Artificial Intelligence and Concerns about its Military Applications

-Dr. Todd Carrico

After decades of being mostly relegated to science fiction, Artificial Intelligence (AI) today is more and more a reality. Whether it's a flashy example, like IBM's Watson outsmarting humans on Jeopardy, or a more subtle example, like intelligent software agents augmenting existing systems to improve performance, it's clear that AI has entered the real world.

As has always been the case with AI, along with excitement over computers performing human-like functions, comes a certain amount of concern. It's not surprising that the recent advances in AI have generated an increase in voiced caution, particularly regarding AI's military applications. Concerns have largely focused on weaponized drones, or autonomous systems, directed by AI, rather than humans.

I believe some degree of concern is warranted, but a general unfamiliarity with AI may be leading to unwarranted concern. I wanted to take the opportunity to clarify a few technological concepts related to AI, as there is significant confusion about a number of AI concepts and clarification may help us focus our concern more appropriately.

While there are many branches of AI, only a few are focused on creating General Intelligence, the kind of intelligence that allows humans to make decisions like which target to engage. Many of the branches of AI focus on developing techniques for solving certain classes of problems in an intelligent fashion, and that intelligence can be inspired by human cognition (expert systems), human physiology (neural nets), animal social behaviors (swarms), or human social behaviors (game theory). Of those focused on creating intelligent machines, including drones,, there are those focused on Narrow AI, intelligence limited to a specific problem domain or functional area, and General AI, intelligence across the whole spectrum of problem domains.

The theoretical capability of General AI is the source of decades-old concern as well as the foundation of many exceptional works of science fiction. If, in fact General AI could give computers the power to "outthink" their creators, what therefore would stand in the way of computers deciding to do away with their pesky keepers? I am not one to shortchange the potential of technology in general or AI in particular, but I believe these concerns are unwarranted. Leading AI experts agree that General AI is still at least a decade away from fruition. I believe the road to general AI will take us to places that will enable us to either see that this existential threat is non-existent or take measures to ensure it doesn't occur.

Another key concept of AI is human involvement. Human-machine teaming holds tremendous potential. AI-enabled systems can generate and evaluate alternatives in seconds based on analysis of more data than a human could learn in a lifetime. This "grunt work" then frees up the human member of the team to perform the higher level cognitive functions that lead to the best decisions.

With human-machine teaming, there is always a "Human in the Loop." Without a human in the decision making process, there is significant cause for concern. Russia's highly publicized use of armed drones that will automatically target and kill anything the system categorizes as an "intruder" is an example of a worrisome system without a human in the loop.

Traditional mines pose much the same risk. Instances of innocents being killed or maimed by mines have led to numerous international treaties and have led the United States Department of Defense (DoD) to develop "smart" mines like the Spider mine system that requires a human decision to deploy a mine.

Whether or not the term Human in the Loop is used or the systems are considered Human-Machine teams, the concept of human control is the key element of concerns related to AI. Great care must be taken to ensure appropriate human involvement and control of AI systems.

Recent analysis and study associated with the United States Department of Defense's Third Offset initiative has resulted in another categorical distinction and two new terms: Autonomy at Rest and Autonomy in Motion. Autonomy at Rest is AI in software systems, such as decision support systems and planning systems - those without

a robotic component. Autonomy in Motion, as you might guess, is AI in robotic systems such as drones, unmanned vehicles and the like.

The focus at CSI has been on using AI within our cognitive computing systems (see CSI website for more on cognitive computing) for Autonomy at Rest systems. The AI in our systems helps us emulate human cognitive reasoning processes in software and serve as a highly capable machine partners in a human-machine teams. Our military applications are designed to enable users to more effectively execute operations planning, assessment and execution management.

Every day we strive to broaden our system's reasoning capabilities and make them more helpful, but our systems are designed to be "human in the loop" systems. Applying the existing classification of AI, CSI systems would be considered Narrow AI systems. Any semblance of General AI is at least a decade down our developmental road. In DoD's new vernacular, CSI systems would be categorized as Autonomy at Rest systems providing decision and planning support.

CSI's Autonomy at Rest systems are capable of interacting with and helping humans control "Autonomy in Motion" systems. Moving forward, DoD will need to ensure its interrelated systems, AI and otherwise, maintain positive human control.

Much has been made of prominent scientists' warnings related to AI, but these scientists aren't advocating for some kind of impossible reversal of the AI technological tide and they aren't concerned about the theoretical threat of tomorrow's General AI. Their concerns revolve around the human control issue. The summary of a July 28, 2015 open letter signed by nearly three thousand AI and Robotics researchers, including luminaries like Steven Hawking and Elon Musk, states that the signers "believe that AI has great potential to benefit humanity in many ways," but goes on to recommend a "ban on offensive autonomous weapons beyond meaningful human control." This is sound advice. Similar to, but significantly greater than the threat posed by conventional mines, AI is a technology that demands international agreement on its use in warfare.

The potential power of AI in decision support and planning cannot be overestimated. By reducing the fog of war and strengthening situational understanding, it could provide unrivaled command and control (or mission command) capability. The cognitive computing systems AI enables can allow people and computers to build better plans, faster and to greater detail, and then execute those plans more effectively with continuous monitoring and assessment. The partnership of man's creativity, insight and complex pattern recognition combined with the computer's ability to manage massive amounts of knowledge, work through every last detail, and monitor everything continuously is a powerful capability. Through the prudent application of AI, this capability is within reach.

The AI community, as well as policy makers around the world, should contemplate how to develop this technology in a responsible and ethical way. Concern is warranted, but the great benefits of AI technology, both in terms of the peace attainable through the deterrence of a dominant military capability and the multitude of quality of life improvements that AI offers, can be secured while addressing these concerns.

Policy makers should immediately begin the process of obtaining an international consensus that mandates human control of AI-enhanced weapon systems. DoD will need to include provisions for maintaining human control of autonomous systems in both its Autonomy at Rest and its Autonomy in Motion efforts. Finally, while we are still a decade or more away from General AI and its potential threat is more nebulous, now is the time to start the dialog that will determine the safeguards and mechanisms that will ensure the prudent control of AI technology, even as AI enabled systems rapidly transform our lives for the better.