HUAWEI — TELECOMMUNICATIONS CONTRACT

Motion

HON CHARLES SMITH (East Metropolitan) [10.06 am] — without notice: I move —

> That this house notes the national security concerns surrounding the awarding of a telecommunications contract to Huawei.

From my perspective, this debate is long overdue. It is one of the most pressing contemporary issues around the globe today when we talk about telecommunications. Let me say from the outset that when I talk about China, the Chinese or Beijing, I am talking about the Communist Party of China, not the Chinese people. They are the most wonderful, hardworking capitalists on the face of the planet. Huawei's current status as the world's largest telecommunications firm and its now prominent role in developing 5G infrastructure throughout the world is likely to make the company an object of scrutiny under the best of circumstances. However, Huawei's parallel role as a national champion of the People's Republic of China's international commercial expansion, as well as its deep and longstanding ties with the ruling Chinese communist party and the obligations of all major Chinese companies to support PRC state goals, would naturally lead to concerns that this company may operate with more than simply profit motives in mind.

For those who do not know, Huawei was founded in 1987 as a spin-off from the People's Liberation Army's engineering corp. It has an opaque ownership structure, and started publishing the names of its board members only after international pressure in 2010. In 2019, China named Huawei as its official national champion for the development of artificial intelligence infrastructure and software. For all practical purposes, Huawei is a subsidiary of the Chinese government. Therefore, we have to ask ourselves where the line is drawn between Huawei's commercial activities and the interests of the Chinese state. According to Steve Bannon, former White House chief strategist, Huawei is the greatest national security threat that America has ever faced. My friend Nigel Farage, a former member of the European Parliament, and Brexit Party leader, was recently quoted in *Newsweek* as saying —

> I think the time has come for people to pick sides.

I could not agree more —

> The question is: Are we to remain with the Western democracies that have always been our allies, or are we to throw our lot in with the Chinese Communist Party?

Perhaps that is a question that major parties can address this morning.

Prior to the 2017 Western Australian state election, members of the now McGowan Labor government—Minister for Transport Saffioti and Minister for Education and Training Sue Ellery—as opposition members travelled to China for five days in 2015, with Huawei picking up the bill for internal flights, accommodation, meals and so on, and providing free phones to those members of the government and opposition who attended, despite their having been briefed about potential security issues. Then, once the McGowan government took office, it announced it was giving a $200 million contract to Huawei because it had won the tender to build and maintain a 4G data network for Perth's rail authority—some would say a happy coincidence. This was done despite Huawei having been banned by the former federal Labor government in 2012 from participating in the national broadband network. This was also done despite Huawei having been banned from bidding for work on Australia's 5G network. The reason behind both those bans was security concerns or, should I say, espionage concerns. This was also done despite the contract decision not going through the usual cabinet decision-making process—all very opaque, indeed.

Why was this company banned by both a commonwealth Labor government and a Liberal–National government but given the okay by the McGowan Labor government? That question has still not been answered. Many public commentators and journalists from around the world, and political thinkers in this country, find the government's decision to award Huawei a contract of this scale incomprehensible. In a memo to Mr McGowan dated 2 July 2018, a state security expert within the Department of the Premier and Cabinet, Justin Court, warned that technology provided by the Chinese may not be able to support a level of security that would be appropriate when the system was upgraded in the future. He was specifically worried about the vulnerability of "mobile data for public safety purposes by law enforcement and emergency services".

When we talk about Huawei and about Beijing and the Chinese Communist Party, we have to discuss influence from the Chinese Communist Party on our democracy. I wonder whether this action or this decision had anything to do with the growing influence of pro–People's Republic of China lobby groups operating in and around our state government. I, for one, am deeply troubled and concerned by political organisations with links to the Chinese Communist Party being active inside political parties and using their apparent growing influence to promote Beijing's interests—interests such as Huawei and interests such as the now enormous Chinese international student trade. It is common knowledge among intelligence circles around the globe that Beijing is exploiting multiculturalism as a ruse for its policy—this is the interpretation. That policy is called "Chinese participation in

politics". Organisations working on behalf of the Chinese government are following advice laid down in 2010 by CCP strategists for maximising political influence in western democracies. This is how it works. They build ethnic Chinese-based political organisations, make political donations, support ethnic Chinese politicians, and deploy votes to swing close-run elections. That is how foreign influence works in our democracy. I wonder whether that is ringing any bells for members in this chamber.

