KAMPALA INTERNATIONAL UNIVERSITY

Research Journal of Humanities, Legal Studies & International Development | **RJHLSID**
***p-ISSN**: 2536-6564 | **e-ISSN**: 2536-6572*
Volume 5, Number 1 April, 2023

Artificial Intelligence and the Security Dilemma

Chris Meserole
Foreign Policy, Strobe Talbott Center for Security, Strategy, and Technology
Brookings Institution, Washington DC

Article DOI: 10.48028/iiprds/rjhlsid.v5.i1.08

Abstract

Recent breakthroughs in machine learning and artificial intelligence (A.I.) have prompted breathless speculation about their national security applications. Yet most of that work has focused narrowly on their implications for autonomous weapons systems, rather than on the broader security environment. Apart from Michael Horowitz and a handful of others, few scholars have sketched out how A.I. might affect core questions of international relations and foreign policy. One key challenge stands out: What influence will A.I. have on security dilemmas between great powers? With the two leading producers of A.I., the United States and China, already eyeing each other warily, the question is far from an idle one. If we are to maintain a stable international order, we need to better understand how artificial intelligence may exacerbate the security dilemma and what to do about it.

Keywords: *Artificial intelligence, Security, Dilemma*

Corresponding Author: **Chris Meserole**

First Published: https://www.brookings.edu/blog/order-from-chaos/2018/11/06/artificial-intelligence-and-the-security-dilemma/

Background to the Study

The Security Dilemma

Political scientists have speculated about the security dilemma ever since it was first formulated in 1949. Fresh from two world wars, scholars of international relations puzzled over a disturbing possibility: What if war could break out even when neither side wanted it? If one country wasn't sure about the military intentions and capabilities of its rival, then it would be rational for that country to stockpile weapons and build up its military in response. The rival might take that precaution as a sign of aggression and respond in kind, sparking further military build-ups and setting the two countries on a path toward war. In essence, the quest for security can make a state less secure. From the longbow to nuclear weapons, major developments in military technology have always compounded the security dilemma. New technologies introduce uncertainty about military capabilities: Each advance brings with it uncertainty about how it will be used, or even how powerful it will be. In the 1930s, for instance, each major power knew the general capabilities of radar, mechanized artillery, and aircraft. But what no one knew for sure at least not until Germany blitzkrieged its way through Poland and France was how they would be used in battle. Likewise, early in the Cold War, both the United States and the Soviet Union worried that the other might develop nuclear missiles more powerful than their own. The result was a nuclear arms race.

Artificial intelligence introduces both forms of uncertainty. No one yet knows exactly how A.I.-enabled weapons will be used on the battlefield, much less how powerful those weapons will be. At the tactical level, A.I. introduces significant uncertainty by virtue of being an enabling technology. Rather than constituting a single weapon system itself, A.I. is instead being built into a wide variety of weapons systems and core infrastructure. Tanks, artillery, aircraft, submarines versions of each can already detect objects and targets on their own and maneuver accordingly. Similarly, A.I. is also being deployed within command-and-control centers and logistical infrastructure. Yet it's unclear how those innovations will change the nature of conflict. What effect will swarms of unmanned submarines have on naval warfare? What happens when today's commodity A.I. isn't just bolted on to existing weaponry and command-and-control centers, but baked into them from the bottom up? Which military will do the best job of integrating A.I. into its weapons systems and tactics, and how much of a battlefield advantage will it convey? Despite the rampant speculation about these questions, answers are still elusive and, to some extent, beside the point. From the perspective of a military strategist, what matters most is that the questions need to be asked at all. The prospect that a rival power might use A.I. weapons systems in innovative and unexpected ways is enough to exacerbate existing security concerns.

