The balloon goes up: China panic reaches new heights of stupidity

Everything made in China is spying on you! Weather balloons! Cars! Closed-circuit security cameras! And your TV, fridge and underpants, too, probably. Or so one would be led to believe by Australia's mainstream media and Parliamentary panic-merchants, who have seized upon the USA's ridiculous overreaction to a wayward Chinese weather balloon to boost Yellow Peril hysteria Down Under into the stratosphere.

According to subsequent reports, a "high-altitude surveillance balloon" originating in China crossed US airspace over Alaska on 28 January, drifted down over Canada for a few days, then re-entered US skies via the northwestern state of Idaho on 31 January. After the balloon was spotted by members of the public, US Air Force Brig.-Gen. Patrick Ryder told reporters at a Pentagon briefing that it neither posed a military threat nor gave rise to any civilian safety concerns, including in regard to civil aviation given its altitude was far higher than any commercial flight path. And on 3 February, as the balloon was floating over the general area one of the USA's three "fields" of intercontinental ballistic missile silos, an unnamed senior Defence Department official told the *Military Times* that balloons had "limited added value from an intelligence collection perspective" beyond what China could already glean from its existing capabilities. The Chinese Foreign Ministry confirmed the same day that the balloon had indeed been launched from China, but stated that it was merely an "unmanned … civilian airship used for research, mainly meteorological"—that is, a weather balloon. "Affected by the Westerlies and with limited self-steering capability, the airship deviated far from its planned course. This is entirely an unexpected situation caused by *force majeure*", a Foreign Ministry spokesman said.

Nonetheless, such is the McCarthyite political climate in the USA today (p. 14) that the Biden Administration decided on 4 February to make a show of shooting the balloon down after all. As of this writing, the US Air Force has reportedly shot down four more airborne "objects" in US and Canadian airspace—literally UFOs (unidentified flying objects), albeit in this case only because the authorities refuse to identify them. 'Literally the dumbest thing ever' Australian anti-China propagandists immediately jumped on the bandwagon to proclaim that China either had sent, or could send spy balloons here—especially after the US State Department told press on 9 February that "We know these balloons are all part of a PRC [People's Republic of China] fleet … developed to conduct surveillance operations", launched mainly from the southern island province of Hainan, which China "has overflown … over more than 40 countries across five continents". The *Sydney Morning Herald* reported 13 February that Australian officials were "seeking urgent clarification from their United States counterparts about whether they believe Chinese spy balloons or similar surveillance devices have flown over Australia", but that its Australian government sources had "no direct information" to that effect and that Defence Minister Richard Marles had said he was "unaware of any such Chinese surveillance devices flying across Australian skies". (If they have, they certainly were not launched from China; the "jet stream" winds that carry them do not cross between hemispheres.)

SMH's foreign and political editor Peter Hartcher, one of Australia's most obnoxious China-bashers, insisted in a 14 February column that contrary to the US Defence Department's comments, using weather balloons for surveillance actually *would* add value after all, as they can be "outfitted with electro-optical sensors or digital cameras that can capture highly precise images. They can transmit to satellites so they can send findings immediately." In fact, he claimed, "balloons have advantages over spy satellites. They can linger longer and get much more concentrated images much faster than a satellite."

Unfortunately for Hartcher, real experts say otherwise. Even James A. Lewis, head of the strategic technologies program at warmongering US think tank the Centre for Strategic and International Studies, wrote 3 February that "Balloons are not an ideal platform for spying. They are big and hard to hide. They go where the winds take them.… China has spy satellites flying over the United States every day, taking pictures, collecting radio signals and other data. Their space intelligence constellations have grown in number and improved dramatically in collection capabilities over the last 20 years. … China has not used balloons for spying before, and using a balloon would be a step back. The most likely explanation is that this is an errant weather balloon". And Former US Marine Corps senior intelligence officer and United Nations weapons inspector Scott Ritter, in a 13 February interview, dismissed the whole idea as nonsense. First, he said, to take useable images from a balloon that is being blown about in the jet stream would require a gyro-stabilised camera platform. "That weighs a lot, and it's expensive", Ritter said. "But let's say you have that." Storing the data on a disk would be impractical, as you could not count on being able to retrieve it. So, he asked rhetorically, "is it going to transmit the data to a satellite? … Why would you send it to a satellite, when *the satellite can take a better picture of anything the balloon can take a picture of*? And the Chinese have satellites in geosynchronous orbit over the United States taking photographs of everything! The whole concept that this is an intelligencecollection platform is stupid, ignorant … literally the dumbest thing ever. This is much ado about nothing. But now what we've done, is further strain our already tenuous diplomatic relations between the United States and China."

Meanwhile in Australia …

With the US

Senator James Paterson's tweet inciting hysteria over security cameras. Photo: Screenshot

balloon fiasco hovering in the background, local mainstream media on 7 February came out with two scare-stories of their own, one almost as ridiculous and the other even more so, both of which revolve around the ravings of Victorian Liberal Senator James Paterson. A member of the US-loyalist, China-hating "Wolverines"[1] clique in Parliament—whom Allan Gyngell, former Director of Australia's peak intelligence agency the Office of National Assessments, once dubbed "immature, juvenile and destructive"—Paterson is effectively a British agent of influence too, being the Australian co-chair of the London-based Inter-Parliamentary Alliance on China (IPAC) founded and led by rabid Sinophobe and disgraced former Conservative Party leader Sir Iain Duncan Smith MP. Paterson is also the immediate past chairman of Canberra's Parliamentary Joint Committee on Intelligence and Security (PJCIS), which is supposed to maintain democratic oversight of Australia's intelligence agencies but in practice merely rubber-stamps their agendas.