Many of the persons and organisations prominent in Australia's "Chinese participation in politics" movement have identifiable linkages with the influence of the CCP's United Front Work Department network. I will give members a brief explanation of what the United Front Work Department network is, in case they do not know. According to Professor Clive Hamilton, the UFWD is a powerful branch of the CCP tasked with influencing and controlling groups outside the party, including groups located abroad, with Chinese President Xi Jinping famously describing the United Front Work Department as a "magic weapon" of the CCP. Let me say that efforts by genuine Chinese Australians, as well as citizens from other under-represented ethnic groups, to further engage in politics should be welcomed. However, Australia and other democratic societies must also recognise when they are at risk of being susceptible to foreign influence from authoritarian governments.

Why have other countries banned Huawei? The state opposition and I raised concerns about national security. Network switches, gateways, routers and bridges are the kit that controls how and where data is sent. It is what Huawei really does. These core infrastructure devices touch everything that traverses the internet, and it is critical to it functioning properly. This is what has our security agencies worried. But not the McGowan Labor government. Taiwan, Japan, the United States and Australia federally have all banned Huawei. The radio systems replacement project, which is what this contract is about, will deliver a total end-to-end digital radio solution across the Public Transport Authority's 180-kilometre electrified rail network. That includes network switches, gateways, routers and bridges.

For those members who do not know the facts, Huawei was banned primarily as a result of the experience of Great Britain. It is worth going over that story, which began in 2005 when British Telecom embarked on a £10 billion upgrade of its network. Huawei was contracted by BT to supply routers, and transmission and access equipment. But it was not until 2010, five years after the company was awarded the contract to supply transmission equipment, that the British government raised concerns with Huawei about its equipment being exploited. Sources briefed by British intelligence have told ABC news here in Australia that the problem was detected inside so-called core switches. These devices are the proverbial stable door for information, letting data in and out. BT noticed these core switches were doing a lot of chattering; to whom they were not sure, but it was concerning enough for the company to be hauled in by UK authorities. Similarly, and more recently in 2019, Bloomberg reported that Vodafone had found backdoors in Huawei software, stating —

> Europe's biggest phone company identified hidden backdoors in the software that could have given Huawei unauthorized access to the carrier's fixed-line network in Italy, a system that provides internet service to millions of homes and businesses, according to Vodafone's security briefing documents from 2009 and 2011 seen by Bloomberg …
>
> Vodafone asked Huawei to remove backdoors in home internet routers in 2011 and received assurances from the supplier that the issues were fixed, but further testing revealed that the security vulnerabilities remained … Vodafone also identified backdoors in parts of its fixed-access network known as optical service nodes, which are responsible for transporting internet traffic over optical fibers …
>
> …
>
> A backdoor, in cybersecurity terms, is a method of bypassing security controls to access a computer system or encrypted data. While backdoors can be common in some network equipment and software because developers create them to manage the gear, they can be exploited by attackers. In Vodafone's case, the risks included possible third-party access to a customer's personal computer and home network …

I strongly encourage members, if they can find the time, to read that Bloomberg article; it is extremely illuminating.

