## Affirmative

### 2AC – No Russia AI Lead

#### Non-unique and we’ll pre-empt their uniqueness warrants – the invasion haulted Russia’s AI developments – even if they win that AI is being implemented and developed now – the war severely changed the trajectory of it

* Agrees that Russia was ahead on Ethical AI and AI implementation in 2021 and they planned to continue this onto 2022, but the invasion stopped that progress that they were making that would’ve put them ahead in the first place

Bendett, 22

[Samuel, Adjunct Senior Fellow at the Center for a New American Security and an Adviser at the CNA Corporation, April 15, 2022, “Russia’s Artificial Intelligence Boom May Not Survive the War”, Defense One, <https://www.defenseone.com/ideas/2022/04/russias-artificial-intelligence-boom-may-not-survive-war/365743/>, accessed 7-18-2022, BB]

But talk of AI has been muted since the Russian invasion of Ukraine. Apart from the widespread use of UAVs for reconnaissance and target acquisition and a single display of a mine-clearing robot—all of which are remote-controlled—there is no overt evidence of Russian AI in C4ISR or decision-making among the Russian military forces, other than a single public deepfake attempt to discredit the Ukrainian government. That does not mean AI isn’t used, considering how Ukrainians are now utilizing artificial intelligence in data analysis—but there is a notable absence of larger discussion about this technology in open-source Russian media.

The gap between Russian military aspirations for high-tech warfare of the future and the actual conduct of war today is becoming clear. In January 2021, Colonel-General Vladimir Zarudnitsky, the head of the Military Academy of the Russian Armed Forces General Staff, wrote that the development and use of unmanned and autonomous military systems, the “robotization” of all spheres of armed conflict, and the development of AI for robotics will have the greatest medium-term effect on the Russian armed forces’ ability to meet their future challenges. Other MOD military experts also debated the impact of these emerging technologies on the Russian military and future balance of forces. Russia continued to upgrade and replace Soviet-made systems, part of the MOD’s drive from “digitization” (weapons with modern information technologies for C4ISR) to “intellectualization” (widespread implementation of AI capable of performing human-like creative thinking functions). These and other developments were covered in detail during Russia’s “Army-2021” conference, with AI as a key element in C4ISR at the tactical and strategic levels.

Meanwhile, Russian military developers and researchers worked on multiple AI-enabled robotics projects, including the “Marker” concept unmanned ground vehicle and its autonomous operation in groups and with UAVs.

Toward the end of 2021, the state agency responsible for exporting Russian military technology even announced plans to offer unmanned aviation, robotics, and high-tech products with artificial intelligence elements to potential customers this year. The agency emphasized the equipment is geared toward defensive, border protection, and counter-terrorism capabilities.

Since the invasion, things have changed. Russia’s defense-industrial complex—especially military high-tech and AI research and development—may be affected by the international sanctions and cascading effects of Russia being cut off from semi-conductor and microprocessor imports.

Throughout 2021, the Russian government was pushing for the adoption of its AI civilian initiatives across the country, such as nationwide hackathons aimed at different age groups with the aim of making artificial intelligence familiar at home, work, and school. The government also pushed for the digital transformation of science and higher education, emphasizing the development of AI, big data, and the internet of things.

Russian academic AI R&D efforts drove predictive analytics; development of chat bots that process text and voice messages and resolve user issues without human intervention; and technologies for working with biometric data. Russia’s development of facial recognition technology continued apace, with key efforts implemented across Moscow and other large cities. AI as a key image recognition and data analytical tool was used in many medical projects and efforts dealing with large data sets.

Russian government officials noted their country’s efforts in promoting the ethics of artificial intelligence, and expressed confidence in Russia’s continued participation in this UN-sponsored work. The Russian Council for the Development of the Digital Economy has officially called for a ban on artificial intelligence algorithms that discriminate against people.

Russia’s Ministry of Economic Development was asked to "create a mechanism for assessing the humanitarian impact of the consequences of the introduction of such [AI] technologies, including in the provision of state and municipal services to citizens," and to prepare a "road map" for effective regulation, use, and implementation. According to the council, citizens should be able to appeal AI decisions digitally, and such a complaint should only be considered by a human. The council also proposed developing legal mechanisms to compensate for damage caused as a result of AI use.

In October, Russia’s leading information and communications companies adopted the National Code of Ethics in the Field of AI; the code was recommended for all participants in the AI market, including government, business, Russian and foreign developers. Among the basic principles in the code are a human-centered approach to the development of this technology and the safety of working with data.

AI workforce development was spelled out as a key requirement when the government officially unveiled the national AI roadmap in 2019. A 2021 government poll that tried to gauge the level of confidence in the government’s AI efforts showed that only about 64 percent of domestic AI specialists were satisfied with the working conditions in Russia.

The survey reflected the microcosm of AI research, development, testing, and evaluation in Russia—lots of government activity and different efforts that did not automatically translate into a productive ecosystem conducive for developing AI, some major efforts notwithstanding.

Among some of the reasons in 2021 that Russia was lagging behind in the development of artificial intelligence technologies were the personnel shortage and the weakness of the venture capital market. The civilian developer community also noted the low penetration of Russian products into foreign markets, dependence on imports, slow introduction of products into business and government bodies, and a weak connection between AI theory and practice.

