that bend either bounce back to their original form or remain bent. The ability of a material to keep its form, without bending or breaking under pressure, is its resistance. Its ability to bounce back from being bent is its elasticity. And a material's stability is its capacity to take stress or force without breaking or bending permanently.[11] Increasing resistance, elasticity, or stability increases a material's resilience. As we discuss later, in the national security context, the engineering approach to resilience has much to offer.

In psychology, resilience tends to focus more on the ability of people to adapt to difficult situations. By one account, resilience is an "ongoing process of continual positive adaptive changes to adversity."[12] Multiple factors enhance the ability of people to develop resilience, including problem-solving capacity, communication ability, having a purpose and positive outlook toward life, and perhaps most importantly, strong and sup-

[7] See, e.g., National Academies of Sciences, Engineering, and Medicine, *Disaster Resilience* (which defines *resilience* as "the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events"). See also Konnikova, "How People Learn to Be Resilient."

[8] Marchant and Stevens, "Resilience," p. 250.

[9] Marchant and Stevens, "Resilience."

[10] Martin-Breen and Anderies, *Resilience*.

[11] Martin-Breen and Anderies, *Resilience*, p. 43.

[12] Martin-Breen and Anderies, *Resilience*, p. 45.

portive relationships with others.[13] In debates over AI policy, psychological resilience might be most important for thinking about challenges to individuals and communities.

Resilience in a third area, ecology, is based on the evolution of seeing ecosystems as static to interpreting them as complex, adaptive systems, inspiring modern notions of resilience-thinking in the 1970s.[14] What makes ecosystems complex is that transformations might be needed by multiple interactive systems—as water levels change, the mix of plants might vary, and that, in turn, will have an impact on animals. Significant adaptation may take place, but the system can still be stable and functioning. We apply this approach—thinking about adaptation and transformation in a complex environment—to examining AI's impact on the economy.

Engineering, psychology, and ecology emphasize different aspects of resilience, but the lessons of each are aligned in an important way: They describe an attribute of people, institutions, or society that enables them to withstand or adapt to pressure and change, without breaking down. Although we invoke the three notions of resilience mentioned above as each offering lessons for one domain of AI impact, these are imperfect mappings that, similar to any metaphor or model, have limits to their analytical utility. In our case, although we describe engineering resilience informing AI's impact on national security and psychological resilience informing AI's impact on individuals and communities, we recognize that ecological notions of resilience have informed national security thinking for decades, and the original notions of ecological resilience are based on relationships within ecosystems.[15]

In the AI context, some scholars have observed that a resilience-based approach is a promising paradigm. Writing before the generative AI boom, Marchant and Stevens briefly suggest AI as a domain in which the theory and tools of resilience as a risk governance framework might be most applicable.[16] Building on that work, computer scientists Arvind Narayanan and Sayash Kapoor's *AI as Normal Technology* recommends that policymakers adopt resilience as the primary approach to policymaking in AI.[17] However, Narayanan and Kapoor focus more on policies related to the uncertainty in the development of AI technology (e.g., funding AI risk research, whistleblower protections) than on the economic, social, and security changes that may result from the adoption of AI. We think that the consequences of AI adoption also require significant attention and that resilience is the right approach to addressing them.

However, the existing dominant public policy approaches to AI are ill-suited to building a resilient society in the face of technological change. We see three possible approaches to AI policy. The first approach is a passive do-nothing strategy, often advocated by the accelerationist camp. This approach cautions that regulatory action related to AI will slow down the development and adoption of AI and, therefore, reduce innovation, global competitiveness, and human flourishing.[18] This approach is problematic from a perspective of resilience. Continued widespread adoption of AI *without* policy initiatives and democratic governance will likely lead to a wide variety of disruptions and changes, which threaten to make the economy, individuals, communities, and national security weaker, more fragile, and less resilient. Rather than usher in a technological utopia, this approach is likely to create further inequality; hollow out individuals and communities; and lead

[13] See, e.g., Sutton, "What Is Resilience & Why Is It Important to Bounce Back?"

[14] Martin-Breen and Anderies, *Resilience*, pp. 36–37; Walker and Cooper, "Genealogies of Resilience," p. 144.

[15] Walker and Cooper, "Genealogies of Resilience," pp. 144 and 146.

[16] Marchant and Stevens, "Resilience."

[17] Narayanan and Kapoor, *AI as Normal Technology*.

[18] Andreessen, "The Techno-Optimist Manifesto"; Nguyen, "Peter Thiel"; Thierer, *Defending Technological Dynamism & the Freedom to Innovate in the Age of AI*.

to mistakes, unnecessary conflict, and deaths. This is, in great measure, the path that the United States has taken as a response to societal changes from the internet and social media.

The second approach, which in large part reflects how Congress has approached AI policy to date, seeks to solve problems and crises only after they are fully evident and after solutions garner widespread political appeal. This wait-and-see approach is at once reactive, behavioral, and technocratic: When there are specific behaviors that are fully and rigorously proven to be problematic, with solutions that can garner near-universal consensus support, only then should policymakers offer policy or regulatory solutions to address those problems. These solutions should also be narrowly tailored to the problems so as not to impede any possible further innovation, flexibility for industry, or profits of companies. From a resilience perspective, this approach is also flawed. It suggests acting only *after* serious problems manifest. In this approach, harms will occur—people will lose jobs, cyberattacks will debilitate critical infrastructure, people will die in more-lethal wars, and teen suicide rates will spike further. Solutions after the fact cannot usually repair the damage done. And solutions that are narrow, technical, and focused on bad behaviors do not create the conditions for withstanding shocks or bouncing back. By definition, such solutions only cabin specific behaviors; they do not aim to create a resilient society. For example, in 2025, Congress passed the TAKE IT DOWN Act, narrow legislation responding to the problem of AI-developed deepfake nudes,[19] six years after the first state law[20] and first academic paper[21] emerged on the issue and eight years after the first mainstream press coverage of the issue.[22] In a different domain, this is also the path the United States chose with semiconductors: Policymakers watched decades of semiconductor manufacturing move offshore until the COVID-19 pandemic exposed supply chain fragility that had economic and national security implications.[23] The United States is now running uphill to re-establish domestic chip manufacturing capacity, which mattered to supply chains for a variety of goods during the pandemic and also undergirds the development of AI.

To build a resilient society in the face of AI's widespread adoption, we therefore argue that the right approach is neither do-nothing nor wait-and-see but instead a proactive, structural approach. Although resilience involves weathering the challenges that may come, a person, institution, or system needs to be resilient *prior to* the challenge becoming a crisis. Some commentators thus refer to "resilience by design."[24] A proactive, structural approach seeks to build into the structures of the economy, society, and national security the design features that are necessary for individuals, institutions, and communities to be resilient.

The mechanisms of resilience can be procedural or substantive.[25] Procedural mechanisms include rules and processes for making decisions—ex ante or ex post—that allow for evaluating the situation. Scholars and process theorists have identified a wide variety of lessons for improving decisionmaking and evaluating systems: Checklists can help prevent mistakes in fast-moving moments.[26] Preplanning and preset procedures, perhaps paradoxically, are more successful than maximal flexibility in managing crises effectively.[27] Redun-

[19] Public Law 119-12, TAKE IT DOWN Act; U.S. Senate Committee on Commerce, Science, and Transportation, "The TAKE IT DOWN Act: List of Supporting Organizations."

[20] Virginia General Assembly, An Act to Amend and Reenact Section 18.2-386.2 of the Code of Virginia.

[21] Chesney and Citron, "Deep Fakes."

[22] Cole, "AI-Assisted Fake Porn Is Here and We're All Fucked."

[23] Ferris, "Biden Signs CHIPS Act, Intended to Relieve the Pandemic-Era Computer Chip Shortage"; Miller, *Chip War*.

[24] Fiksel, *Resilient by Design*.

[25] Marchant and Stevens, "Resilience," p. 254. However, we depart from the authors in how we characterize the specifics within each category.

[26] Gawande, *The Checklist Manifesto*.