China has an established track record of cyberattacks, and article 7 of China's National Intelligence Law states, in part —

> … any organisation or citizen shall support, assist, and cooperate with state intelligence work according to law …

Huawei furiously asserts its independence. Even yesterday, I think, the new CEO said that it was laughable to say that Huawei was associated with the Chinese state. It is well known around the globe in intelligence circles that it is part of the Chinese Communist Party, and it cannot shake the suspicions of the so-called Five Eyes intelligence network. It has also recently been revealed that the system to be installed here in WA by Huawei could be used to track people. Last year, Premier Mark McGowan told Parliament that the Huawei network was —

> … a closed system to provide communications between train drivers and their headquarters.

Obviously, he either has no idea what he is talking about or has simply been outplayed by this company. In a briefing note signed by Minister for Transport Rita Saffioti, just weeks before Huawei was announced as the contractor, the Public Transport Authority said that the Huawei network would transmit voice and data to serve a range of potential railway uses. It has been revealed that these so-called "railway uses" now include data capability for personal security, body-worn cameras, CCTV images sent back to central monitoring rooms, and geolocation services to track personnel and assets. According to the media, the Premier and Minister Saffioti then tried to downplay the importance of the project by characterising it as a simple telephone system for train drivers. A document that was recently released to the WA opposition under freedom of information laws revealed that the timely and successful implementation of the new digital system is a precursor to the planned automatic train control project and Metronet extensions. Opposition integrity and procurement spokesman Hon Tjorn Sibma accused the government of deliberately covering up the sensitivity of this project. I think he might be right.

There is a swathe of United States indictments against Huawei. I really do not have time to go through them, but I will just summarise them briefly to give members a taste of what this company has been up to. Huawei in America has been charged with a raft of what they call over there "racketeering" charges, including stealing company information and doing business in countries that it has been banned from doing business in. It has also been charged with stealing intellectual property and was blacklisted, on security grounds, in 2019. To reiterate, these charges in the US relate to a company that did business in countries that have been sanctioned by the US, the United Nations and the European Union, including Iran and North Korea. Huawei got around those sanctions by using local affiliates to ship goods and services to customers in those countries. That is why it has been banned. It is also alleged that the company, through Skycom—another subsidiary—provided the Iranian government with surveillance technology that was used to monitor, identify and detain protesters during anti-government demonstrations.

Our most staunch ally, the United States, maintains that Huawei equipment poses a serious threat to our national security. At issue is the possibility that Huawei is ultimately under the control of the Chinese government. As each generation of telecommunications infrastructure gets smarter, they require constant updates and monitoring by the manufacturer. That is where the danger lies.

HON TJORN SIBMA (North Metropolitan) [10.26 am]: I want to laud Hon Charles Smith for bringing this topic of discussion to the house in the manner in which he has done so. I think the phraseology of his motion is very sober and restrained. I note the obvious point that issues of national security are not ordinarily within the jurisdiction of state government and state Parliaments; however, we live in very interesting times when the norms and easy comforts of restricted responsibility can no longer be indulged. The greatest threat we, as an institution, face is that of complacency. The very worst sin that any leader at any level of government in Australia at the moment can be guilty of is the sin of naivety. We can no longer be naive, because that naivety could jeopardise the welfare of our community in a number of ways that we might not be able to fully comprehend or meaningfully contemplate. However, we have been warned. I refer to an extraordinarily frank address made in public by the director-general of the Australian Security Intelligence Organisation, Mike Burgess. Two weeks ago he delivered ASIO's director-general's annual threat assessment. I will quote a couple of passages from that address. My internet is down and I have this on my phone, but it is replicated on the Australian Strategic Policy Institute's analysis and commentary site, The Strategist. The speech was given on 25 February. I want to read two quotes from it, because they have a bearing on the substance of this motion.

The first quote is —

> Almost every sector of our community is a potential target for foreign interference, particularly:
>
> - our parliamentarians and their staff at all levels of government;
> - government officials;
> - the media and opinion-makers;
> - business leaders; and
> - the university community

How then are we to gauge this level of threat? The director-general of ASIO is very clear about the current situation. I quote directly from him again —

> The level of threat we face from foreign espionage and interference activities is currently unprecedented. It is higher now, than it was at the height of the cold war.