Russia’s likely plans to concentrate on these areas in 2022 were revised or put on hold once Russia invaded Ukraine. The sudden pull-out of major IT and high-tech companies from Russia, coupled with a rapid brain drain of Russia’s IT workers, and the ever-expanding high-tech sanctions against the Russian state may hobble domestic AI research and development for years to come. While the Russian government is trying to prop up its AI and high-tech industry with subsidies, funding, and legislative support, the impact of the above-mentioned consequences may be too much for the still-growing and evolving Russian AI ecosystem. That does not mean AI research and development will stop—on the contrary, many 2021 trends, efforts, and inventions are being implemented into the Russian economy and society in 2022, and there are domestic high-tech companies and public-private partnerships which are trying to fill the void left by the departed global IT majors. But the effects of the invasion will be felt in the AI ecosystem for a long time, especially with so many IT workers leaving the country, either because of the massive impact on the high-tech economy, or because they disagree with the war, or both.

One of the most-felt sanctions aftereffects has been the severing of international cooperation on AI among Russian universities and research instructions, which earlier was enshrined as one of the most important drivers for domestic AI R&D, and reinforced by support from the Kremlin. For most high-tech institutions around the world, the impact of civilian destruction across Ukraine by the Russian military greatly outweighs the need to engage Russia on AI. At the same time, much of the Russian military AI R&D took place in a siloed environment—in many cases behind a classified firewall and without significant public-private cooperation—so it’s hard to estimate just how sanctions will affect Russian military AI efforts.

While many in Russia now look to China as a substitute for departed global commercial relationships and products, it’s not clear if Beijing could fully replace the software and hardware products and services that left Russian markets at this point.

Recent events may not stop Russian civilians and military experts from discussing how AI influences the conduct of war and peace—but the practical implementation of these deliberations may become increasingly more difficult for a country under global high-tech isolation.

### 2AC – No China AI Lead

#### China doesn’t lead in AI ­– reports use false metrics (i.e., patents, research publications) – insert this graph

Ghi et al. 21 (Trung Ghi; Abhishek Srivastava; Arthur D. Little; "The Global AI Arms Race – How Nations can Avoid being Left Behind", January 2021, PRISM, https://www.adlittle.com/sites/default/files/prism/Global%20AI%20article.pdf, DOA: 7-18-2022)//ATJ

There are several country rankings of AI strength across the world. Those that focus on metrics such as patents and research publications tend to list China first, followed by the US, with third place disputed between European and Asian countries including South Korea, Japan and India.

However, taking a broader approach using a composite AI-readiness index (from Oxford Insights) that factors in governance, skills and education, infrastructure and data, and government/public services reveals the top three countries to be Singapore, the UK and Germany. (See Figure 1.)

Chart

Description automatically generated

#### Still pertinent today – the US leads by a wide margin above China – insert this chart

O.I. 22 (Oxford Insights; "Government AI Readiness Index 2021", January 2022, Oxford Insights, https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/61ead0752e7529590e98d35f/1642778757117/Government\_AI\_Readiness\_21.pdf, DOA: 7-18-2022)//ATJ

Table

Description automatically generated

Figure 1: the US firmly leads the AI index, with China coming in at 15th.

#### Not unique — China is not overtaking the US.

Cooper and Kompella 22 — James Cooper, professor of law and director of International Legal Studies at California Western School of Law, research fellow at Singapore University of Social Sciences, J.D. from the University of Toronto (Canada), LL.M. from the University of Cambridge (U.K), and Kashyap Kompella, technology industry analyst and CEO of RPA2AI, a global artificial intelligence advisory firm, Masters in Business Laws from National Law School of India University (India), 2022 (“No, China is not winning the AI race,” *The Hill*, February 3rd, Available Online at <https://thehill.com/opinion/technology/592270-no-china-is-not-winning-the-ai-race/>, Accessed 07-19-2022)

The global competition between the United States and China continues apace. Technology is rightly seen as providing unique leverage to win this geopolitical race. The U.S. long has been the global technology powerhouse, but not surprisingly, we have heard much about the Chinese government’s ambition to dominate high-tech industries such as 5G telecommunications, autonomous vehicles, blockchain, and semiconductor chips.

In this light, as a horizontal technology that can be applied across all sectors, artificial intelligence (AI) has become a strategic priority and the Chinese focus on superiority in this field is touted as something about which the U.S. should be concerned. Some have gone so far as to conclude that the West has already lost the AI race.

Don’t believe the hype. To be sure, the availability of large amounts of data is at the heart of AI success. It is tempting to think that less-democratic regimes that amass huge amounts of data about their citizens and have scant regard for privacy can develop better AI systems using that data. However, all other things being equal, better and higher quality AI systems emerge from countries with strong data privacy and data protection regulations because AI systems must undergo greater scrutiny during their development and deployment. An example of this can be seen in the United States regarding fair lending practices and consumer protection from credit bureaus. Further, the market for AI is global, and such high-quality AI systems find buyers in other countries as well.

Around the globe, Big Tech’s rising power has resulted in calls for more oversight. In a drastic move that stunned the industry and analysts alike, the Chinese government recently rewrote the rulebook for the country’s technology industry. In effect, China is vacating entire swaths of digital and creative industries, arenas that serve as training grounds and talent factories for other industries. This more restrictive approach may not bode well for China’s AI industry in the long term. China may find itself constrained on the extent of automation and AI in its manufacturing sector — labor-intensive manufacturing remains China’s main strength, and a high degree of automation can result in job losses, labor unrest, and instability.