[27] Super, "Against Flexibility."

dancy offers a backstop to ensure sound decisionmaking. And periodic assessments, such as after-action reviews, can help improve how individuals and groups function.[28] Substantive mechanisms are far wider in design because they are contextual, but the central aim of such policies is to ensure that a person, institution, or community has the capabilities needed to weather potential challenges. Examples include social safety nets, stockpiles of goods, and community connectivity.

With respect to AI, policymakers should prioritize policies that ensure that the market economy, individuals, communities, and national security institutions are resilient. This effort includes creating the policy foundations for an adaptable workforce and economy that reduce instability and inequality; building individual psychological resilience through developing personal agency and fostering strong and supportive social communities; and establishing procedures and substantive policies to withstand and respond to cyberattacks. Importantly, actions along these lines will not only have benefits for AI but will also strengthen resilience in the face of other challenges. The ultimate goal would be a society that can adopt AI at scale while minimizing instability, crises, and other disruptions that harm individuals and the country.

A Resilient Economy

The economic consequences of AI receive significant attention. In this section, we discuss the impact of AI on the quality of work, near-term effects on pricing, market concentration, and inequality. We then outline policies to improve economic resilience to those effects.

Many predict that AI will have macro-level economic effects, particularly on jobs and the future of work. Anthropic's Dario Amodei has suggested that AI could destroy half of entry-level white collar jobs.[29] Policy experts, such as Molly Kinder at the Brookings Institution, have offered projections of the types of job losses that AI might induce.[30] Media reports frame job losses as a significant concern for workers, and early indicators show that AI may already be affecting jobs for specific demographics and industries.[31] Some economists, such as David Autor, are more hesitant to jump to mass unemployment, observing that AI could create opportunities for augmenting work rather than merely automating it.[32] Still others, such as Jensen Huang of Nvidia, do not believe AI will lead to massive job losses, unless "the world runs out of ideas."[33]

Predictions are difficult. But it seems hard to imagine that there will not be some amount of automation and augmentation that will lead to both some degree of job losses from increased efficiencies for certain workers and some number of new jobs created that never existed before. The scale, timing, and net effects are inherently uncertain, but that uncertainty does not mean there will not be disruption, change, and a transition—as there has been with the diffusion of other general-purpose technologies. Industrialization reshaped the economy, moving people from farms to factories over a century ago. Advances in information and communications technologies vastly sped up the time it takes to record, print, copy, and disseminate written communications—disrupting various jobs from typists to couriers.

---

[28] For a history of after-action reports in the Army, see Morrison and Meliza, *Foundations of the After Action Review Process*. After-action reviews also have been applied in other contexts. For a discussion on evaluation after-action reviews in fire stations, see, for example, Allen, Baran, and Scott, "After-Action Reviews." For a discussion on periodic review requirements, see Marchant and Stevens, "Resilience," p. 256.

[29] VandeHei and Allen, "Behind the Curtain."

[30] Kinder et al., *Generative AI, the American Worker, and the Future of Work*.

[31] Brynjolfsson, Chandar, and Chen, "Canaries in the Coal Mine?"

[32] Autor and Thompson, "Expertise."

[33] Quiroz-Gutierrez, "Jensen Huang Says AI Isn't Likely to Cause Mass Layoffs Unless 'the World Runs Out of Ideas.'"

At the macro level of labor markets, the question of how to address this disruption is one that is not new and, importantly, is not specific to AI. It has existed with other technological changes, which both augmented and automated work, and similar questions arise with other policy changes, such as increased offshoring because of free trade agreements. Therefore, the challenge is not necessarily how to address AI-specific job losses but how to make workers and labor markets more resilient generally.

But just as the field of ecology evolved from seeing static environments to complex adaptive ecosystems,[34] the impact on work and workers is more just the macro-level net impact on job numbers. At the micro level, technology frequently changes the quality and type of work people do, and in some categories, it can make workers significantly worse off. Take the examples of how automation and AI have changed trucking and customer support work.

In the 2010s, truck driving was frequently heralded as a field that would soon be automated.[35] But as of mid-2025 at least, more than 1.5 million U.S. truckers are driving, more than any monthly measure in the 2010s.[36] The trucking example is instructive for two reasons. First, the timeline of prediction seems to have been wrong, even if automotive automation technology is advancing. Second, technology did transform trucking by changing the nature and quality of the work. Policymakers encouraged the adoption of new surveillance technologies—electronic logging devices—in hopes of addressing safety issues from truckers driving for too long without breaks and rest. Although perhaps well-intentioned, this approach worsened an underlying issue of how truckers are paid and how trucking companies operate. According to the drivers themselves, as the leading sociological study shows, the experience of being a trucker has gotten worse, truckers attempt to evade—or even destroy—the technology, and they have many complaints about pay and conditions.[37] It is perhaps no surprise that there is a trucker shortage.[38]

In customer support, companies increasingly use AI-enabled management software that degrades working conditions. Image recognition systems analyze photos taken each minute from employees' webcams for behavioral anomalies, and audio analysis tools are used on agents' tone, speed, and volume of speech to gauge empathy. Workers see these systems being used to determine disciplinary actions, leading to increased stress and absenteeism and decreased job satisfaction, even though repeated studies show the accuracy of these technologies used in workplaces to be questionable.[39] Other surveillance technologies, such as keystroke and mouse tracking, are used to determine idle time, leading to dehumanizing management techniques, such as quantifying the number of minutes per month that an agent can take bathroom breaks. This degree of surveillance leads customer support to report that workers experience "chronic anxiety and insomnia."[40]

In both examples, there will be executives who cheer AI as resulting in great efficiencies and profits, while the experience of work is miserable for truckers and support agents. In these examples, workers became AI jockeys: humans who serve technology rather than technology serving humans. Science fiction author and technologist Cory Doctorow has referred to this as the "reverse centaur problem." When technologies are like a *centaur* (a human head in control), they can expand a person's capacities. But a *reverse centaur* (a human

[34] Martin-Breen and Anderies, *Resilience*, pp. 36–37.

[35] Frey and Osborne, "The Future of Employment."

[36] U.S. Bureau of Labor Statistics, "All Employees, Truck Transportation [CEU4348400001]."

[37] Levy, *Data Driven*.

[38] Cameron, "America Doesn't Have Enough Truck Drivers."

[39] Christl, *Surveillance and Algorithmic Control in the Call Center*, pp. 35–39, 43–44.

[40] Christl, *Surveillance and Algorithmic Control in the Call Center*, p. 39.

body as the workhorse and the technology as the brains) is far less desirable.[41] These shifts have consequences for people's happiness, dignity, and self-worth.

AI is likely to transform markets themselves in additional ways (absent policy action) beyond the nature of work. First, although the long-term effects of AI on such economic matters as consumer prices are hard to predict, near-term effects are more foreseeable. AI is increasingly used to enable price hikes in the form of dynamic and personalized pricing.[42] As companies collect people's data, they can use AI to figure out exactly when people are price-insensitive and need to buy goods or services and then can charge as much as possible for them. Airlines have been pioneers in dynamic pricing for years, and airline consultants now push integrating AI into their pricing systems as a way to further increase consumer prices.[43] Media reports suggest grocery stores have considered similar strategies,[44] and a recent investigation found that the delivery service Instacart was varying grocery prices by as much as 23 percent.[45]

Second, AI is likely to deepen the current era of monopoly and oligopoly, relative to other periods of U.S. history.[46] Many layers in the AI-tech stack are unlikely to be competitive, because of high capital costs for entry, network effects, efficiencies of scale, and switching costs. The result are emergent oligopolies—within markets for chips, cloud computing, and foundation models. Big AI companies are starting to vertically integrate up and down the AI-tech stack, limiting opportunities for competition in the platform-dependent layers.[47] Over time, this effort is likely to also lead to higher prices, as "a long line of economic literature argues" that increased competition is associated with lower prices, increased product quality, and greater innovation.[48] AI will also enable further cartel-like behaviors within other industries; for example, algorithms have been used to coordinate (and raise) prices in rental housing.[49] Absent effective regulatory policies to prevent this, we should expect further innovations along these lines.

