Opinion **Artificial intelligence**

The Pentagon needs a new AI strategy to catch up with China

Defence leaders unfamiliar with artificial intelligence, cyber or hypersonics should educate themselves or get out of the way

NICOLAS CHAILLAN

China's hypersonic missiles would require AI-enabled defences to stop them © Imagine China/Reuters

Nicolas Chaillan 9 HOURS AGO

The writer was formerly the first chief software officer at the US Air Force and Space Force. He is now chief technology officer at cyber security firm Prevent Breach

When I resigned from the Pentagon in September, I warned that without urgent action we would lose the artificial intelligence war against China within a year. Due to our complacency, we have watched the Chinese Communist party not only catch up with the US in many warfighting capabilities but, worse, lead in some of the most crucial ones like AI and cyber security. Pentagon leaders like to call China a "near peer adversary", but this demonstrates how badly they have underestimated Beijing.

I don't, and you shouldn't. Whoever wins the AI race will control the planet. When the US has conducted virtual exercises pitting AI-powered jets against top pilots, the AI systems have prevailed. China's hypersonic missiles will only be stopped using AI-enabled defences.

The solutions to this threat are clear. The Pentagon must embrace agility and understand that innovation involves failure. It should set up a joint IT office, centralising all functions such as IT procurement, cloud services, data warehousing, AI, cyber security and training into a dedicated Technology and Information Merged Enterprise, which reports directly to the Department of Defense's deputy secretary. The department also needs to boost public-private partnerships, be more accountable

itself, and refuse to empower those who do. If you are a leader and you don't know the subject matter, then educate yourself and be prepared to take advice, or step out of the way. We must mandate at least one hour per day of continuous learning for employees. The other common mistake is to create more siloed AI and data teams or even worse, a "cyber force". We do not need specialist units rushing in to save the day. Software, cyber and AI must be baked-in to every DoD team. Concepts such as the Pentagon's Defense Digital Service, set up ostensibly to deliver new technology across the DoD, have failed in part because they exist in a vacuum. We must also create respected career paths for software, cyber security, data science, AI and machine learning, with progression of pay and titles so they are not seen as dead ends.

To update its workforce, the Pentagon should collaborate more with industry. The US has incredible companies innovating across all sectors, from self-driving cars to space exploration and quantum computing. Unfortunately, the DoD continues to over-classify information. This prevents it from informing industry partners about the extent of China's aggressions — which range from embedding spies in our companies to stealing intellectual property and conducting cyber attacks. As a result, many US companies still refuse to work with the Pentagon. I believe that if it was able to share more about the nature of the threat, more would want to partner with the military to win this fight.

Bringing in expertise from outside defence means fixing the clearance processes, so people can move in and out of government to gain skills and experience. We must allow DoD folks to spend time working at start-ups and innovative companies such as Tesla and SpaceX, and return to implement their knowledge for the military. Without sufficient talent, US defence cannot succeed.

Finally, we must stop preparing for the wrong battles. The next war will be software-defined, it won't be won with a $1.7tn programme of fifth generation F35 fighter jets or $12bn aircraft carriers. China can take down our power grid without firing a single shot, because of kindergarten-level cyber security in our critical national infrastructure. This shows we are investing in the wrong defence capabilities. As we have seen recently with the Colonial Pipeline hack, the risk is tangible. We must act now to trade off some F35 jets for scalable autonomous systems such as drone swarming, self-flying jets and ships, hypersonic and cyber capabilities, and military advances in space.