Meanwhile, there is bipartisan support for AI in the United States. Former President Trump proposed increasing funding for AI development through the National Science Foundation. The National AI Initiative Act of 2020 signaled a sense of urgency and suggested that several federal agencies create a national strategy on artificial intelligence. The Biden administration has formed the Artificial Intelligence Research Resource Task Force to develop a roadmap to foment AI research and spark innovation nationwide. There is draft legislation, at both the state and federal level, to promote responsible use of AI and prevent its misuse.

Strong objections to the use of facial recognition and other AI systems by law enforcement in the U.S., raised by civil liberties advocates, have led some local authorities, such as the City of San Francisco, to ban such systems. To use a Silicon Valley phrase, these debates are “not a bug, but a feature.” They shine a light on the limitations of AI systems and help to set the “rules of the road” for proper use of AI. This will establish the U.S. as a global leader in AI regulation, once lawmakers and regulators do their work. China, meanwhile, has faced strong global criticism for using facial recognition software to monitor and surveil Uyghurs in its Xinjiang region. China has outlined a set of AI ethics principles, but the jury is still out on enforcement and how they function in practice.

The increasing number of AI research papers and patents by Chinese researchers is often cited as proof that China has caught up with the United States in this field. The increased focus is good for the Chinese AI ecosystem, and it will help them solve China-specific problems. But dominance in this emerging strategic industry is not guaranteed. The U.S. has several strategic advantages, including: the strengths of its higher education and research institutes, which attract the best STEM talent from across the world; the largest venture capital ecosystem; and the largest number of technology unicorns (start-ups with private valuations greater than $1 billion).

China is not overtaking the U.S. in artificial intelligence. The current evidence and trajectory paint a clear picture: The conditions for AI to flourish, such as incentives to experiment, freedom to pursue opportunities without restrictions, and the coming guardrails to prevent misuse, favor U.S. leadership. This is still the United States’s game to lose — though maybe both countries could win through collaboration. To solve planet-scale problems such as climate change, we are going to need AI solutions from both competitors.

#### The US leads China in defense AI — increased spending.

Greene 21 — Tristan Greene, editor and technology reporter at TNW, 2021 (“Here’s why the US continues to beat China in the AI race,” *TNW*, June 2nd, Available Online at <https://thenextweb.com/news/heres-why-the-us-continues-to-beat-china-in-the-ai-race>, Accessed 07-18-2022)

The global AI race was supposed to be a sprint. Back in 2017 when driverless cars and domestic robots were thought to be just around the corner, the promise of deep learning made it seem like we were mere months away from living in an AI-powered utopia.

As it turns out, the global AI race is more of a marathon. And the US has a huge lead that’ll be difficult to overcome for any country, but especially China.

The setup

It was easy to believe China would pull ahead a few years ago. US big tech companies such as Microsoft and Apple had always co-existed with eastern outfits. But, once deep learning exploded in 2014, many experts believed China would use its government influence to direct the flow of research in ways the EU and US’ respective leaders simply couldn’t.

And, for a while, it looked like that was going to be enough to propel the PRC to the top of the global AI leaderboards.

In the west, a lion’s share of AI research ends up patented by businesses who keep their algorithms in a walled-garden. But in the east things are different.

Per an article in the Harvard Business Review:

Unlike in Western developed economies where companies are the primary holders of AI patents, in China, the majority of AI patents are filed by universities and research institutes, most of which are government owned or sponsored.

China’s big problem

The biggest problem China has when it comes to AI is a lack of innovation. Consumer demand is at an all-time high for deep learning technologies in China, but this social trend isn’t translating into breakthroughs.

In essence, China is still playing catch up. The Chinese government may be pouring more money into research and producing more of it, but US tech companies are raising and spending more on research outside of academia.

The US government still spends more on defense AI than China, and US businesses spend more money on cutting-edge research than Chinese companies do.

Simply put, the biggest technology companies in the US can afford to invest in breakthrough research even when such research leads nowhere. The profit margins are much leaner at most Chinese firms so the incentive is typically on producing a profit.

Unfortunately for China, much of its AI position is rooted in developing Chinese-language versions of language recognition software and creating surveillance technology – neither of those are very marketable outside of places where Chinese is spoken or where privacy laws exist.

What it all means

Deep learning might not be the best path forward for artificial intelligence technologies. This is great news for big tech companies in the US. But it’s bad news for China.

In the US, where most of the AI breakthroughs tend to come from big tech companies with large enough coffers to afford supercomputers and high enough salaries to lure away academia’s brightest, scientists won’t miss a beat if we transition away from deep learning

But China’s heavily-saturated market likely won’t extend beyond its own bubble, much less the deep learning bubble that could pop and leave AI-only companies behind. There’s a reason why there’s only one Chinese firm among the top five richest technology companies in the world.

It’ll be tough for academia in China to keep up with big tech in the US no matter how much data it can generate or acquire.

We’re more likely to see these kinds of catch-up cycles end in cooling-off cycles when heavy government investment doesn’t pay off. China could be headed for an AI winter.