Finally, on the current policy trajectory, AI is also likely to deepen inequality. Economic inequality is deeply problematic from the perspective of societal and political resilience. Since the times of the ancient Greeks and Romans, people have recognized that economic inequality is a destabilizing force, leading to divides between the rich and poor that can erupt into protests, violence, and revolution.[50] Past technological revolutions have also deepened inequality and led to significant imbalances of political power: The industrial revolution begat the Gilded Age of robber barons. The tech revolution led to what some have called a Second Gilded Age, in which the existing levels of inequality are at century-level highs.[51] Signs of extreme wealth concentration are already appearing. On the *Forbes* Real Time Billionaires tracker, as of early 2026, each of

[41] Doctorow, "Reverse-Centaurs and Chickenization."

[42] Nguyen, "The Next Frontier of Surveillance."

[43] McCarthy, "How Delta Is Using AI for Ticket Pricing and What It Means for Air Travel."

[44] Grant, "In These Grocery Stores, Prices Change While You Watch."

[45] Wells et al., "Same Cart, Different Price."

[46] Decker and Williams, "A Note on Industry Concentration Measurement" (which notes that "concentration has generally risen in recent decades"). See also Wu, *The Curse of Bigness*; Stoller, *Goliath*; Sitaraman, *The Great Democracy*.

[47] Narechania and Sitaraman, "An Antimonopoly Approach to Governing Artificial Intelligence"; Corrigan, *Promoting AI Innovation Through Competition*.

[48] Council of Economic Advisers, *Benefits of Competition and Indicators of Market Power*.

[49] Vogell, "America's Largest Landlord Makes Deal with DOJ to Settle Price-Fixing Claims in RealPage Case."

[50] Plato, *The Republic*; Aristotle, *Politics*; for more-recent discussions that include discussions of the role of technology, see United Nations Department of Economic and Social Affairs, *World Social Report 2020*; Wu, *The Age of Extraction*.

[51] Zeitz, "The Gilded Age Is Back—and That Should Worry Conservatives."

the top five, and eight of the top ten, richest men lead or led companies central to today's AI boom.[52] Beyond the CEOs of companies, leading AI researchers are getting pay packages worth more than one-quarter of $1 billion in some instances.[53] The godfather of AI, computer scientist Geoffrey Hinton, predicted that "AI will make a few people much richer and most people poorer."[54]

Building a resilient economy will therefore require addressing inequality and building economic security for all—the kind of economic security that allows people to take risks, adapt, and transform themselves and their livelihoods without fear of financial disaster. Household economic security is foundational to social and economic resilience. Economic status tracks many of the important metrics of resilience and general well-being: life expectancy, physical and mental health outcomes, housing security, social connectedness, educational attainment, and so on.[55] And decreases in economic security are associated with increases in "deaths of despair" (i.e., drug-related, alcohol-related, and suicide deaths).[56]

As a policy matter, building economic resilience will require strengthening and simplifying the United States' overly complex, and incomplete, social infrastructure: unemployment insurance, health care, education, retirement, collective bargaining, and other basic social protections to provide economic security that AI adoption might degrade.[57] It will mean structuring markets with fair rules—such as enforcing and strengthening anti-monopoly laws, bolstering collective labor bargaining, and applying such policy tools as price controls—so that people are treated with respect and can exercise their autonomy and so that smaller businesses can thrive without being acquired by the largest firms. In the workplace, that means giving workers a seat at the table in determining how and when AI should be deployed at work and prohibiting particularly intrusive or inhibiting surveillance (e.g., during off-duty times, of personal devices, in homes, in ways that discourage unionization). For consumers, it means banning surveillance pricing so individuals can comparison shop without getting price gouged. And it means addressing inequality. There are many ways to do so, including through tax policy. One AI-specific idea would be to give a dividend from or an ownership share in AI companies to every American because everyone contributed to the data that make AI possible. Other proposed ideas include instituting wealth taxes and increasing corporate taxes.

Resilient Individuals and Communities

About two decades ago, the internet started shifting from static webpages to interactive websites and mobile apps based on user-generated content. Central to this time is the rise of modern social media platforms—such as Facebook, Twitter/X, Instagram, Snapchat, and TikTok—and the cultural changes they enable, both good and bad. In this section, we discuss two issues that became prominent during the rise of social media that are now being amplified by AI: a mental health crisis among children and business models predicated on surveillance.

The lessons of these failures of social media are important because AI products are moving in the direction of social networks in several ways: AI companies are releasing social networks (e.g., OpenAI's Sora) and social networks are investing heavily in AI (e.g., Meta Superintelligence Labs, xAI's Grok), AI companion

[52] "The World's Real-Time Billionaires List."

[53] Isaac, Tan, and Metz, "A.I. Researchers Are Negotiating $250 Million Pay Packages."

[54] Criddle, "Computer Scientist Geoffrey Hinton."

[55] Barakat and Konstantinidis, "A Review of the Relationship Between Socioeconomic Status Change and Health."

[56] Knapp et al., "Economic Insecurity and Deaths of Despair in U.S. Counties," p. 2.

[57] Greenstein, *Changes in the Safety Net over Recent Decades and Their Impact*; Bremmer, *The Power of Crisis*.

apps mimic the data-attention features of social networks (e.g., Replika, Character.AI),[58] and mainstream chatbots are incorporating social media–like features (e.g., advertising, integrated shopping).[59]

The era of social media is associated with significant consequences for children, privacy, and information integrity, among other social consequences. First, in the past few years, society has begun recognizing the online harms experienced by young people, especially teen girls. Jonathan Haidt argues in his book, *The Anxious Generation*, that smartphones, social media, and online engagement have been primarily driving sharp upticks in anxiety, depression, loneliness, and suicidal ideation, along with reduced self-confidence and attention spans, since the 2010s. Some commenters question Haidt's work, often citing a study by the National Academies of Science, Engineering, and Medicine that concludes that there is not sufficiently robust research to establish a causal link between social media and population-level mental health harms.[60] However, this logic typifies the failures of the second policy approach we presented in the "Resilience and AI Policy" section (i.e., seeking solutions only after crises are fully evident), limiting society's ability to take a resilience-based approach. As then–Surgeon General Vivek Murthy stated about this crisis, "in an emergency, you don't have the luxury to wait for perfect information."[61] His report is a call for action in the context of research findings: "[T]he current body of evidence indicates that while social media may have benefits for some children and adolescents, there are ample indicators that social media can also have a profound risk of harm to the mental health and well-being of children and adolescents."[62] In addition to calling for more research, in his report, Murthy urges action: "[W]e must . . . urgently take action to create safe and healthy digital environments that minimize harm and safeguard children's and adolescents' mental health and well-being during critical stages of development."[63]

As AI and social media increasingly intersect, the immediate-term consequences include technology companies developing features and products that could worsen mental health and social interaction trends. Already, individuals are using chatbots as therapists, new companion bot tools are being released, and lawsuits have been filed by the parents of children who have died by suicide after using those chatbots.[64] If the unintended consequence of Instagram, originally a camera app that allowed users to share filtered photos, was a meaningful decline in the self-confidence of teens, the unintended consequences of children depending on nonhuman friends for social interaction could be much worse.[65]

Responses to these dangers have varied. Federal lawmakers have proposed legislation to require companies to consider the safety of children when designing products, but these proposals have not advanced.[66] Multiple states have enacted child-safety laws, though many are being challenged in court.[67] Local policymakers, galvanized by activist groups of parents and others, have found success in banning phones during school hours.[68] And a strong grassroots desire to prevent technological harms to children and create the

[58] Bietti, "The Data-Attention Imperative."

[59] Barcay, "Advertising Is Coming to AI."

[60] National Academies of Sciences, Engineering, and Medicine, *Social Media and Adolescent Health*.

[61] Murthy, "Surgeon General."

[62] Office of the Surgeon General, *Social Media and Youth Mental Health*, p. 4.

[63] Office of the Surgeon General, *Social Media and Youth Mental Health,* p. 4.

[64] Hill, "A Teen Was Suicidal."

[65] Abrams, "How Can We Minimize Instagram's Harmful Effects?"

[66] Paul, "Parents Are Desperate to Protect Kids on Social Media."

[67] Tanner and Turner Lee, "Children's Online Safety Laws Are Failing LGBTQ+ Youth."