For all the doubt about how A.I. will be used, however, there's even greater uncertainty about how powerful it will ultimately be. Artificial intelligence is a function of algorithms, data, and computing power. Each of those factors have improved at a fairly regular, but exponential, clip which means we can forecast the progress of A.I. fairly reliably in the short run, but not long term. On the algorithm side, progress over time in transfer or one-shot learning could radically improve the proficiency and even "common sense" of A.I. Even more, on the hardware side, advances in neuromorphic processors and quantum computing may supercharge today's

cutting-edge A.I. To be sure, there's still debate over how well-suited quantum computers are for the optimization algorithms that power the most common forms of machine learning. Yet quantum machine learning nonetheless holds enormous promise particularly for efficiently searching through the kind of vast action spaces that, say, a multi-agent drone swarm will have to manage. Given the breakthroughs in multi-agent reinforcement learning powered by today's GPUs, it's daunting to think of what the U.S. or Chinese militaries could do with the quantum computing of tomorrow. (Indeed, this is partly why China aims not just to be the world leader in A.I. by 2030, but to win the quantum computing race, too.) The uncertainty about how A.I. will be used and how powerful it will be poses profound challenges for today's military strategist. On the one hand, a rival power may use commodity A.I. weapons systems in novel ways and gain the kind of first-mover advantage that Germany once did with the blitzkrieg. On the other, a rival power may instead develop better and more powerful A.I. itself and use it to gain an insurmountable military edge. Either prospect is enough to exacerbate existing security dilemmas.

What to Do

How to resolve the "irreducible dilemma" of great power rivalry is never an easy task. This is especially true today, when the world's two leading powers China and the United States are increasingly unsure about the military capabilities of the other, as well as their intentions. Fortunately, both powers can work to reduce the uncertainty introduced by A.I. When it comes to how A.I. might be used, each military can rely on red-teaming and war games to think through novel and innovative tactics. In addition, each can publicly broadcast new tactical capabilities. Demonstrations like the one China's navy held last June, in which it tested a fleet of more than 50 drones, reduce uncertainty about how they might actually use A.I.-weapons systems.

The more difficult question is how to prevent uncertainty about the future development of A.I. from destabilizing the security dilemma between the two countries even further. At issue is how A.I. is produced. In the past, most major new military technologies were primarily developed by the military, but A.I. is a "dual use" technology, the development of which is instead commercially driven and dependent on a global supply chain. Although there are advantages to market-driven development most notably, markets themselves can serve as an important source of information about A.I. capabilities, it also introduces strategic risks and complexity costs.

Conclusion/Recommendation

Any strategy for mitigating the uncertainty introduced by A.I. will need to grapple with that complexity. The United States and China have three general options for managing A.I. going forward:

1. **Full cooperation.** The United States and China could commit to fully open trade with respect to commercial A.I., while establishing bilateral organizations to monitor its military applications. Although this option would reduce uncertainty about the military capabilities of each power, it would also increase the dependence of each on technology transfer from the other.

2. **Full competition.** The United States and China could impose strict export controls on A.I.-related hardware and software and double-down on their domestic A.I. efforts. Such a move would decrease the dependence of each country on technology transfer from the other. However, fully disentangling the global supply chain would impose enormous economic costs. Further, the resulting "A.I. arms race" would intensify the security dilemma: By removing markets as an information mechanism, it would increase uncertainty about each power's A.I. capabilities.
3. **Partial cooperation and competition.** The United States and China could impose export controls on select hardware and software, while establishing bilateral channels to increase information sharing about the affected technologies. This option would keep the costs of disentangling the global supply to a minimum, while also limiting the potential dependence on technology transfer for critical A.I. technologies.

Each option is far from ideal. Full cooperation is a non-starter, since the United States and China are too suspicious of the other's intentions to risk growing more dependent on technology from the other, much less allowing greater technology transfer to the other. Likewise, full competition isn't feasible since neither country can afford the costs of completely de-coupling supply chains, especially in the short run. Partial cooperation and competition, meanwhile, risks being too clever by half, particularly if the export controls are applied ad hoc.

Partial cooperation and competition, despite its risks, is the least-worst option. The challenge will be to find a guiding principle for why some dual-use technologies are restricted while others are not. One possibility is to leverage the distinction between the consumption and production of A.I. The United States and China could allow for relatively free trade in terms of A.I. applications, for instance, while imposing strict export restrictions on the hardware that will be required to produce those applications, such as the neuromorphic chips and quantum computers that will be integral to their use. Partial cooperation and competition would by no means be a panacea. But a limited A.I. arms race is far preferable to an all-out one and would minimize the risk that the broader security dilemma between China and the United States spirals into actual armed conflict.

Reference

https://www.brookings.edu/blog/order-from-chaos/2018/11/06/artificial-intelligence-and-the-security-dilemma/