### 2AC – Regulation good

#### AI arms race leads to a race to the bottom on AI safety, which undermines international stability

Scharre 21 (Paul Scharre, holds a **Ph.D.** in War Studies from King’s College London and an M.A. in Political Economy and Public Policy and a B.S. in Physics, cum laude, from Washington University in St. Louis, Vice President and Director of Studies at the Center for a New American Security, previously worked in the Office of the Secretary of Defense; "Debunking the AI Arms Race Theory", Texas National Security Review, vol. 4, iss. 3, summer 2021, 121-132, DOI: 10.26153/tsw/13985, DOA: 4-14-2022)//ATJ

Race to the Bottom on Safety A related risk of a “racing” dynamic among competitors could come from an acceleration, not of the pace of operations on the battlefield, but of the process of fielding new AI systems. AI systems today have a host of safety and security problems that can make them brittle, unreliable, and insecure.29 Because machine learning in particular can create new ways in which systems can fail, militaries face novel challenges in adopting AI systems.30 Militaries will have to adopt new methods to test, evaluate, verify, and validate AI systems (also known as TEVV).31 Such concerns related to autonomy are well known in the U.S. defense community,32 although at present they have not been solved to a satisfactory degree. Machine learning introduces additional challenges with regard to testing, evaluation, verification, and validation. A rush to field AI systems before they are fully tested could result in a “race to the bottom” on safety, with militaries fielding accident-prone AI systems. There are strong bureaucratic and institutional imperatives for militaries to field systems that are robust and secure. Indeed, designing systems to military specification standards often means making them more robust for a wider range of environmental conditions and shocks than comparable commercial systems, even at the expense of other aspects of performance, such as size, weight, or usability. AI presents novel challenges, however, in achieving the robustness needed for operating in the complex, hazardous, and adversarial environments that often characterize military operations. Certain AI methods today, such as deep learning, remain relatively immature with significant reliability challenges. A 2017 Department of Defense report by the JASON scientific advisory group explained that deep neural networks are immature as regards the “illities”, including reliability, maintainability, accountability, validation and verification, debug-ability, evolvability, fragility, attackability, and so forth. … Further, it is not clear that the existing AI paradigm is immediately amenable to any sort of software engineering validation and verification. This is a serious issue, and is a potential roadblock to DoD’s [Department of Defense’s] use of these modern AI systems, especially when considering the liability and accountability of using AI in lethal systems.33 The Defense Department’s 2018 AI strategy calls for building AI systems that are “resilient, robust, reliable, and secure.”34 Yet, the current state of technology makes achieving this goal particularly difficult for AI systems that incorporate deep learning, a subfield of AI that has seen significant growth and attention in recent years. While there is active research underway to improve AI safety and security, militaries will have to adapt to the technology as it currently is, at least for the time being. An ideal process would be for militaries to engage in experimentation, prototyping, and concept development, but also to subject AI systems to rigorous TEVV under realistic operational conditions before deployment. Taking shortcuts on testing and evaluation and fielding a system before it is fully tested could lead to accidents, which, in some settings, could undermine international stability. In evaluating new technologies, militaries may be relatively accepting of the risk of accidents, which may lead them to tolerate the deployment of systems that have reliability concerns. In building and fielding new capabilities, militaries have to weigh the possibility of an accident occurring against other concerns, such as forgoing valuable military capabilities. The military operational environment is fraught with risk, in both training and real-world operations. Military institutions balance managing this risk with other factors, such as the need for training, developing new capabilities, or accomplishing the mission. Military institutions view casualties from training accidents or testing new capabilities as a tragic but unavoidable part of the business of preparing for war. Militaries expect high performance from their forces, often while they are performing dangerous tasks, but militaries neither demand nor expect accident-free operations in most settings.35 From 2006 to 2020, over 5,000 U.S. servicemembers were killed in non-war related accidents, the majority of which occurred within the United States. Accidents overall accounted for nearly 32 percent of U.S. servicemember deaths during this period, and even accounted for a significant portion of servicemember deaths in Iraq (19 percent) and Afghanistan (16 percent).36 These accident rates are not unusual for the U.S. armed forces. This is business as usual. Accidents draw the attention of senior military and civilian officials when a spate of accidents occur in a short amount of time — such as a series of aircraft crashes,37 ship collisions,38 or training accidents.39 Yet, as one report on naval accidents from 1945 to 1988 notes, “peacetime naval accidents are a fact of life.”40 The same is true of military air and ground operations. Other nations’ militaries may do an even poorer job of managing risk when it comes to accidents than the U.S. military. For example, the Soviet/Russian submarine community has a much higher accident rate than the U.S. submarine community.41 New technologies in particular present an increased risk of accidents, yet militaries may press ahead out of a desire to develop and field what they perceive to be a valuable capability. For example, the V-22 Osprey tiltrotor aircraft suffered four crashes during development, killing 30 U.S. servicemembers in total, yet the Defense Department continued development.42 The V-22 program manager cited a rush to develop the technology as a factor in the accidents, stating, “Meeting a funding deadline was more important than making sure we’d done all the testing we could.”43 Taking shortcuts on testing in particular appears to have been a factor in at least one fatal crash. According to a Government Accountability Office investigation of the V-22 program, “schedule pressures” led the program to conduct only 33 of 103 planned tests of an aerodynamic phenomenon called a “vortex ring state,”44 a phenomenon that later caused an April 2000 crash that killed 19 servicemembers.45 Absent competitive dynamics, militaries may be able to manage the challenges of fielding safe AI systems to a more-or-less satisfactory degree, albeit with some risk of an accident occurring. However, out of a desire to field AI capabilities ahead of competitors, militaries may be more willing to accept risk than they might otherwise be and to field systems that are prone to mishaps.46 Similar competitive dynamics may have played a role in accidents with self-driving cars and commercial airline autopilot technology, as companies rushed to beat others to market.47 These dynamics, while not an arms race, could lead militaries to engage in a “race to the bottom” on safety. This risk could become particularly acute in wartime. Managing these risks is challenging because assessing them can be difficult, especially when it comes to new technologies. Accident rates may be well-known for mature technologies, but they are unknown for technologies still in development. In the case of the V-22 Osprey development, for example, it is not as though the Defense Department knew that developing it would lead to multiple crashes and 30 fatalities but decided that achieving the capability was worth the cost. Engineers, testers, and program managers are flying in the dark when it comes to new technologies — that is, after all, the point of testing new systems. The concern is not only that organizations may take measured risks to field new capabilities, but also that institutional and bureaucratic imperatives may lead organizations to distort their own perceptions of risk, further contributing to accidents. This sociological phenomenon has been cited as a cause in the 1986 Space Shuttle Challenger explosion, for example.48