[68] Higham, "Map Shows US States with School Phone Bans."

space for more social interaction unmediated by technology has recently become mainstream across parent groups and even medical organizations.[69] At the same time, the big AI companies have supported blocking states and local governments from enacting or enforcing any AI regulation—a policy that President Donald Trump has sought to advance via executive order.[70]

A second social challenge stems from advertising as the dominant business model for many big tech companies. Although online advertising began, in form and function, similar to its offline predecessors (i.e., an advertiser pays a media property to show text and images publicizing a product to viewers of that media), Google and Facebook in particular quickly realized that their data about user behavior could be used for targeting ads. This evolution to privacy-invasive advertising, which some call the internet's Original Sin,[71] was part of a larger shift in the economic model of much of Silicon Valley toward what Shoshana Zuboff labeled "surveillance capitalism" that incentivizes companies to collect more information about their users and created an industry of opaque data brokers that trade in highly personal information.[72] For many years now, AI technologies have been used in advertising to inform ad content, facilitate real-time bidding for placement, microtarget populations, match user-generated content and ads, test-ad variant efficacy, and more.[73] More recently, OpenAI has announced that it will begin integrate advertising into its ChatGPT product offerings, promising that "ChatGPT's responses are driven by what's objectively useful, never by advertising" and "your data and conversations are protected and never sold to advertisers."[74] These promises recall the 1998 academic paper by Google's founders about the "transparent" search engine as competition to ones with the biased and insidious business model of advertising.[75]

Ultimately, AI has enabled content recommendations to increase user engagement and, in turn, enhance advertising. With the adoption of AI, business, government, and other sectors will have even greater incentives to collect personal data via real-time facial recognition of live video feeds of public areas, automated license plate readers and location tracking, and even increasingly sophisticated forms of gait recognition (i.e., near-unique patterns in how people walk).

These forms of inescapable surveillance threaten individual autonomy and democratic values. Near-constant surveillance is happening in online and offline spaces because of the ease with which AI can analyze enormous amounts of data and make those insights commercially useful for advertisers. Ubiquitous surveillance erodes autonomy because people need spaces "free from others' gaze, judgement, questions, and intrusions . . . breathing space."[76] Without that breathing room, free expression and autonomy are severely limited by what the subjects of surveillance believe is acceptable to the powerful, leading to individuals self-censoring private conversations and explorations.[77] A free and liberal democracy is ultimately predicated on people making key decisions about their society—who to vote for, whether to challenge an incumbent

[69] Vasconcellos et al., "Electronic Screen Use and Children's Socioemotional Problems"; American Medical Association, "AMA Highlights Harmful Effects of Screen Time in Youth."

[70] Executive Order 14365, "Ensuring a National Policy Framework for Artificial Intelligence"; Kang, "Emboldened by Trump, A.I. Companies Lobby for Fewer Rules."

[71] Zuckerman, "The Internet's Original Sin."

[72] Zuboff, *The Age of Surveillance Capitalism*.

[73] Ford et al., "AI Advertising."

[74] Simo, "Our Approach to Advertising and Expanding Access to ChatGPT."

[75] Brin and Page, "Reprint of: The Anatomy of a Large-Scale Hypertextual Web Search Engine" (original paper published in 1998).

[76] Véliz, *Privacy Is Power*.

[77] Zuboff, *The Age of Surveillance Capitalism*.

politician, when to protest, how to organize, who to do business with, how to worship—on their own and collectively based on information that reflects a shared reality in a "zone of privacy."[78] Ultimately, as privacy scholar Carissa Véliz concluded, "The power that privacy grants us collectively as citizens is necessary for democracy."[79]

A resilience approach to the social challenges of AI needs to take a structural approach rather than the piecemeal, narrow reforms that are generally proposed to address these issues. Drawing on the lessons of psychological resilience, research shows that individuals do better when they are connected to other people personally and have strong social support systems. Research shows that loneliness is a public health crisis and that interpersonal engagement is critical to happiness and well-being.[80] This finding is not surprising, given that humans are social animals, but it takes on critical importance in thinking about how to ensure individuals are resilient in an age of artificial connections that crowd out relationships in the real world. Interestingly, ecological resilience also depends on "the persistence of relationships within a system,"[81] in a way that is instructive about the importance of civic institutions and communities that produce those social connections.

For individuals, building resilience through stronger social ties means structuring space and time to foster personal connections and development—without digital devices and with privacy. Many have already made proposals in this direction. Haidt has argued for banning smartphones in schools to help students learn and prevent a variety of developmental issues that teenagers with smartphones exhibit.[82] Legal scholar Elettra Bietti describes "non-alienated time as a sanctuary and public good" that can help with the fact that society has shifted from information scarcity to information overload.[83] Some summer camps have prohibited cell phones altogether, so kids develop relationships with each other and with the outdoors, unmediated by technology.[84] Small groups of people have taken up flip phones and even landline telephones as an alternative to smartphones for their children to communicate.[85] Far from theoretical ideas, these efforts build on the years of experiences of educators recognizing the benefit of digital technology-free zones: In 2009, 91 percent of individual public schools banned cell phones, which dropped to 66 percent in 2015. Now, states are moving back: Three dozen states have enacted phone restrictions or bans in schools.[86] Relatedly, a law in Australia prohibits social media accounts for children younger than 16, and the European Parliament urged European Union members to adopt similar national measures.[87]

Psychological resilience is also about problem-solving, a positive outlook on life, and an ability to communicate and engage with others effectively. AI potentially also threatens these elements, especially as kids could rely on technology rather than learning how to think. Schools are bringing back handwritten blue book exams and in-class participation and engagement as ways to ensure that students learn rather than outsource

[78] Fukuyama, *Liberalism and Its Discontents*.

[79] Véliz, *Privacy Is Power*, p. 82.

[80] Office of the Surgeon General, *Our Epidemic of Loneliness and Isolation*.

[81] Walker and Cooper, "Genealogies of Resilience," p. 146, quoting Holling, "Resilience and Stability of Ecological Systems."

[82] Haidt, *The Anxious Generation*.

[83] Bietti, "The Data-Attention Imperative," pp. 48–49, 52–55.

[84] Gibson, "The Latest Reason to Send a Teen to Summer Camp?"

[85] Fares, "Gen Z Goes Retro."

[86] Vigdor, "New Jersey Is Latest State to Ban Student Phones in Schools."

[87] "What Countries Do to Regulate Children's Social Media Access."

thinking to AI chatbots.[88] In the educational context, policy expert Oren Cass has proposed reviving computer labs in primary and secondary education—a specific class in which students learn how to use technology, so as to preserve other parts of the school day for learning without reliance on technology.[89] Even Alpha School, a school created to focus on AI-based learning, builds most of its day around non-AI activities.[90]

These kinds of proposals all share something important in common: They *structurally* build time and space for personal development and interpersonal engagement—without specific technologies that distract and alienate. This is different from relying on individuals to police themselves, with such nudges as disclosures of time spent online. Part of the reason these structural reforms are critical is because the temptations of technology can create a collective action problem. Many people might wish to avoid technology in certain settings (such as schools), but, unless everyone does, the presence of some using technology creates social pressure for others also to do so.

A more fundamental form of structural reconfiguring that can benefit adults and kids would be banning extractive business models, such as surveillance advertising, and requiring data minimization to stem the limitless data collection and hoarding.[91] Today's data-attention platforms depend on data to target content and ads.[92]

As applied to today's AI, the parallels are evident. Rather than lose a generation addicted to AI bots or companions and ceding to ubiquitous surveillance, as we have with smartphones and social media, we should build time and space away from AI right now at the technology's incipiency. That means designing curricula and school policies that enable children to learn without AI before exposing them to possible benefits of learning with AI, as well as developing the skills of writing and thinking without AI before being able to rely on tools that generate and refine text. That also means developing social and cultural norms that encourage regular time without technology and related surveillance at all, so that people can build relationships with family, friends, neighbors, and co-workers—so they have people to talk to, not just technologies.

Resilient National Security

In many ways, national security was the starting point of AI. The Defense Advanced Research Projects Agency (DARPA) funded much of the most consequential AI research and development in the second half of the 20th century because of AI's potential to create "game-changing capabilities" for defense and warfighting.[93] Most often, DARPA funded university-based researchers, though it and other parts of the U.S. Department of Defense[94] also initiated and funded other labs, companies and contractors, and research think tanks.[95]

Today, AI is shifting many dynamics in national security. In this section, we discuss tactical warfighting; the development of chemical, biological, radiological, and nuclear (CBRN) weapons; and cybersecurity.

