

Australian government alleges cyber-attack to ramp-up provocations against China

Oscar Grenfell
19 June 2020

Over the past days, the Australian government has escalated its role as an attack dog in a US-led campaign against China, aimed at ensuring American hegemony in the Asia-Pacific.

On Tuesday, Foreign Minister Marise Payne delivered a speech accusing China of spreading “disinformation” during the coronavirus pandemic and of fomenting “division,” particularly through the use of the internet. She warned that Beijing was seeking to “undermine liberal democracies” and made clear that Australia would pursue an aggressive foreign policy in the region and internationally.

As if on cue, Prime Minister Scott Morrison announced this morning that Australia was being subjected to an ongoing “major state-based cyber-attack.” Morrison claimed that the operation had targeted “all levels of government, industry, political organisations, education, health, essential service providers and operators of other critical infrastructure.”

Asked by reporters whether Beijing was responsible, Morrison said that the government was “not making any public attribution about these matters.” In the same breath, however, he said that there were “few countries capable of such sophisticated activity.”

His statements have already had their desired effect, with corporate journalists rushing to declare that China is the prime suspect. Less than an hour after Morrison’s remarks, for instance, the *Sydney Morning Herald* published an article baldly declaring that China is “understood to be a likely source of the threat.”

It appears that none of the reporters at Morrison’s press conference asked any of the obvious questions, starting with whether he had evidence for his sweeping assertions.

It was not even clear that Morrison was speaking about a specific cyber-attack that could be attributed to one source. Asked whether he would describe the alleged operation as “unprecedented in scale,” Morrison evasively stated “This is ongoing activity, it hasn’t just started. This is a constant threat to Australia.”

In other words, despite the atmosphere of national

emergency that he sought to cultivate, Morrison could not even confirm a specific “cyber-attack” in recent days. He did not provide a single concrete example of an institution that had been hacked.

Notwithstanding the supposed breadth of the operation and the fact that it had targeted virtually every government service, Morrison said that there had been “no large-scale personal data breaches,” leaving open the possibility that nothing had been successfully hacked.

The purpose of the announcement was to whip-up a wartime atmosphere to justify further provocations against China. In this campaign, the government has the complete support of the Labor Party opposition, which has played a central role in fully aligning Australia with the US drive against Beijing.

Labor Party leader Anthony Albanese repeated Morrison’s vague talking points, telling reporters that “cyber-attacks are a real issue,” and stating: “What the evidence is, is that these attacks are expected to be more often.”

The political establishment is confident that its unsubstantiated assertions will be promoted by a pliant corporate media. For years, the official press has trumpeted McCarthyite claims that Australia is the target of pervasive “Chinese interference,” legitimising the country’s involvement in a US military build-up throughout the region and serving as the pretext for sweeping attacks on democratic rights.

Like the allegations of “Chinese interference,” the claims of a “cyber-attack” are being spearheaded by the intelligence agencies.

This morning, the Australian Signals Directorate (ASD), the country’s electronic spying agency, took the unusual step of issuing a statement to the media, confirming the “sustained targeting of Australian governments and companies by a sophisticated state-based actor.”

According to Nine Media, the ASD identified the techniques used as including “links to fake websites designed to steal users’ details, links to malicious files, and use of email tracking services to identify when users were

opening emails.” The Australian Cyber Security Centre similarly warned of “copy-paste compromises.”

The agencies appear to be describing a phishing operation, where an entity emails a link or attachment under false pretences that activates malicious software if it is clicked upon. Such emails have been encountered by virtually every internet user. They are widely used by private computer hackers and online scammers, further casting doubt on the official insistence that the supposed attack is “state-based.”

The claims are being used to promote Australia’s collaboration with US-led intelligence networks. Morrison stated that he spoke to British Prime Minister Boris Johnson about the operation last night and had “sought cooperation from Australia’s Five Eyes intelligence partners, the United States, Canada, New Zealand as well as the UK.”

His announcement dovetails with similarly unsubstantiated warnings last month from the US Department of Homeland Security and the Federal Bureau of Investigations that American government institutions and companies were being hit by malware originating in China.

The Australian intelligence agencies, including the ASD, are fully-integrated into the US-led Five Eyes network. As revealed by Edward Snowden, they collaborate on a daily basis, including in mass spying operations and other illegal activities, such as computer hacking, targeting ordinary people and foreign governments alike.

The timing of Morrison’s announcement and the ASD statement coincides with a major ratcheting-up of US rhetoric against China. It will doubtless be cited by Trump administration officials as further evidence of the threat that China poses to the US-led “rules-based order.”

Foreign Minister Payne’s Tuesday address to the Australian National University’s National Security College, which is closely connected to the intelligence agencies, was along similar lines. She vaguely asserted that China had “carried out targeted disinformation campaigns seeking to undermine democratic debate and exacerbate social polarisation, and improve their own image in the COVID-19 context.”

Payne favourably cited Twitter’s recent suspension of 32,000 accounts that it claimed were “state-linked.”

As with the fraudulent claims of Russian-interference in the 2016 US election, the Australian political establishment will use allegations of Chinese-interference to intensify online censorship. The government is establishing a task force to combat “online misinformation.” This is a prelude to the branding of social and political opposition, above all from the working class, as being the result of “foreign” efforts to “exacerbate social polarisation.”

Payne appeared to walk back earlier threats from Morrison to “disengage” from international institutions. Morrison,

who has sought to identify himself closely with Trump, denounced “negative globalism” in terms similar to those of the US president earlier this year.

Payne restated the longstanding consensus of the Australian ruling elite that it would seek to prosecute its own predatory interests and “punch above its weight” through “multilateral engagement.” She “affirmed...that international standard setting bodies create rules that are vital to Australia’s security, interests, values and prosperity.”

Payne made clear that she was not calling for some form of peaceful global collaboration, but that Australia would aggressively intervene in international institutions. She stated: “There are times to pursue quiet diplomacy behind the scenes. But there are also times to voice our concerns and persuade others of the need for a course of action.”

The context of her speech, and her earlier allegations of Chinese “misinformation,” demonstrated that such “action” would be directed against Beijing.

Yesterday, the *Australian* revealed that Australian defence chiefs and their American counterparts were in the “early stages of planning joint exercises in the strategic western Pacific outpost of Guam, home to the US Andersen Air Force Base.”

It reported that already on Monday, the HMAS Anzac, Ballarat and Arunta left Fleet Base West in Sydney to participate in “various exercises” in the Pacific. On Tuesday, the HMAS Canberra, Hobart and Stuart departed for “training and maritime surveillance operations.”

Australia was also “awaiting an invitation from India to join the Malabar naval exercises in the Bay of Bengal later this year alongside the US and Japan.” Such an exercise would be particularly provocative, cementing a “quadrilateral alliance” strongly opposed by Beijing because it involves four of the largest military powers in the region.

Australia will also participate in the August RIMPAC exercises, hosted by the US in Hawaii, which is the biggest marine warfare drill in the world.

The recent movements of Australian warships follow major US provocations threatening military conflict with China, including last week’s deployment of three aircraft carrier strike groups to the Pacific.



To contact the WSWWS and the Socialist Equality Party visit:

[wsws.org/contact](https://www.wsws.org/contact)