#### Proactive AI regulations protect consumers and drive innovation – squo ex-post measures cede AI to industry, decimate public support for emerging tech, and crushes innovation – facial recognition proves

* businesses want proactive regs on AI because the public doesn’t trust the companies because of the lack of regs
* Empirics prove – credit bureaus
* Facial recognition is hated and the gov is thinking about banning it now only because the companies making it in the beginning had no regulatory framework to operate in
* Reed says ex-post regs coming now

MacCarthy 20 (Mark MacCarthy, holds a **PhD** in philosophy from Indiana University, MA in Economics from Notre Dame, and a BA from Fordham University, Senior Fellow in Governance Studies at the Center for Technology Innovation at Brookings, adjunct professor at Georgetown University; "AI needs more regulation, not less", 3-9-2020, Brookings, https://www.brookings.edu/research/ai-needs-more-regulation-not-less/, DOA: 4-19-2022)//ATJ

In the early 1970s, the fledgling credit card industry routinely and shortsightedly held cardholders liable for fraudulent transactions, even if their cards had been lost or stolen. In response, Congress passed the 1974 Fair Credit Billing Act to limit cardholder liability. This protection increased public trust in the new payment system and spurred growth and innovation. Because they could no longer just pass fraud losses on to cardholders, payment networks devised one of the first commercial applications of neural networks to detect out-of-pattern card usage and reduce their fraud losses.

Smart regulation, like the above example, that gets out in front of emerging technology can protect consumers and drive innovation. In the last several decades, however, policymakers have forgotten this beneficial side effect of regulation, preferring to give industry players free rein to deploy emerging technologies as they see fit.

The grim results of that laissez-faire philosophy are all around us today in the form of a still-growing backlash against tech companies. The public darkly suspects that these companies are interested primarily in promoting their own dominance and not dealing with deleterious ramifications. As a result, policymakers at the state and local levels are beginning to consider technology bans on AI applications such as facial recognition. The path forward is not deregulation or prohibitions, but smart, proactive regulation that establishes a framework for both public protection and innovation growth.

THE WHITE HOUSE AI GUIDANCE HAS GOOD AND BAD NEWS

The White House recently released guidance for the regulation of AI applications, establishing a framework that future rulemaking or legislation can build upon. The good news is that the administration is committed to a sectoral approach. Since AI is just a collection of statistical techniques that can be used throughout the economy, it makes no sense to have a federal AI commission to enforce one-size-fits-all rules. The White House report wisely encourages sectoral regulators to formulate rules for the AI applications within their jurisdiction. In a recent op-ed, former White House official R. David Edelman makes a similar point about not regulating AI as if it were a single thing.

Unfortunately, the report also perpetuates the out-of-date, hands-off approach. It encourages regulators to think of their activity as one which holds innovation back. Regulators are told that they must “avoid regulatory or non-regulatory actions that needlessly hamper AI innovation and growth.” Regulation is seen as a cost, a hindrance, a delay, or a barrier which must be reluctantly accepted as a last resort only if absolutely necessary.

The idea that measures such as transparency, accountability, and fairness might promote AI growth and innovation is foreign to this framework. But in today’s world, the real task for AI regulators is to create a rules structure that both protects the public and promotes industry innovation—not to trade off one against the other.

NEW LEGISLATION IS NEEDED

Many AI applications cry out for before-the-fact legislation, not just application of existing rules. When Illinois passed its Artificial Intelligence Video Interview Act last year, some commentators thought it was overreacting to science fiction speculations. But the law, which established requirements for notice, consent, and explanations when employers use AI to analyze videos of job applicants, is already behind the curve. A host of companies, such as HireVue, are already using AI video analysis to score job applicants.

Employment screening is riddled with insular, clubby judgments that perpetuate a uniform workplace rather than finding talented or creative types. Companies are right to look for fairer and more accurate algorithmic screening techniques.

Still, except for the new Illinois state law, AI hiring algorithms are devoid of consumer protections. Vendors provide neither validity tests to show that these techniques detect traits relevant to job performance, nor disparate impact assessments to reveal potential discriminatory effects. Employers can turn job applicants down on the basis of these screenings without ever having to explain the basis for these adverse actions.

Policymakers used to know what to do when faced with such a promising emerging technology: They would throw a regulatory net around it to provide for growth and consumer protection. When computerized credit bureaus began to spread in the late 1960s, Congress got ahead of the emerging technology and put in place the 1970 Fair Credit Reporting Act, which established consumer-protection rights and shielded the bureaus from defamation suits. The industry expanded rapidly, but consumers remained safe. Passing a national law now to regulate AI-driven employment tests might similarly provide win-win benefits to AI firms, employers, and job applicants.