[88] Cohen, "They Were Every Student's Worst Nightmare."

[89] Cass, "Bring Back the Computer Lab."

[90] Alpha School, "Welcome to Alpha."

[91] See, for example, U.S. House of Representatives, Banning Surveillance Advertising Act.

[92] Bietti, "The Data-Attention Imperative."

[93] Fouse, Cross, and Lapin, "DARPA's Impact on Artificial Intelligence."

[94] Executive Order 14347, signed September 5, 2025, authorized the use of Department of War as a secondary name for the U.S. Department of Defense. This publication refers to the secretary and department by their current statutory names under Public Law 81-216, National Security Act Amendments of 1949.

[95] RAND is an example of a think tank that was started to serve the Department of Defense. See Prasad and Schneide, "When RAND Made Magic in Santa Monica."

The notion of national security is certainly much broader than just these three domains,[96] but we focus on these three domains as illustrative of requiring systemic solutions and because policies in these areas could represent major steps toward national security resilience to particularly salient changes anticipated from AI.

First, AI and automated weapon systems are likely to increase lethality in warfighting.[97] Militaries have long leveraged leading technologies to increase battlefield effectiveness, and, in many ways, there is "nothing particularly surprising or inherently worrisome" about that in the AI era.[98] But to see the challenges, consider the fact that for more than a decade, the U.S. military has grappled with the implications of a different new technology: lethal drones. Since the George W. Bush administration began using remote-operated lethal strikes from unmanned aerial vehicles (UAVs) in Iraq, Afghanistan, and elsewhere, every subsequent administration has significantly shifted its policies related to when and how lethal drone strikes can occur.[99] The lack of consistency in these policies is especially troubling as nations around the world increasingly experiment and deploy UAV systems enabled with AI.

If the ethical issues presented by these systems in the recent wars in Gaza, Ukraine, and Nagorno-Karabakh are any indication,[100] ethical dilemmas from AI systems will only intensify. One major area in which ethical questions have emerged in diplomatic discussions is lethal autonomous weapon systems (LAWS). Although LAWS are not in widespread development today, experts have said that if the United States believed that a geopolitical adversary developed such technologies, the United States would have to do the same.[101] The diplomatic dimensions of military AI that could avoid this dynamic are also challenging.

Second, the United States focused significant attention on the impact of AI on CBRN risks, and real progress has been made to mitigate risks. However, with respect to nuclear weapons, only 61 countries agreed to ensure human control of AI used in nuclear systems.[102] China was not part of this agreement, though it agreed to similar principles bilaterally with the United States.[103] But several nuclear-armed states, including Russia, have not made such agreements. In addition, multinational approaches do not cover the growing CBRN threat from nonstate actors.

Many see the increase in biosecurity threats as the most concerning risk from rapid AI development. Innovation in biology cuts two ways: New AI-developed pharmaceuticals could save lives, while novel AI-developed pathogens could threaten them. Access to the necessary knowledge and technologies (e.g., AI biological design models, benchtop nucleic-acid synthesizers, cloud labs) is expanding. Biosecurity risks existed and were expanding well before today's wave of AI, but many fear that AI systems could one day enable a bad actor to develop a high-consequence pathogen that could evolve into a pandemic.[104]

Third, AI is changing the nature of cybersecurity. Today, cyberattackers have an inherent advantage over cyber defenders—the former have to find one exploitable vulnerability, while the latter have to protect every digital connection. Observers debate whether AI will further tilt cyberspace to the advantage of attackers or

[96] White House, *National Security Strategy*.

[97] National Intelligence Council Strategic Futures Group, *Global Trends 2040*.

[98] Weissman and Wooten, "A.I. Joe," p. 4.

[99] Savage and Schmitt, "Trump Relaxes Limits on Counterterrorism Strikes Outside Conventional War Zones."

[100] Satti, "AI."

[101] Sayler, *Defense Primer*.

[102] Rosen, "From Principles to Action."

[103] Renshaw and Hunnicutt, "Biden, Xi Agree That Humans, Not AI, Should Control Nuclear Arms."

[104] National Academies of Sciences, Engineering, and Medicine, *The Age of AI in the Life Sciences*; Pannu et al., *Defining Hazardous Capabilities of Biological AI Models*.

shift the dynamics of cyberspace to enable greater defenses.[105] Because nearly all aspects of society are dependent on digital infrastructures of various types, the surface area for cyber risks is vast.[106]

Consider, for example, the national security risks associated with cloud computing. Nearly all major corporations; a growing number of governmental organizations, including many parts of the Department of Defense; and many critical infrastructure providers depend on cloud providers, creating a vast attack surface for nation-state adversaries. There is additional risk because our modern cloud infrastructure is critical for geopolitical priorities such as AI. Because cloud computing is largely unregulated, the U.S. government has incomplete methods of understanding the risk or tracking issues.[107]

Governmental organizations have long issued various recommendations to improve the resilience of cyberspace, including setting minimum service-delivery goals;[108] embedding anticipation, recovery, and adaptation into system engineering;[109] ensuring governmental and economic continuity to reduce cyberattack payoff;[110] shifting responsibility toward long-term investments;[111] and prioritizing research on "hard problems."[112] However, these efforts do not solve the broader systemic issues or change the trajectory of cybersecurity. A broader ideal of cybersecurity would treat resilience as a public good and treat "public cybersecurity" similarly to the way policymakers approach public health, as Deirdre Mulligan and Fred Schneider have proposed.[113]

Experts anticipate that AI is making the development and deployment of cyberattacks easier by potentially aiding the search for vulnerabilities to exploit, developing personalized social engineering techniques, and developing hard-to-detect malicious code. But AI also has the potential to help digital infrastructure managers find vulnerabilities to patch, develop defenses for attacks, and detect malicious code.

A resilience framework can help organize and inspire national security policy priorities in the context of AI adoption. For starters, policymakers should focus on evaluating and reforming necessary processes that could help strengthen resilience. Some scholars and analysts have argued that the introduction of AI into military contexts may not be as seamless as in business, because training data might be scarce or flawed and because the judgments about the goals may be uncertain.[114] The result is that processes that ensure and create the space for human involvement might actually be more important rather than less important.[115] The International Committee of the Red Cross has suggested that decisionmaking will need to include space for humans to ensure compliance with the laws of war[116] but also will need to protect against humans rubber-

[105] Lohn, *Anticipating AI's Impact on the Cyber Offense-Defense Balance*.

[106] White House, *National Resilience Strategy*.

[107] For a broader discussion about market and national risks associated with cloud computing, see Ramzanali, "How to Regulate the Cloud."

[108] President's Council of Advisors on Science and Technology, *Report to the President on Strategy for Cyber-Physical Resilience*.

[109] Ross et al., *Developing Cyber-Resilient Systems*.

[110] Cyberspace Solarium Commission, *Final Report*.

[111] White House, *National Cybersecurity Strategy*.

[112] National Academies of Sciences, Engineering, and Medicine, *Cyber Hard Problems*; National Academies of Sciences, Engineering, and Medicine, "Forum on Cyber Resilience."

[113] Mulligan and Schneider, "Doctrine for Cybersecurity," pp. 70–71.

[114] Goldfarb and Lindsay, "Prediction and Judgment"; Probasco et al., *AI for Military Decision-Making*.

[115] Goldfarb and Lindsay, "Prediction and Judgment."

[116] International Review of the Red Cross, *ICRC Position Paper*.

stamping AI systems.[117] Focusing on these issues and matching solutions, such as bans on certain aspects of AI and warfare[118] and setting up rules for the use of force, should be high priorities. Similarly, process solutions could be a critical component of strengthening the resilience of biological research and improving the resistance and stability of cybersecurity systems.[119]

Substantively, national security policymakers should also seek to ensure that systems are resilient by design. Cybersecurity offers a helpful example. Cybersecurity failures are often blamed on human error (e.g., weak and repeated passwords, phishing, misconfigured software). But individuals are often the least well-positioned to ensure secure systems: They generally have less knowledge and little incentive to worry about systemic risks. Experts fall prey to online scams, even before AI's involvement.[120] A better system design, as the 2023 National Cybersecurity Strategy recommends, would be to shift burdens from individuals, small businesses, and other end users to companies that control digital infrastructure, such as cloud providers and now AI model developers.[121] Policy options could include requiring security-by-design regimes; positive incentives, preferences, or support for building such regimes; and legal liability for failures to incentivize the adoption of stronger security protocols.

