The AI Revolution's Outsized Impact on Deterrence

By

Rob Kittinger, Ph.D.

The impact of artificial intelligence (AI) on national security at large and deterrence specifically cannot be overstated. The business leaders competing in the field of AI, like Sam Altman, Elon Musk, and Mark Zuckerberg comprehend this truth, although they probably know little about the impact on deterrence theory. Superintelligence is just around the corner, and how well it integrates with deterrence policy is not yet fully known.

As of today, ChatGPT-5 Pro is said to have an IQ of 148, as tested officially by Mensa Norway. It is now significantly smarter than most adult humans in the United States (who average 99.7). Grok 4 may be weeks away from becoming even smarter, but the progress at which AI reasoning inches ahead matters little when humans write code for these programs. However, AI *has* started to write its own code. In tandem, Mark Zuckerberg is building a super team dubbed the "superintelligence AI" lab and he offered a single person, Daniel Francis, $1.25 Billion for a four-year contract (or a $312 million per year salary). Further, Zuckerberg has gone on to poach the top AI talent from OpenAI, Anthropic, and Google, nearing 24 people in total out of a team of only 44.

Unfortunately, U.S. companies are also allowed to funnel money into Chinese AI companies, in part because it is a less expensive alternative than U.S. developed AI. China, as a near-peer adversary cannot be allowed to reach superintelligence first because whoever wins the AI race to superintelligence will have nearly unlimited computing ability and will be able to launch devastating cyber-attacks with ease.

If there are two teams approaching the finish line in a winner-take-all superintelligence race, then there is also a direct implication for long-term deterrence on global war. Imagine the following scenarios:

SCENARIO 1: The U.S. is ahead in the race to superintelligence, but China works diligently to steal code, launch cyber-attacks, and intimidate U.S. scientists. Eventually, China assassinates critical AI scientists, prompting the U.S. to threaten the use of nuclear weapons against China to stop its attacks. Yet, just before all-out war, China ceases its efforts, having become successful in its bid to cripple the U.S. AI industry so it can reach superintelligence first.

SCENARIO 2: The U.S. is ahead, but China is only barely behind. China uses its innovative AI models to wargame nearly unlimited sequences and calculates what it believes is the perfect

attack to prevent the U.S. from reaching superintelligence first. In this scenario, the attacks never ramp up. Instead, it results in a massive, unprovoked first strike that incapacitates the U.S. This might be a nuclear strike or simply an EMP strike that decimates the U.S. power grid. Either way, China wins again.

SCENARIO 3: The U.S. and China hide their governments' AI progress. Public companies continue progressing toward superintelligence, but one or both achieve it in a military or national laboratory behind closed doors. They ponder the best way to use it, leveraging it like the nuclear football in global diplomacy (i.e., setting the briefcase on the floor next to the President). They may have accessed superintelligence but lack confidence in the technology to use it for the near future.

SCENARIO 4: The U.S. and China hide their governments' AI progress, and both achieve superintelligence behind closed doors. Then one day, one of them launches an attack on the other, prompting the other side to launch its own superintelligence response. The two AI agents battle across every sector of society, arm-wrestling for control. Seemingly trivial differences between one model and another let one win in one sector and the other win in another.

This article does not presume that the outcome of a superintelligence race is represented in one of these four scenarios. Rather, it argues that AI will inevitably complicate the landscape of deterrence as it may give confidence of victory in otherwise stable situations. This moment in history is nothing less than the moment when scientists Leo Szilard and Albert Einstein wrote President Roosevelt to warn of the potential use of fission in bombs.

The United States government must think carefully about the current state of AI in the world and what it will mean for deterrence strategy. We need to have a planned response if a superintelligence cyberattack is launched against the U.S. This includes physically isolating our command-and-control systems and planning for surprise attacks, itself planned by another country's AI technology. Worse yet, military planners need to consider how to detect and respond to multiple grey zone micro-attacks that may be a component of a larger cascading attack.

We are amid our generation's Manhattan Project moment. The 2023 *Oppenheimer* movie culminates in the detonation of the 1945 Trinity test. Perhaps if the United States plans well, in 80 years, we may all be able to enjoy a movie about Zuckerberg forming his superintelligence lab.

Rob Kittinger, PhD, is a Senior Fellow at the National Institute for Deterrence Studies. The views expressed are his own.