THE BACKLASH AGAINST FACIAL RECOGNITION

The troublesome experience with facial recognition shows what can happen when companies rush AI applications to market without a regulatory safety net. Tests at the National Institute for Standards and Technology have demonstrated that the technology on the market now has discriminatory effects. Nevertheless, with almost no public scrutiny, local law enforcement agencies have been using the technology. The latest such story concerns widespread law enforcement access to Clearview’s trove of (illegally obtained!) photos in pursuit of lawbreakers—apparently oblivious of the civil liberties risks involved.

As a result of this rush to market, facial recognition technology is in trouble both here and abroad. Privacy and civil liberties groups have urged a suspension of federal government use of facial recognition systems, pending further review. Scholars have called for a ban, and some states and cities have already implemented partial bans.

A ban might be throwing out the baby with the bathwater. But, if the only alternative is after-the-fact regulation to correct whatever mistakes turn up, a ban or moratorium might make sense. In a welcome, if belated, development, key industry participants have come out in favor of a proactive regulatory framework.

PROACTIVE REGULATION IS NEEDED

Machine learning is the “most important general-purpose technology of our era.” The calls for modest regulation that lets industry take the lead are part of a failed regulatory philosophy, one that saw its natural experiment over the past several decades come up lacking. AI is too important and too promising to be governed in a hands-off fashion, waiting for problems to develop and then trying to fix them after the fact.

It is time to return to the way we used to regulate emerging technologies. Industry leaders like Google CEO Sundar Pichai have recently recognized the advantages of proactive, sector-by-sector regulation of AI applications. Thoughtful, far-sighted policymakers, like those in the 1970s who regulated and jump-started new payment systems and credit bureaus, need to set the rules and priorities for this vital technology in a way that protects consumers and provides for innovation and growth.

#### Absent the plan, companies have free reign in AI – that leads to demoware proliferation that produces useless applications of AI (i.e., deepfakes/image generation vs military/defense uses)

* It’s not a question of “who implements AI first” if American AI is bad

Marcus 22 (Gary Marcus, holds a **PhD** from MIT, founded Geometric Intelligence, a machine learning company purchased by Uber two years later in 2016; "Artificial General Intelligence Is Not as Imminent as You Might Think", 6-6-2022, Scientific American, https://www.scientificamerican.com/article/artificial-general-intelligence-is-not-as-imminent-as-you-might-think1/, DOA: 7-18-2022)//ATJ

To the average person, it must seem as if the field of artificial intelligence is making immense progress. According to the press releases, and some of the more gushing media accounts, OpenAI’s DALL-E 2 can seemingly create spectacular images from any text; another OpenAI system called GPT-3 can talk about just about anything; and a system called Gato that was released in May by DeepMind, a division of Alphabet, seemingly worked well on every task the company could throw at it. One of DeepMind’s high-level executives even went so far as to brag that in the quest for artificial general intelligence (AGI), AI that has the flexibility and resourcefulness of human intelligence, “The Game is Over!” And Elon Musk said recently that he would be surprised if we didn’t have artificial general intelligence by 2029.

Don’t be fooled. Machines may someday be as smart as people, and perhaps even smarter, but the game is far from over. There is still an immense amount of work to be done in making machines that truly can comprehend and reason about the world around them. What we really need right now is less posturing and more basic research.

To be sure, there are indeed some ways in which AI truly is making progress—synthetic images look more and more realistic, and speech recognition can often work in noisy environments—but we are still light-years away from general purpose, human-level AI that can understand the true meanings of articles and videos, or deal with unexpected obstacles and interruptions. We are still stuck on precisely the same challenges that academic scientists (including myself) having been pointing out for years: getting AI to be reliable and getting it to cope with unusual circumstances.

Take the recently celebrated Gato, an alleged jack of all trades, and how it captioned an image of a pitcher hurling a baseball. The system returned three different answers: “A baseball player pitching a ball on top of a baseball field,” “A man throwing a baseball at a pitcher on a baseball field” and “A baseball player at bat and a catcher in the dirt during a baseball game.” The first response is correct, but the other two answers include hallucinations of other players that aren’t seen in the image. The system has no idea what is actually in the picture as opposed to what is typical of roughly similar images. Any baseball fan would recognize that this was the pitcher who has just thrown the ball, and not the other way around—and although we expect that a catcher and a batter are nearby, they obviously do not appear in the image.

Likewise, DALL-E 2 couldn’t tell the difference between a red cube on top of a blue cube and a blue cube on top of a red cube. A newer version of the system, released in May, couldn’t tell the difference between an astronaut riding a horse and a horse riding an astronaut.

When systems like DALL-E make mistakes, the result is amusing, but other AI errors create serious problems. To take another example, a Tesla on autopilot recently drove directly towards a human worker carrying a stop sign in the middle of the road, only slowing down when the human driver intervened. The system could recognize humans on their own (as they appeared in the training data) and stop signs in their usual locations (again as they appeared in the trained images), but failed to slow down when confronted by the unusual combination of the two, which put the stop sign in a new and unusual position.

Unfortunately, the fact that these systems still fail to be reliable and struggle with novel circumstances is usually buried in the fine print. Gato worked well on all the tasks DeepMind reported, but rarely as well as other contemporary systems. GPT-3 often creates fluent prose but still struggles with basic arithmetic, and it has so little grip on reality it is prone to creating sentences like “Some experts believe that the act of eating a sock helps the brain to come out of its altered state as a result of meditation,” when no expert ever said any such thing. A cursory look at recent headlines wouldn’t tell you about any of these problems.