At the same time, some cyber instances are beyond the capacity of even digital infrastructure providers. For example, no one company is likely to be able to respond to nation-state investments in breaking cyber intrusions into critical networks (e.g., Salt Typhoon).[122] These kinds of attacks require the federal government to more seriously prioritize mandating technical solutions (e.g., post-quantum cryptography, zero-trust architectures) and funding digital transitions. As a result, resilience may require greater federal government involvement, beyond ways assumed by prior cybersecurity reviews. Cyber incidents today are handled mainly in private markets: Firms hire consultants to design and test systems; buy cyber insurance to cover possible losses; and turn to corporate responders, such as CrowdStrike, during attacks. As AI amplifies threats, the federal government may need to assume more of these roles. Urban firefighting offers an analogy. After the Great Fire of London in 1666, new regulations spurred private fire insurance; buildings bore fire marks for insurers' brigades, but one policyholder's protection meant little if a neighbor's building burned.[123] Over time, public options for firefighting emerged: Boston funded a small fire company in the late 1600s.[124] Today, firefighting is almost entirely public, with only niche private fire responders. Similarly, some commentators have proposed a more centralized cyber response force,[125] the digital equivalent of a public fire brigade, to contain major incidents as AI-driven attacks outpace private capacity and affect larger swaths of the digital world.

To increase the resilience of a material, as stated earlier, engineers can increase resistance (keeping form under pressure), elasticity (flexing or bouncing back after pressure), or stability (withstanding stress with-

[117] Holland, *Decisions, Decisions, Decisions*.

[118] For example, no domestic or international policy exists that prohibits or even limits development of LAWS (see Sayler, *Defense Primer*).

[119] For example, a framework for nucleic acid synthesis screening limited to recipients of federal funding could be expanded to apply more broadly (see National Science and Technology Council, *Framework for Nucleic Acid Synthesis Screening*).

[120] Wilson, "I've Written About Loads of Scams."

[121] White House, *National Cybersecurity Strategy*.

[122] National Security Agency et al., C*ountering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System*.

[123] McAllister, "The Original Firefighters."

[124] Secretary of the Commonwealth of Massachusetts, *History of Firefighting in Boston*.

[125] Wood, "Minnesota Governor Activates National Guard amid St. Paul Cyberattack."

out permanent change). In reflecting on AI's impact on national security, this approach to resilience means asserting and resisting change to deep-seated values as pressures in automated warfare increase. It means flexing our institutional approaches to biological research so that we avoid irreversible attacks. And it means reforming our approach to securing our digital infrastructure so that our digital lives are stable. More systematically, if we want our national security institutions to meet their mission of protecting our country while withstanding outside force or pressure—as is the objective of resilience in the engineering context—we will need to design them from the start to do so.

Conclusion

The societal shifts from AI are well underway. AI tools were in our lives well before the explosion of popularity of today's consumer chatbots that began with the introduction of ChatGPT in late 2022. For many years, AI systems have sorted the content and ads that most people interact with daily online—such as social media, search engines, e-commerce, and streaming services. And AI has been used in less apparent contexts (e.g., facial recognition used on closed-circuit TV footage, bank fraud detection, recidivism forecasting in criminal justice).

Today's AI systems seem to be on an unstoppable trajectory to change every part of society. Even if there are technical limits to the gains from scaling the transformer-based AI architectures that underpin large language models and other systems popular today,[126] investment in AI is continuing at a pace that suggests some degree of ongoing innovation, accelerating product development, and continuing societal adoption. Repeating society's do-nothing response to social media or our current wait-and-see approach to AI policy may lead to irreversible harms.

Instead, as we recommend, society needs a proactive, structural approach to building resilience. Even if we are confident that AI adoption will affect society in significant ways, we cannot predict how or when those changes will materialize. Policies centered on the goal of resilience would transform economic, social, and national security policy domains so that they—and individuals and communities—could better withstand whatever changes and disruptions may come. We have agency in determining how society uses AI, when we should create spaces without AI, and how public policy should respond to the disruptions that individuals experience because of widespread adoption of AI. We should use that human agency to build a more resilient society.

Ultimately, the broad variety of policies we have put forth in this paper is not easy to achieve in today's political environment—pulled together, the policies are transformative. But that is commensurate with the scale of disruptiveness that AI is expected to bring to society, and it is what is needed to benefit from the technological changes that are coming while maintaining the character of a market economy, free individuals, and a secure country. Instead of starting with what is politically feasible in the narrowest sense, policymakers will have to build the political will for a grand strategy for resilience.

[126] Marcus, "The Fever Dream of Imminent Superintelligence Is Finally Breaking."

Abbreviations

AI	artificial intelligence
CBRN	chemical, biological, radiological, and nuclear
DARPA	Defense Advanced Research Projects Agency
LAWS	lethal autonomous weapon systems
UAV	unmanned aerial vehicle

References

Abrams, Zara, "How Can We Minimize Instagram's Harmful Effects?" *Monitor on Psychology*, Vol. 53, No. 2, December 2021.

Allen, Joseph A., Benjamin E. Baran, and Cliff W. Scott, "After-Action Reviews: A Venue for the Promotion of Safety Climate," *Accident Analysis & Prevention*, Vol. 42, No. 2, 2010.

Alpha School, "Welcome to Alpha: Where Learning Transforms Lives," webpage, undated. As of January 13, 2026:
https://alpha.school/the-program/

American Medical Association, "AMA Highlights Harmful Effects of Screen Time in Youth," press release, November 14, 2017.

Andreessen, Marc, "The Techno-Optimist Manifesto," webpage, Andreessen Horowitz, October 16, 2023. As of January 13, 2026:
https://a16z.com/the-techno-optimist-manifesto/

Aristotle, *Politics*, trans. by Carnes Lord, University of Chicago Press, 2013.

Autor, David, and Neil Thompson, "Expertise," *Journal of the European Economic Association*, Vol. 23, No. 4, August 2025.

Barakat, Caroline, and Theodore Konstantinidis, "A Review of the Relationship Between Socioeconomic Status Change and Health," *International Journal of Environmental Research and Public Health*, Vol. 20, No. 13, June 2023.

Barcay, Daniel, "Advertising Is Coming to AI. It's Going to Be a Disaster," *Tech Policy Press*, November 26, 2025.

Bietti, Elettra, "The Data-Attention Imperative," *Florida Law Review*, Vol. 78, last updated October 27, 2025.

Bremmer, Ian, *The Power of Crisis: How Three Threats—and Our Response—Will Change the World*, Simon & Schuster, 2023.

Brennan, Kate, Amba Kak, and Sarah Myers West, *Artificial Power: 2025 Landscape Report*, AI Now Institute, June 3, 2025.

Brin, Sergey, and Lawrence Page, "Reprint of: The Anatomy of a Large-Scale Hypertextual Web Search Engine," *Computer Networks*, Vol. 56, No. 18, December 2012.

Brynjolfsson, Erik, Bharat Chandar, and Ruyu Chen, *Canaries in the Coal Mine? Six Facts About the Recent Employment Effects of Artificial Intelligence*, Stanford Digital Economy Lab, November 13, 2025.

Burgess, Matt, "AI 'Nudify' Websites Are Raking in Millions of Dollars," *Wired*, July 14, 2025.

Cameron, Hugh, "America Doesn't Have Enough Truck Drivers," *Newsweek*, July 10, 2025.

Cass, Oren, "Bring Back the Computer Lab," Institute for Family Studies, July 31, 2025.

Chesney, Bobby, and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review*, Vol. 107, No. 6, December 2019.

Christl, Wolfie, *Surveillance and Algorithmic Control in the Call Center*, Cracked Labs, May 2023.