On the evening of 7 February Sky News Australia reported that "Australians are being told for the first time to avoid buying Chinese manufactured vehicles if they want to protect their privacy and data", with so-called national and cyber security experts "warning modern cars manufactured in the communist nation are 'data-hoovering computers on wheels' with the ability to build 'patterns of life'.

"'Long gone are the days when a car was a mode of transport to get you from A to B', said the Director of Cyber Intelligence at [Melbourne-based cybersecurity company] CyberCX, Katherine Mansted. 'There are more lines of code in your standard car in Australia than there is in a Boeing 747 jet.' The intelligence expert warned that with 'software comes vulnerability' when it comes to hacking, surveillance and data collection threats." Specifically, "modern cars have the technology to track and trace where users have been", and there are "broader concerns vehicle SIM cards, which transmit 'Over the Air' updates, are acting as potential back doors for hackers or security services to listen into vehicle conversations without the driver knowing."

First, the reason aircraft such as the 747 have comparatively few "lines of code" in their computer systems is precisely because of a design imperative to keep everything as simple, rugged, and therefore preferably analogue and manual as practicable (witness the multiplicity of pilot-operated instruments, switches and controls in even the simplest aircraft's cockpit, compared to a standard car) to reduce the risk of failure, including by limiting the number of potential access points whereby "hackers" might remotely sabotage or seize control of the aircraft.

Modern cars, by contrast, are essentially consumer appliances, designed for maximum convenience with a minimum of user input, thereby sacrificing durability and introducing a multiplicity of potential points of failure, including of data protection. But as US technology magazine *Wired* reported last July, the problem is world- and industry-wide—and China was among the first to crack down on it. Tesla Corporation sells more electric vehicles in China than anywhere else; but due to their own well-known "data-hoovering" they are banned from proximity to major PRC government events. For example, "The city of Chengdu barred Teslas in advance of a June [2022] visit from President Xi Jinping", *Wired* reported, and they are also forbidden from some military sites. "While no official reason was released, the bans seem to be out of concern that the vehicles' impressive array of sensors and cameras may offer a line of sight into meetings of Beijing's senior leadership. … The firm has acquiesced to Beijing's data localisation demands, setting up a dedicated data centre in China, but it cannot shake the characterisation that it is a foreign company—and, therefore, a national security threat." Note that China has not, however, blacklisted Tesla altogether, as Paterson et al. hint should be done with increasingly popular Chinese-owned brands Haval, Great Wall and MG. Paterson is quoted warning vaguely that "Certainly, if you are a politician, or a journalist, or an activist or an academic who is working on issues relating to China or national security, then you need to be extra cautious about the Chinese technology devices that you use"—as though anyone involved in actual issues of national security were not already subject to some of the world's most stringent safeguards. Otherwise, Paterson's professed concerns could, ironically, be addressed by emulating China's "data localisation" policy.

The truly absurd “spying” story, however, dropped the next morning in *The Australian*. The paper reported that as the result of an audit launched by Paterson when he was PJCIS chairman, “Government departments and agencies have revealed at least 913 cameras, intercoms, electronic entry systems and video recorders developed and manufactured by controversial Chinese companies Hikvision and Dahua are operating across 250 sites, including in buildings occupied by sensitive agencies such as Defence, Foreign Affairs and the Attorney-General’s Department.” Claiming the commonwealth “was ‘riddled with CCP spyware’”, the paper reported, Paterson had “called on the Albanese government to immediately get rid of the devices.”

It can be safely assumed that most if not all of this “spyware” was installed during the decade to May 2022 in which Paterson’s own party were in government. More to the point, as the office of Attorney-General Mark Dreyfus told the *Australian*, “The Protective Security Policy Framework requires all commonwealth agencies to manage security threats, risks and vulnerabilities that impact its people, information and assets.” To which the Department of Home Affairs added that on both of the two rented office spaces where it was supposedly exposed, “The systems were not connected to Home Affairs’ operational CCTV [closed-circuit television] network or their internal computer systems. ‘Building owners have confirmed the cameras are not connected to the internet, and in their current set-up, cannot be connected to the internet’, the department said.” Which is to say that despite Commonwealth counterintelligence agency the Australian Security Intelligence Organisation (ASIO) having undoubtedly checked the devices for “spyware” before they were installed, and despite them in some (probably many) cases *not even being connected to the internet*, Paterson would have us believe they somehow magically, untraceably transmit data back to China anyway. Despite the patent absurdity of this proposition, however, Defence Minister Richard Marles immediately buckled and “ordered his department to investigate and remove” all 913 of the devices—which means that the order actually came from Prime Minster Anthony Albanese, since Marles only has authority over his own department.

In the interview cited above, Scott Ritter opined that the only reason the “spy balloon” nonsense gained any traction in the first place, is that both the American public and officialdom have been inculcated with a cartoon-villain image of China, in which everything it does must have some nefarious purpose. “We are not allowed to assume innocence”, he said. “We are not allowed to assume normalcy. We can only assume that the Chinese are all a bunch of yellow, slanteyed plotters…. [That’s] how stupid Americans are, that this is what we think.” The same, sadly, is obviously true of Australia.

Footnote:

1. Named for the heroes of the 1984 movie Red Dawn, a paranoid Cold War fantasy wherein a group of high-schoolers wage guerrilla war against Soviet and Cuban paratroopers who invade the US state of Colorado for some reason.

By Richard Bardon, *Australian Alert Service*, 15 February 2023