The subplot here is that the biggest teams of researchers in AI are no longer to be found in the academy, where peer review used to be coin of the realm, but in corporations. And corporations, unlike universities, have no incentive to play fair. Rather than submitting their splashy new papers to academic scrutiny, they have taken to publication by press release, seducing journalists and sidestepping the peer review process. We know only what the companies want us to know.

In the software industry, there’s a word for this kind of strategy: demoware, software designed to look good for a demo, but not necessarily good enough for the real world. Often, demoware becomes vaporware, announced for shock and awe in order to discourage competitors, but never released at all.

Chickens do tend to come home to roost though, eventually. Cold fusion may have sounded great, but you still can’t get it at the mall. The cost in AI is likely to be a winter of deflated expectations. Too many products, like driverless cars, automated radiologists and all-purpose digital agents, have been demoed, publicized—and never delivered. For now, the investment dollars keep coming in on promise (who wouldn’t like a self-driving car?), but if the core problems of reliability and coping with outliers are not resolved, investment will dry up. We will be left with powerful deepfakes, enormous networks that emit immense amounts of carbon, and solid advances in machine translation, speech recognition and object recognition, but too little else to show for all the premature hype.

Deep learning has advanced the ability of machines to recognize patterns in data, but it has three major flaws. The patterns that it learns are, ironically, superficial, not conceptual; the results it creates are difficult to interpret; and the results are difficult to use in the context of other processes, such as memory and reasoning. As Harvard computer scientist Les Valiant noted, “The central challenge [going forward] is to unify the formulation of … learning and reasoning.” You can’t deal with a person carrying a stop sign if you don’t really understand what a stop sign even is.

For now, we are trapped in a “local minimum” in which companies pursue benchmarks, rather than foundational ideas, eking out small improvements with the technologies they already have rather than pausing to ask more fundamental questions. Instead of pursuing flashy straight-to-the-media demos, we need more people asking basic questions about how to build systems that can learn and reason at the same time. Instead, current engineering practice is far ahead of scientific skills, working harder to use tools that aren’t fully understood than to develop new tools and a clearer theoretical ground. This is why basic research remains crucial.

#### AI regulation is key to development – developers only get on board if they can ensure that AI won’t become a threat

Stepken, 21

[Axel, chairman of the board of management, October 27, 2021, “AI regulation – why it will boost innovation”, LinkedIn, <https://www.linkedin.com/pulse/ai-regulation-why-boost-innovation-axel-stepken>, accessed 7-18-2022, BB]

Most people tend to flinch automatically at the mention of regulation. However, regulatory agreements and normative requirements are what enable us to benefit from today’s global trade networks. I firmly believe that an assured regulatory framework enhances, rather than impairs, innovation and economic opportunities.

When it comes to innovative technologies, regulation frequently lags behind market development. This is nothing new. Regulatory oversight, particularly for disruptive technologies such as AI applications, is expected to provide a reliable framework for both users and companies, while keeping efforts and expenses at a reasonable level. But at the same time, it is expected to support the dynamic development of these technologies and steer them safely towards the greater and common good.

Complex fields of regulation

The fundamental principles of good AI regulation include legal compliance, interoperability, IT security and data protection, but also the ethical principles of the European Union. Technology- and process-related requirements can be drawn up based on previous regulations and easily operationalised. A more difficult aspect in the case of AI applications involves ethical considerations and how to weigh them against technological aspects. In addition to the above, AI applications including their tasks and results may have enormous implications for the realities of people’s lives. This certainly does not make regulatory oversight any easier.

What is more important, the performance of an AI application, which I can improve by feeding it a significantly greater quantity of more detailed data, or protection of a patient’s personal data?

This is one of the questions that regularly comes up for AI applications in the medical field.

EU draft legislation: new dimension of risk assessment

In April 2021, the European Parliament took a first significant step in this direction by publishing the world’s first draft legislation for categorising AI systems in risk classes. The proposal for a regulation provides for four AI risk classes and is aimed at building an “ecosystem of trust” towards AI applications. A new and important aspect is that the proposal looks not only at the potential risks, but also at the options of individuals affected by AI decisions – in other words, how they can understand, doubt or even, if necessary, reverse these decisions. This is a completely new dimension of risk assessment and goes far beyond risk management as practised today.

Regulatory oversight welcome

These efforts cannot come too soon. International competition in the development and application of AI systems is progressing rapidly, with stakeholders asking more and more often which of the many possibilities of AI systems can be reconciled with European values. The need for information and regulation in this area is demonstrated by the increasing number of companies publishing codes of AI ethics, designed to provide guidance for the companies’ actions and inspire consumer trust. Various surveys among consumers and companies alike show a demand for regulatory oversight and certification of AI applications One examples are the surveys (in German) Unternehmer-Studie 2020 or Verbraucher-Studie 2021 conducted by TÜV-Verband among companies or consumers respectively.

Regulation brings benefits

While many of us associate the concept of regulatory oversight with negative connotations, it has tangible benefits when implemented in a moderate and practical manner.

“AI quality made in Germany” or “Made in the EU” enables companies and their AI systems to stand out from their market companions from other countries.

Regulation establishes transparency and trust, enabling faster market penetration and thus growth in sales revenue.

Conclusive regulation provides a framework for the development of AI systems which may act as a catalyst for high quality.

It will provide companies with a stable, secure and certain legal framework for their business operations.

Regulation creates transparency and trust

Regulated and verified AI applications create transparency and trust for consumers and companies alike, which in turn enable faster market penetration.