Cohen, Ben, "They Were Every Student's Worst Nightmare. Now Blue Books Are Back," *Wall Street Journal*, May 24, 2025.

Cole, Samantha, "AI-Assisted Fake Porn Is Here and We're All Fucked," *VICE*, December 11, 2017.

Corrigan, Jack, *Promoting AI Innovation Through Competition*, Center for Security and Emerging Technology, May 2025.

Council of Economic Advisers, *Benefits of Competition and Indicators of Market Power*, issue brief, Executive Office of the President, April 2016.

Criddle, Cristina, "Computer Scientist Geoffrey Hinton: 'AI Will Make a Few People Much Richer and Most People Poorer,'" *Financial Times*, September 5, 2025.

Cyberspace Solarium Commission, *Final Report*, March 2020.

Decker, Ryan, and Jacob Williams, "A Note on Industry Concentration Measurement," FEDS Notes, February 3, 2023.

Doctorow, Cory, "Reverse-Centaurs and Chickenization," in *Enshittification: Why Everything Suddenly Got Worse and What to Do About It*, MCD, 2025.

Executive Order 14365, "Ensuring a National Policy Framework for Artificial Intelligence," Executive Office of the President, December 11, 2025.

Fares, Omar H., "Gen Z Goes Retro: Why the Younger Generation Is Ditching Smartphones for 'Dumb Phones,'" The Conversation, May 9, 2023.

Ferris, Gabe, "Biden Signs CHIPS Act, Intended to Relieve the Pandemic-Era Computer Chip Shortage," ABC News, August 9, 2022.

Fiksel, Joseph, *Resilient by Design: Creating Businesses That Adapt and Flourish in a Changing World*, Island Press, 2015.

Ford, John, Varsha Jain, Ketan Wadhwani, and Damini Goyal Gupta, "AI Advertising: An Overview and Guidelines," *Journal of Business Research*, Vol. 166, November 2023.

Fouse, Scott, Stephen Cross, and Zachary Lapin, "DARPA's Impact on Artificial Intelligence," *AI Magazine*, Vol. 41, No. 2, June 23, 2020.

Frey, Carl Benedikt, and Michael Osborne, "The Future of Employment: How Susceptible Are Jobs to Computerisation?" working paper, Oxford Martin Programme on Technology and Employment, September 1, 2013.

Fukuyama, Francis, *Liberalism and Its Discontents*, Farrar, Straus and Giroux, 2022.

Future of Life Institute, "Pause Giant AI Experiments: An Open Letter," March 22, 2023.

Gawande, Atul, *The Checklist Manifesto: How to Get Things Right*, Metropolitan Books, 2009.

Gibson, Caitlin, "The Latest Reason to Send a Teen to Summer Camp? No Cellphones," *Washington Post*, June 21, 2025.

Goldfarb, Avi, and Jon R. Lindsay, "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War," *International Security*, Vol. 46, No. 3, Winter 2021–2022.

Grant, Conor, "In These Grocery Stores, Prices Change While You Watch," *Wall Street Journal*, August 1, 2025.

Greenstein, Robert, *Changes in the Safety Net over Recent Decades and Their Impact*, Hamilton Project, May 2025.

Haidt, Jonathan, *The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness*, Penguin Press, 2024.

Higham, Aliss, "Map Shows US States with School Phone Bans," *Newsweek*, June 27, 2025.

Hill, Kashmir, "A Teen Was Suicidal. ChatGPT Was the Friend He Confided In," *New York Times*, August 26, 2025.

Holland, Arthur Michael, *Decisions, Decisions, Decisions: Computation and Artificial Intelligence in Military Decision-Making*, International Committee of the Red Cross, No. 4757, April 2024.

Holling, C. S., "Resilience and Stability of Ecological Systems," *Annual Review of Ecology and Systematics*, Vol. 4, 1973.

International Review of the Red Cross, *ICRC Position Paper: Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centered Approach*, IRRC No. 913, March 2021.

Isaac, Mike, Eli Tan, and Cade Metz, "A.I. Researchers Are Negotiating $250 Million Pay Packages. Just Like N.B.A. Stars," *New York Time*s, July 31, 2025.

Kang, Cecilia, "Emboldened by Trump, A.I. Companies Lobby for Fewer Rules," *New York Times*, March 24, 2025.

Kinder, Molly, Xavier de Souza Briggs, Mark Muro, and Sifan Liu, *Generative AI, the American Worker, and the Future of Work*, Brookings Institution, October 10, 2024.

Knapp, Emily A., Usama Bilal, Lorraine T. Dean, Mariana Lazo, and David D. Celentano, "Economic Insecurity and Deaths of Despair in U.S. Counties," *American Journal of Epidemiology*, Vol. 188, No. 12, April 2019.

Konnikova, Maria, "How People Learn to Be Resilient," *New Yorker*, February 11, 2016.

Levy, Karen, *Data Driven: Truckers, Technology, and the New Workplace Surveillance*, Princeton University Press, 2023.

Lohn, Andrew, *Anticipating AI's Impact on the Cyber Offense-Defense Balance*, Center for Security and Emerging Technology, May 2025.

Marchant, Gary E., and Yvonne A. Stevens, "Resilience: A New Tool in the Risk Governance Toolbox for Emerging Technologies," *UC Davis Law Review*, Vol. 51, November 2017.

Marcus, Gary, "The Fever Dream of Imminent Superintelligence Is Finally Breaking," *New York Times*, September 3, 2025.

Martin-Breen, Patrick, and J. Marty Anderies, *Resilience: A Literature Review*, Bellagio Initiative: Institute of Development Studies, Resource Alliance, and Rockefeller Foundation, December 31, 2011.

McAllister, Sean, "The Original Firefighters: How Insurers Protected London from Fire," *Zurich Magazine*, September 1, 2023.

McCarthy, Kelly, "How Delta Is Using AI for Ticket Pricing and What It Means for Air Travel," ABC News, August 5, 2025.

Miller, Chris, *Chip War: The Fight for the World's Most Critical Technology*, Scribner, 2022.

Morrison, John E., and Larry L. Meliza, *Foundations of the After Action Review Process*, U.S. Army Research Institute, July 1999.

Mulligan, Deirdre K., and Fred B. Schneider, "Doctrine for Cybersecurity," *Daedalus*, Vol. 140, No. 4, Fall 2011.

Murthy, Vivek H., "Surgeon General: Why I'm Calling for a Warning Label on Social Media Platforms," *New York Times*, June 17, 2024.

Narayanan, Arvind, and Sayash Kapoor, *AI as Normal Technology*, Knight First Amendment Institute, April 15, 2025.

Narechania, Tejas N., and Ganesh Sitaraman, "An Antimonopoly Approach to Governing Artificial Intelligence," *Yale Law and Policy Review*, Vol. 43, No. 95, Fall 2024.

National Academies of Sciences, Engineering, and Medicine, "Forum on Cyber Resilience," webpage, undated. As of January 13, 2026:
https://www.nationalacademies.org/units/DEPS-CSTB-13-03

National Academies of Sciences, Engineering, and Medicine, *Disaster Resilience: A National Imperative*, National Academies Press, 2012.

National Academies of Sciences, Engineering, and Medicine, *Social Media and Adolescent Health*, National Academies Press, 2024.

National Academies of Sciences, Engineering, and Medicine, *The Age of AI in the Life Sciences: Benefits and Biosecurity Considerations*, National Academies Press, 2025.

National Academies of Sciences, Engineering, and Medicine, *Cyber Hard Problems: Focused Steps Toward a Resilient Digital Future*, National Academies Press, 2025.

National Intelligence Council Strategic Futures Group, *Global Trends 2040: The Future of the Battlefield*, April 2021.

National Science and Technology Council, *Framework for Nucleic Acid Synthesis Screening*, Executive Office of the President, September 2024.

National Security Agency, Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, et al., *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System*, vers. 1.1, U/OO/198904-25, PP-25-3703, 2025.

Nguyen, Stephanie T., "The Next Frontier of Surveillance: Investigating Pricing Systems," *Yale Journal on Regulation*, September 21, 2025.

Nguyen, Tina, "Peter Thiel: Strict AI Regulation Will Summon the Antichrist," *The Verge*, September 25, 2025.

