AI Insight Forum - AI, Risk, Alignment, & Guarding Against Doomsday Scenarios
December 6, 2023
Written Statement of Martin Casado

The Greatest Technological Risks in the AI Era

The Threat of AI Doomerism

Over the last year, media headlines have been dominated by a loud chorus of individuals who claim that AI will lead to the end of humanity. This message is often offered with minimal or no data to substantiate their claims. The danger here lies not just in the potential overestimation of AI's capabilities, but also in the way these alarmist viewpoints can distort public perception and policy-making. Without evidence-based discourse, these doomsday predictions risk inciting unnecessary panic, leading to misguided regulations that could stifle innovation and hinder the beneficial applications of AI. Additionally, the focus on unsubstantiated fears may divert attention and resources away from addressing real and immediate challenges posed by AI, such as cybersecurity threats and protection of consumer data. It's critical that discussions and decisions about AI are grounded in factual, data-driven analysis rather than speculative fears. This will ensure that its development is aligned with the public's best interests.

Prohibition of Open Source AI

Since the advent of the internet, open source technology has played a pivotal role in fostering innovation, encouraging competition, and democratizing access to technology. Think of open source not just as code, but as a practice where software's DNA is laid out for the world to see, tweak, and share. It's this very ethos that has rallied a dynamic global tribe of thinkers, builders, and visionaries, all converging, iterating, and crafting the digital wonders we witness today. Open source technology is the reason the internet has succeeded far beyond our

imagination and we must protect it and encourage it in the AI era. Prohibiting or inhibiting open source AI will have grave consequences for society in several ways:

1. **Decreased Safety & Security** - At first glance, laying your code bare for all to see might seem counterintuitive to security. But it's precisely this open scrutiny that makes it a bastion of safety, and makes overbearing regulations unnecessary. Think of open source as the software world's version of peer review. Thousands, if not millions, of eyes pore over each line, searching for flaws, vulnerabilities, and potential exploits. It's this vast, global community that ensures any gaps in the defense are rapidly detected and fortified. In proprietary/closed systems, vulnerabilities might remain undiscovered for extended periods of time, putting consumers in extended periods of serious risk. Conversely, in the open source sunlight, they're swiftly spotlighted and addressed, crafting a digital landscape that's not only innovative but also inherently secure. While proponents of AI safety guidelines often point to the “blackbox” nature of AI models – i.e. that the reasoning behind their conclusions are not “explainable” – recent advances by the AI industry have now solved this problem, ensuring the integrity of open source code models.

2. **Regulatory Capture by Large Tech Corporations** - Overburdensome and misguided policies that allow the future of AI to be dictated by a few large corporations is among the most dangerous risks for the American people. This concentration of power can lead to decisions that prioritize corporate power, malicious social engineering to influence society, corporate or state revisions of history, and significant negative impacts on consumers. In contrast, open source AI serves as a powerful democratizing force. It ensures that the development and deployment of AI models involve a global community, bringing together a wide range of insights and ethical frameworks. With open source AI, we guarantee that the models used by the American people remain transparent, accountable, and adaptable by a multitude of voices, rather than being controlled by an exclusive elite. By

advocating for open source, we aren't just preserving code; we are securing a future where technology is a collective endeavor, reflective of the wisdom of humanity as a whole. Open source AI ensures that the AI era is marked by inclusivity and fairness, benefiting everyone.

3. **Restricting Academic Research** - Prohibiting or inhibiting open source AI would have detrimental consequences for academic research. Embracing open source liberates academia from the constraints imposed by proprietary tools, granting scholars the freedom to analyze, adapt, and enhance software without hindrances. It provides researchers with an expansive, license-free laboratory for exploration. Additionally, emerging AI innovations, such as LLMs, demand substantial financial and computational resources for effective utilization. Without accessible open source models, academic researchers, who often lack the financial and computational means required to create LLMs and other resource-intensive models, would find themselves excluded from contributing to the progress of this technology.

The Risk of Strangling AI to American National Security

It's not hyperbole to assert that America's AI leadership is crucial, especially when viewed through the prism of our dynamic with China. As Beijing aggressively integrates AI into its military strategies, surveillance apparatus, and economic master plans, America's place as a technological beacon isn't just about Silicon Valley startups—it's about safeguarding our national security. If we let our AI momentum wane, we risk being outpaced in areas like cybersecurity, intelligence operations, and modern warfare, handing strategic advantages to a formidable competitor. We lose on hard power.

But this also has significant economic and ideological ramifications. AI is a foundational computing technology that will continue to transform all sectors of the economy and drive the creation of new industries and jobs in ways we cannot yet anticipate. The ability of the U.S. economy to disproportionately benefit from AI – as with microchips and the internet – depends critically on whether AI is developed by companies within the U.S. Additionally, America's AI endeavors are intertwined with our democratic fabric, emphasizing individual freedoms, privacy, and an ethos of open innovation. In stark contrast, China's AI trajectory is heavily influenced by state control and surveillance priorities. If America stands at the forefront of AI, we can drive global norms that prioritize these democratic values in the emerging AI-driven world. Overbearing regulations risk ceding our leadership to China reshaping the global tech ecosystem in a way that's less transparent and more authoritarian, with ripple effects that could redefine the internet's DNA for the next 20 years. We also lose on soft power.

While the U.S. currently holds a distinct edge over China—thanks in no small part to our homegrown technology sector pioneering groundbreaking LLMs in AI—this advantage is *not* guaranteed. These monumental advancements, borne out of an ecosystem that championed unbridled AI R&D, now face an ironic twist. Just as we're unlocking AI's immense potential, there's a rising chorus suggesting we pump the brakes. Calls for industry restraint and AI licensing will pave the way for regulatory frameworks that incumbent behemoths will exploit, sidelining the very startups that inject fresh innovation into our tech landscape. As we navigate the rise of AI, we must ensure that the spirit of innovation that got us here isn't smothered by the very mechanisms intended to safeguard it.