Australia-China Relations Institute
澳中关系研究院

Opinion

# Deterring China isn't all about submarines. Australia's 'cyber offence' might be its most potent weapon

Greg Austin
May 4 2023

Note: This article appeared in *The Conversation* on May 4 2023

Australia doesn't need to wait ten or 20 years for its new submarines, or for long-range missiles, to project effective military power against China.

It has the ability to use its cyber forces to strike strategic targets inside China now, or for the sake of deterrence, to hold out that threat.

Cyber attacks are aimed at breaking into enemy military networks to disrupt or disable their systems. They can be used against a variety of weapons and communications systems.

Cyber forces are now an integral part of a country's strike capability in wartime. The United States is even now planning wartime cyber attacks against China, should they be needed. According to 2018 figures, the Americans have a force of around 240,000 defence personnel and contractors in place to contribute to cyber defence and cyber attack, with up to one-third likely available to support the latter.

In the event of war, these US cyber attacks could be sustained across the full range of Chinese war capacity. The aim would be to gain what's called 'decision dominance'. This is the 'disintegration' of China's systems and decision-making, 'thereby defeating their offensive capabilities' – if we can interpret remarks of the former commander of US Indo-Pacific Command, Admiral Philip Davidson, to be a reference to China.

Australia has been much more guarded in discussing cyber offence than the US, but the two allies are in step. Canberra is in the process of tripling the size of its offensive cyber forces under Project Redspice, announced last year.

It could attack military command and control assets anywhere in China in the event of war. Softer targets might include critical national infrastructure, such as the energy grid supporting the war effort.

Australia's cyber force will remain small compared with the US. But it can also call on private domestic or foreign corporations to design attack packages against China, as the US does.

Australia is aiming for world-class offensive options in cyberspace. The AUKUS allies coordinate closely together on cyber operations, and this area of activity is a prime focus for the new grouping.

In 2020, the United Kingdom set up a new organisation, its National Cyber Force, dedicated to offensive strike operations.

As part of this 'cyber three' alliance with the US and UK, Australia's cyber force will likely remain the country's most powerful strike capability against China for decades to come.

**China's cyber security weakness**

Of course, success isn't assured with cyber attacks. But causing disruption on a significant scale can be achieved with a highly focused effort across all phases of offensive cyber operations, especially in coordination with our allies.

The most important phase is the first one: ensuring up-to-date intelligence on the other side's systems. The effort put into cyber intelligence against China's armed forces is actually the foundation of cyber offensive teams, even if the intelligence people aren't counted as having an 'offensive' role.

China is adept at cyber offence. But contrary to popular belief, cyber security isn't a strong point for China, and this makes it particularly vulnerable to attack in wartime. The International Institute for Strategic Studies has assessed that China has certain fundamental weaknesses that will take many years to overcome, including in its cyber security industry, education and policy.

Chinese leaders believe they're well behind the US and allies in terms of military cyber capability. This will likely constrain their choices about starting any war over Taiwan.

**Political sensitivities?**

There's no need for Australia to be shy about this offensive capability against China on political grounds, because China is planning to do the same against us in the event of war.

China is already conducting cyber espionage on Australia and other countries in preparation for a major crisis. It's almost certainly developing capabilities to disable enemy military systems and infrastructure if needed.

Defence Minister Richard Marles recently restated the long-held view that the more offensive capabilities we have, for example through submarines, the more the country can contribute to allied deterrence of potential aggressors.

Australian political leaders must prioritise the military's ability to attack targets in China at scale, in the unlikely event of war. And leaders need to ensure cyber forces have more highly trained people dedicated to this task and a more powerful domestic cyber industry.

For military and political leaders to go down this path more robustly, the Australian Defence Force will also need to reassess the military balance of power in the Asia-Pacific to take account of the US and its allies' cyber superiority over China.

This might also allow Australians to feel more secure about possible Chinese military threats. The choices Chinese leaders might make in provoking a crisis will be shaped by their view that their armed forces aren't as competitive in this dimension of US and allied military power.

*Professor Greg Austin is an Adjunct Professor at the Australia-China Relations Institute, University of Technology Sydney.*