Office of the Surgeon General, *Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community*, U.S. Department of Health and Human Services, 2023.

Office of the Surgeon General, *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*, U.S. Department of Health and Human Services, 2023.

Pannu, Jaspreet, Sarah L. Gebauer, Henry Alexander Bradley, Dulani Woods, Doni Bloomfield, Allison Berke, Greg McKelvey, Jr., Anita Cicero, and Tom Inglesby, *Defining Hazardous Capabilities of Biological AI Models: Expert Convening to Inform Future Risk Assessment*, RAND Corporation, CF-A3649-1, 2025. As of February 5, 2026:
https://www.rand.org/pubs/conf_proceedings/CFA3649-1.html

Paul, Kari, "Parents Are Desperate to Protect Kids on Social Media. Why Did the US Let a Safety Bill Die?" *The Guardian*, February 16, 2025.

Plato, *The Republic*, trans. by Benjamin Jowett, Dover Publications, 2000.

Prasad, Pradyumna, and Jordan Schneide, "When RAND Made Magic in Santa Monica," *Asterisk*, June 2024.

President's Council of Advisors on Science and Technology, *Report to the President on Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World*, Executive Office of the President, February 2024.

Probasco, Emilia S., Helen Toner, Matthew Burtell, and Timothy G. J. Rudner, *AI for Military Decision-Making*, Center for Security and Emerging Technology, April 2025.

Public Law 119-12, TAKE IT DOWN Act, May 19, 2025.

Quiroz-Gutierrez, Marco, "Jensen Huang Says AI Isn't Likely to Cause Mass Layoffs Unless 'the World Runs Out of Ideas,'" *Fortune*, July 15, 2025.

Ramzanali, Asad, "How to Regulate the Cloud: A Blueprint to Address the Market Failures and National Security Risks of Cloud Computing," Vanderbilt Policy Accelerator, September 2025.

Renshaw, Jarrett, and Trevor Hunnicutt, "Biden, Xi Agree That Humans, Not AI, Should Control Nuclear Arms," Reuters, November 17, 2024.

Rosen, Brianna, "From Principles to Action: Charting a Path for Military AI Governance," Carnegie Council for Ethics in International Affairs, September 12, 2024.

Ross, Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, National Institute of Standards and Technology, NIST Special Publication 800-160, Vol. 2, Rev. 1, December 2021.

Satti, Arsalan A., "AI: The New Paradigm of War," Milton Wolf Seminar on Media and Diplomacy, Annenberg School for Communication, University of Pennsylvania, 2024.

Savage, Charlie, and Eric Schmitt, "Trump Relaxes Limits on Counterterrorism Strikes Outside Conventional War Zones," *New York Times*, March 1, 2025.

Sayler, Kelley M., *Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems*, Congressional Research Service, IF11150, January 2, 2025.

Secretary of the Commonwealth of Massachusetts, "History of Firefighting in Boston," video, undated. As of January 13, 2026:
https://www.sec.state.ma.us/divisions/state-house-tours/did-you-know/Firefighting.htm

Simo, Fidji, "Our Approach to Advertising and Expanding Access to ChatGPT," OpenAI, January 18, 2026.

Sitaraman, Ganesh, *The Great Democracy: How to Fix Our Politics, Unrig the Economy, and Unite America*, Basic Books, 2019.

Sitaraman, Ganesh, "A Grand Strategy of Resilience," *Foreign Affairs*, September–October 2020.

Stoller, Matt, *Goliath: The 100-Year War Between Monopoly Power and Democracy*, Simon & Schuster, 2019.

Super, David A., "Against Flexibility," *Cornell Law Review*, Vol. 96, No. 6, September 2011.

Sutton, Jeremy, "What Is Resilience & Why Is It Important to Bounce Back?" PositivePsychology.com, January 3, 2019.

Tanner, Brooke, and Nicol Turner Lee, "Children's Online Safety Laws Are Failing LGBTQ+ Youth," Brookings Institution, July 9, 2025.

Thierer, Adam, *Defending Technological Dynamism & the Freedom to Innovate in the Age of AI*, Civitas Institute, June 6, 2025.

United Nations Department of Economic and Social Affairs, *World Social Report 2020: Inequality in a Rapidly Changing World*, 2020.

U.S. Bureau of Labor Statistics, "All Employees, Truck Transportation [CEU4348400001]," retrieved from Federal Reserve Bank of St. Louis, September 1, 2025.

U.S. House of Representatives, Banning Surveillance Advertising Act, H.R. 5534, September 18, 2023.

U.S. Senate Committee on Commerce, Science, and Transportation, "The TAKE IT DOWN Act: List of Supporting Organizations," May 19, 2025. As of January 13, 2026: https://www.commerce.senate.gov/services/files/53C5E77B-B58C-4BB7-8B56-C4034875D13E

VandeHei, Jim, and Mike Allen, "Behind the Curtain: Top AI CEO Foresees White-Collar Bloodbath," Axios, May 28, 2025.

Vasconcellos, Roberta Pires, Taren Sanders, Chris Lonsdale, Philip Parker, James Conigrave, Samantha Tang, Borja del Pozo Cruz, Stuart J. H. Biddle, Rachael Taylor, Christine Innes-Hughes, et al., "Electronic Screen Use and Children's Socioemotional Problems: A Systematic Review and Meta-Analysis of Longitudinal Studies," *American Psychological Association*, Vol. 151, No. 5, May 2025.

Véliz, Carissa, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, Bantam Press, 2021.

Vigdor, Neil, "New Jersey Is Latest State to Ban Student Phones in Schools," *New York Times*, January 8, 2026.

Virginia General Assembly, An Act to Amend and Reenact, Section 18.2-386.2 of the Code of Virginia, Relating to Unlawful Dissemination or Sale of Images of Another Person; Penalty, Chapter 490, 2019 Acts of Assembly of Virginia, March 18, 2019.

Vogell, Heather, "America's Largest Landlord Makes Deal with DOJ to Settle Price-Fixing Claims in RealPage Case," *ProPublica*, August 12, 2025.

Walker, Jeremy, and Melinda Cooper, "Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation," *Security Dialogue*, Vol. 42, No. 2, April 2011.

Weissman, Robert, and Savannah Wooten, "A.I. Joe: The Dangers of Artificial Intelligence and the Military," Public Citizen, February 29, 2024.

Wells, Katie J., Lindsay Owens, Angel Han, and Alan Smith, "Same Cart, Different Price: Instacart's Price Experiments Cost Families at Checkout," Groundwork Collaborative and Consumer Reports, December 9, 2025.

"What Countries Do to Regulate Children's Social Media Access," Reuters, November 26, 2025.

White House, *National Security Strategy*, October 2022.

White House, *National Cybersecurity Strategy*, March 2023.

White House, *National Resilience Strategy*, January 2025.

Wilson, Michael, "I've Written About Loads of Scams. This One Almost Got Me," *New York Times*, September 18, 2025.

Wood, Colin, "Minnesota Governor Activates National Guard amid St. Paul Cyberattack," *StateScoop*, July 29, 2005.

"The World's Real-Time Billionaires List," *Forbes*, webpage, undated. As of January 13, 2026: https://www.forbes.com/real-time-billionaires/

Wu, Tim, *The Curse of Bigness: Antitrust in the New Gilded Age*, Columbia Global Reports, 2018.

Wu, Tim, *The Age of Extraction: How Tech Platforms Conquered the Economy and Threaten Our Future Prosperity*, Knopf, 2025.

Zeitz, Joshua, "The Gilded Age Is Back—and That Should Worry Conservatives," *Politico*, March 2, 2025.

Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019.

Zuckerman, Ethan, "The Internet's Original Sin," *The Atlantic*, August 14, 2014.

About the Authors

Asad Ramzanali is the director of AI and technology policy at the Vanderbilt Policy Accelerator. His research focuses on the government's role in enabling innovation and regulating harms from technology. He holds a master of public policy.

Ganesh Sitaraman holds the New York Alumni Chancellor's Chair in Law at Vanderbilt University and is the director of the Vanderbilt Policy Accelerator. He teaches and writes about constitutional law, the regulatory state, economic policy, democracy, and foreign affairs. He holds a J.D.