RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg

No. 125 – 25 June 2019

Singapore Defence Technology Summit

Why the Sky is not Falling: The Diffusion of Artificial Intelligence

By Zoe Stanley-Lockman

SYNOPSIS

While AI proliferation seems limitless and uncontrollable, what are the key ingredients necessary for organisations, particularly militaries, to leverage the technological enablers and limit unwanted diffusion?

COMMENTARY

IN ITS second iteration, the Singapore Defence Technology Summit (SDTS) this week focuses on a key theme: the proliferation of technology and the impact of that proliferation on security, defence, and society. At the outset, controlling the proliferation of emerging technologies such as artificial intelligence (AI) – a key strategic technology area the Summit will explore – seems daunting. The cat may already be out of the bag, as the saying goes.

Many presume that the commercial nature of AI means it will automatically proliferate. On the one hand, there is reason to believe that AI will be accessible to many – including to nefarious or adversarial actors. But conversely, there is also significant evidence that "AI democratisation" arguments are overblown. While AI has the potential to expand the attack surface, it should not be seen as an equalising force.

AI for All

Be it to leverage a marketing advantage or laud impressive advancements in machine learning, AI seems to be everywhere. Organisations explicitly seeking responsible openness see sharing and collaboration as important values in the AI community. AI hype also characterises the field as democratising, particularly with pre-built AI "starter packs" of algorithms and user-friendly interfaces that make it possible for anyone – for better or for worse – to enter into the field. With such links, the narrative of AI democratisation also connotes that access to AI is unfettered.

AI certainly does challenge traditional counter-proliferation techniques. Computer scientists have likened preliminary attempts to place export controls, a key mechanism to prevent undesirable proliferation of critical technologies, on AI to "controlling the export of math" itself.

Because advances in AI come from modifications to a set of algorithms widely available in the public domain, there is a limit to how effective export controls can be. Unlike other sophisticated technologies, such as research on nuclear materials, there are no secrets that export control regimes can try to prevent from spreading.

Furthermore, in a strategic context, one second-order effect of emerging technologies is that the lower the cost, the higher the willingness to deploy it is. In particular, financial intensity, one of the key components to determining the diffusion potential of an innovation, typically translates to more experimentation. With technologies dependent on open-source information, such as AI, widespread interest and experimentation can therefore be expected.

Not So Fast…

Nevertheless, diffusion is often assumed too easy. Anyone who looks at the military potential of AI as a panacea – or, conversely, an existential danger – need only revisit debates from the late 1990s and early 2000s, when some predicted that network-centric warfare and related concepts would reduce war to targeting exercises. The intervening decades have proven anything but.

Similarly, AI should not be seen as a great equaliser: not all militaries and not all adversaries will be capable to build up the talent, computing power and data, and organisational capacity required to sufficiently scale up their usage of AI to produce appreciable effects.

The most obvious hindrance to AI proliferation is a shortage of the most important resource: talent. AI talent is critical because the context and purpose of each algorithm is unique enough that it cannot be presumed to be transferrable. For AI to diffuse to smaller countries, those countries will need the resources to attract and retain the talent, which is already a steep challenge.

Additionally, in an era of heightened competition, regulations that renationalise, inadvertently or otherwise, research communities could reimpose barriers and hamper international collaboration.

But there are less conspicuous barriers to systematic AI adoption, too. While talented lone actors could plausibly create an artificial narrow intelligence (ANI) for single use, more capital would be required to systematise the usage of AI by militaries. Currently, it takes 100 million times more computing power to train an AI than to deploy that trained algorithm.

In other words, significant computing power – which not all lone actors and small militaries can be presumed to access – and large datasets are prerequisite even to relatively basic AI deployments. Without the talent, computing power, and data (including expensive storage costs, such as in the cloud), there is a ceiling to how useful or effective proliferated AI could be. As such, militaries should instead distinguish between narrow exploitation of AI and scaled-up systematisation.

Taking the Shortcut: AI Accelerators

There is an exception to the high computing power costs associated with training an AI: AI accelerators, or hardware such as specialised AI chips that can speed up operations that, with generalised chips, would otherwise require time and more processing power.

Currently tensor processing unit (TPU) chips, developed by Google as AI accelerators for data centres, are among the most advanced on the market for neural network machine learning. Other application-specific integrated circuits (ASICs) also increase the "performance per watt" to decrease computing power needs and other related expensive deployment costs, such as cooling systems for data centres. Such generational leaps in the hardware may allow for lower costs, faster transfer speeds and smaller sizes to fit into more devices.

Still, even with hardware advancements, computing power availability is not fungible. The good news for AI non-proliferation is that this hardware is likely to be easier to control than algorithms themselves. For instance, Google has chosen to make TPUs available to select users. While placing export controls on AI algorithms does not seem plausible, export control regimes such as the Wassenaar Arrangement for dual-use items may be more effective at controlling the diffusion of AI accelerators.

In fact, the United States is currently considering future rules on AI chipsets, which, if eventually transformed into controls at the Wassenaar level, could change the barriers to entry to deploy AI.

Strategic Culture

Most importantly, not all organisations are primed to transform their cultures and structures to best leverage AI. In tandem with financial intensity, described above, organisational capital is the other key determinant to the pace at which an innovation diffuses throughout international systems. This is perhaps the most important takeaway for AI proliferation: access does not equal absorption.

For militaries, institutions notorious for their cultural conservatism, identifying the appropriate role of AI in defence decision-making – let alone investing in and implementing it – is difficult. Even for tasks that are ripe for AI, the results delivered by machines may require more investment that, for financial, political, or cultural reasons, are not acceptable.

The barriers to entry for small-scale adoption are sufficiently low that militaries, or perhaps non-state adversaries, may be able to define narrow tasks – likely the dull and dirty, non-lethal, low-hanging fruit. Smaller militaries with resource constraints will find some of these constraints more challenging than others.

On the one hand, they can expect to be able to invest in narrow AI applications and could select AI niches that do not impose intensive training costs. Instead of native development of AI systems requiring large datasets and computing power, hardware such as application-specific integrated circuits (ASICs) would come with pre-packaged applications that could help them to this end.

On the other hand, smaller militaries may be leaner and find fewer organisational boundaries to leapfrog from analogue to AI capabilities, where software-based transformation can prioritise security and agility from the outset.

Many will be able to find some utility for AI. Ultimately, only few will be able to afford the talent, computing power, datasets, data storage, hardware, and organisational capacity to develop systematic purposes for AI and scale the usage accordingly.

Zoe Stanley-Lockman is Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies (IDSS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. This is part of a series.