Alleged hacking of Australian parliament feeds anti-China frenzy

Peter Symonds
20 February 2019

Unsubstantiated claims that a "sophisticated state actor" hacked into the Australian parliament's computer network this month make clear that the upcoming national elections due in May will take place in a political climate poisoned by xenophobia, directed above all against China.

In a statement on Monday, Prime Minister Scott Morrison relayed allegations by the intelligence agencies that the Parliament House computers and all three major parties—the ruling Liberal and National parties, and opposition Labor Party—had been targeted. "Our cyber experts believe that a sophisticated state actor is responsible for this malicious activity," he said.

Alistair McGibbon, head of the Australian Cyber Security Centre, provided few details of the alleged breach. He said it was too early to tell what information had been accessed but declared that it had been the right decision "in terms of risk management, to go publicly with this issue before we knew the full extent."

Neither Morrison nor McGibbon explained why their statements would assist in "risk management" given that so little is known about the hacking. Moreover, parliament and all parliamentarians, as well as presumably the entire intelligence-defence-police apparatus and other state agencies, would have been informed of the breach when it was identified on February 8.

The decision to go public was made not on security grounds but as part of the intensifying campaign to brand China's alleged interference in Australian politics as a national security threat in the lead up to the election. McGibbon declared that the sophistication of the hacking was such that only a "state actor" from "a limited list of countries" could have carried it out. He admitted, however, that "we have low confidence at being able to publicly state who we think it is."

Other "security experts" quickly filled in the blank for the breathless media accounts of the hacking—it had to be China.

A comment in yesterday's *Australian* by Peter Jennings, executive director of the Australian Strategic Policy Institute, for example, was headlined "Suspicion for parliamentary hack must fall on China." On the basis of no additional evidence, Jennings concluded that "China is the one country with the means and the motive to take on the risk of attacking Australia's political parties."

Jennings simply cited previous unsubstantiated allegations of hacking and "seeking to suborn Australian political parties through donations and otherwise engage in bullying tactics to shut opponents up." A former deputy defence secretary with close ties to intelligence/military agencies in Canberra and Washington, Jennings has been in the forefront of the hysterical campaign denouncing alleged Chinese "interference" in Australian politics.

This campaign is a component of Australia's involvement with the Trump administration's escalating confrontation with China over trade and economic issues, as well as the continuing military build-up in the Indo-Pacific, begun under Obama, in preparation for war.

Last year the Morrison government and the Labor opposition joined forces to enact draconian "foreign interference" legislation, which vastly expands police powers that are the basis for war-time measures to crack down on anti-war opponents, "enemy aliens" and any industrial action.

In a foretaste of what is being prepared, billionaire Chinese entrepreneur Huang Xiangmo was stripped of his permanent residency status this month and prevented from returning to Australia after being

deemed an agent of foreign interference (see: “Chinese billionaire stripped of Australian residency as “foreign interference” campaign ramps up”).

Significantly, the hacking allegations have been prominently published in the US and international press, including the *New York Times*, *Wall Street Journal* and *Financial Times*, to feed the growing frenzy of anti-Chinese propaganda. Unsubstantiated claims of Chinese interference in Australian politics over the past two years have been picked up by the American political establishment and media to justify their own aggressive actions towards China.

China has vigorously denied the allegations. Chinese foreign ministry spokesman Geng Shuang told the media: “One should present abundant evidence when investigating and determining the nature of a cyberspace activity, instead of making baseless speculations and firing indiscriminate shots at others.”

Geng warned: “Irresponsible reports, accusations, pressurising and sanctions will only heighten tensions and confrontation in cyberspace and poison the atmosphere for cooperation.” He called for international cooperation to deal with cybersecurity threats—an appeal that will be ignored in Canberra and Washington

Significantly, top cybersecurity adviser MacGibbon told the *New York Times* that Australian agencies had blocked the hacking activities before determining the identity of the hacker. That defensive action, he said, “also does other unpleasant things, like remove some of the forensic evidence we’re interested in.” In other words, who carried out the hacking can no longer be determined with any certainty.

The accusations being made against China are utterly hypocritical. Edward Snowden, a former employee of the US National Security Agency (NSA), revealed the vast extent of its spying operations not only on rivals like China and Russia, but on its allies, international organisations, such as the UN and European Union, as well as on tens of millions of its own citizens.

The NSA collects and stores many billions of emails, phone calls, texts, videoconference and webcam recordings, facial images and credit card records. As part of the “Five Eyes” network, Australia together with Britain, Canada and New Zealand, is a key component of US mass surveillance operations.

Australia and other key US allies have banned Chinese corporations like Huawei from any involvement in the new 5G networks that are being rolled out around the world. While the stated pretext is to guard against the China’s spying and other malevolent cyber activities, it is far more likely that the NSA is deeply concerned that Chinese equipment will compromise its surveillance activities. It collaborates closely with American tech corporations.

Despite the many unanswered questions about the reported hacking attack, the Australian media and political establishment has uncritically echoed the allegations presented by the government and intelligence agencies. Labor opposition leader Bill Shorten immediately supported the government’s claims, declaring that other countries such as the US had been subject to electoral interference and “we are not exempt or immune.”

As Morrison admitted in his statement “there is no evidence of any electoral interference.” Nor have the intelligence agencies provided any indication of what was accessed by the hacker or for what purpose. None of this, however, will halt the rising drum beat of anti-Chinese propaganda as the federal election draws closer.