AI will only be able to unfold its full potential if people are reassured that AI applications will not disrupt our societal and economic principles. Given this, I am certain that clear and reliable regulatory oversight of AI applications with a healthy sense of perspective will generate competitive edge for Germany and Europe.

#### Regulated AI is key to hamper innovations and get developers on board

Maliha, 21

[George, MD, is a second-year internal medicine resident at the University of Pennsylvania Health System, 7-13-2021, “To Spur Growth in AI, We Need a New Approach to Legal Liability”, Harvard Business Review, <https://hbr.org/2021/07/to-spur-growth-in-ai-we-need-a-new-approach-to-legal-liability>, accessed 7-18-2022, BB]

Artificial intelligence (AI) is sweeping through industries ranging from cybersecurity to environmental protection — and the Covid-19 pandemic has only accelerated this trend. AI may improve the lives of millions, but it also will inevitably cause accidents that injure people or parties — indeed, it already has through incidents like autonomous vehicle crashes. An outdated liability system in the United States and other countries, however, is unable to manage these risks, which is a problem because those risks can impede AI innovations and adoption. Therefore, it is crucial that we reform the liability system. Doing so will help speed AI innovations and adoption.

Misallocated liability can hamper innovation in several ways. All else being equal, an AI designer looking to implement a system in one of two industries will avoid the industry that places more liability on the designer. Similarly, the end users of an AI system will resist adoption if an AI algorithm carries further liability risk without some compensation. Liability reforms are needed to address these issues. Many of the changes we advocate involve rebalancing liability among the players — from end users (physicians, drivers, and other consumers of AI) to more upstream actors (e.g., designers, manufacturers).

#### All their link evidence assumes reactionary regulation, not liability regulations

Maliha, 21

[George, MD, is a second-year internal medicine resident at the University of Pennsylvania Health System, 7-13-2021, “To Spur Growth in AI, We Need a New Approach to Legal Liability”, Harvard Business Review, <https://hbr.org/2021/07/to-spur-growth-in-ai-we-need-a-new-approach-to-legal-liability>, accessed 7-18-2022, BB]

Granted, a regulatory scheme that attempts to specify an AI system completely will almost certainly hamper innovation. But those costs may be acceptable in particular areas such as drug development, where comprehensive Food and Drug Administration regulatory schemes can replace liability completely.

Given the tremendous innovation engendered by AI, it is often easy to ignore liability concerns until the offering makes it to market. Policymakers, designers, and end users of AI should develop a balanced liability system to facilitate AI — rather than merely react to it. Building this 21st century liability system will ensure that 21st century AI will flourish.

### 2AC – R&D turn

#### Non-unique and link turn – DoD is losing the tech race now – investing more in R&D is key to combine the private and military sectors to maintain their competitive edge

Hoffman, 20

[Daniel, retired clandestine services officer and former chief of station with the Central Intelligence Agency. His combined 30 years of government service included high-level overseas and domestic positions, 7-13-2020, “The US cannot compete with China if our military doesn’t invest in R&D”, The Hill, <https://thehill.com/opinion/national-security/506991-the-us-cannot-compete-with-china-if-our-military-doesnt-invest-in/>, accessed 7-18-2022, BB]

The Department of Defense (DOD) last month declared that 20 Chinese companies, including telecommunications firm Huawei and video surveillance company Hikvision, are a threat to U.S. national security because of their relationship with the Chinese military. DOD emphasized that Chinese president Xi Jinping’s military-civilian fusion strategy of exploiting high-technology is the blueprint for “China’s global ‘return’ to military preeminence.”

China is relentlessly harnessing artificial intelligence, neuroscience and quantum communication to support military research and development and ubiquitous spying on its citizens and adversaries. The Trump administration has taken steps to strengthen our defense against China, but the U.S. will not outcompete China without dominating this century’s revolution in technology.

China’s ruthless communist autocracy imposes its will on China’s businesses through dictatorial fiat. The U.S. is poised to win the competition to develop and deploy high-technology under the power of free markets and innovative defense acquisition policies. The key to ensuring American success is for DOD and private industry to turbo-boost their collaboration.

U.S. private industry now spends more on research and development (R&D) than the U.S. military, which, according to the most recently released budget, calls for increasing research, development, testing and evaluation of spending by 8.7 percent to $104 billion. DOD is less influential today as a purchaser of high-technology than in the past. Defense dominates fewer U.S. industries. In 1965, DOD accounted for over 75 percent of all U.S. semiconductor purchases. By 2012, all governments worldwide represented less than 2 percent of the semiconductor market.

In order to excel in the high-technology domain, DOD must attract companies to participate in the defense marketplace or risk losing its military advantage. DOD needs to incentivize private industry to invest its own resources into military-relevant R&D. Private industry, in turn, will benefit from access to DOD capital, expertise and facilities.

When encountering challenges working with DOD, companies naturally diversify their revenue streams. Some companies choose not to compete for defense contracts because of excessive and constantly changing regulations, increased costs, auditing requirements, and instability of funding caused by sequestration, continuing resolutions and lapses in appropriations.

The COVID-19 pandemic has highlighted the importance of maintaining a domestic manufacturing base and being able to speed up the acquisition process, both of which are critical to the drive for technological superiority. The U.S. must strengthen supply chains to ensure fast, reliable access to critical parts, especially in the event of a national emergency. Even the most technologically advanced capabilities will prove ineffective if we do not have the domestic manufacturing capabilities to manufacture, operate and maintain these systems.