They are sobering and measured assessments from a security professional. This gentleman has competence and knowledge in this domain that I cannot profess to have. However, potentially what distinguishes me from a life experience perspective is that I spent six years in a national security organisation, the Department of Defence. Therefore, these issues do not necessarily come as any surprise to me. However, what has developed exceedingly

apace in the last 20 years is the sophistication of espionage techniques and the capacity and power that communications technology presents.

I do not want to dwell much further on the national security dimension as it pertains necessarily to the government's decision to award this contract to Huawei, a company that is storied in the annals of national security literature and concern across the globe. What has concerned me about this issue bears on the substance of this motion, and it is this point: the government at no point has ever sought in a full-throated way to defend its decision to award this particular contract of this particular value to this particular company for this particular purpose and at this particular time. The government has not given a sustained, open and transparent defence of its decision-making process. That is a point to which this chamber can usefully devote its attention.

Something has always struck me as odd about this particular contract. This is an observation—it is not gratuitous; it is factually based—about the style of government, particularly as it relates to Metronet announcements. The Minister for Transport is all over the Metronet micro-achievements like a rash, to the degree to which she will name tunnel boring machines and the like. The government likes to laud Metronet in every capacity and at every opportunity it can avail itself of. This procurement for a communications platform is essential to the Metronet rollout. Why was this particular contractual decision not given the same prominence as just about every other Metronet announcement? That to me is the curious point.

My colleague Hon Charles Smith has been very generous in acknowledging me and the work of the state opposition in trying to draw out some useful factual information via the freedom of information process. I again lament that we are compelled to act through that process because the government is reluctant in this fora, in the ordinary proceedings of question time, to provide anything approximating useful, open, transparent and accountable information in a timely way. Therefore, we have no opportunity but to go digging. That is absolutely to the government's enduring shame. What is most curious about this particular procurement is the absence of the government's patting itself on the back.

I want to read in an email. As is my wont, I will protect the identity of the individual public servants, because, if I were not to do that, I do not think it would do them any particular favours. This email was sent on 2 July 2018 by a media manager person at the Public Transport Authority, and it is addressed to individuals within the office of the Minister for Transport. I quote —

> As you are aware we are on track to sign a contract with Huawei for the Radio Systems Replacement project later this week.
>
> In preparation for this, we have prepared the following:
>
> 1. Ministerial media statement
> 2. Website FAQ's
> 3. Detailed FAQ's (backgrounder for PQ's/ —

That is presumably parliamentary questions —

> Ministerials)

The following curious point is then made —

> I understand there is no appetite for the Minister to announce this proactively, but a media statement has been prepared just in case.
>
> … Huawei will release their own media statement at this time to technology media only. If everything goes according to plan, this will occur later this week—you will be advised at the time.

This is a very year curious approach to government announcements. It begs the question: why? I have sought at every opportunity to be as charitable and as reasonable to the government as I can be and to give it every opportunity to defend its decision-making on the awarding of this contract to this company, which it is implied, even at the level of a bureaucrat, is a highly sensitive, contestable and controversial decision. For at least the last 18 months, I have sought two key documents and two key documents only—the tender evaluation panel report that led to the decision to award the Huawei–UGL consortia as the one that should deliver the contract, and the contract itself. In the absence of those two documents, the public cannot be reassured in any meaningful way that the government has made the right and appropriate decision in this case. The government still has very serious questions to answer. Whenever anybody raises probity or security concerns in the manner in which they have been raised, the messenger is shot. That is an inappropriate response.

HON ROBIN SCOTT (Mining and Pastoral) [10.36 am]: I would like to thank Hon Charles Smith for his non-government business motion today. He has obviously done his research, and he has brought to light some

really scary information. I also want to thank Hon Tjorn Sibma, a man who spent six years in the defence of Australia, who also has raised alarms and flashing lights.

From the outset, I want it known that I am not against the Chinese people, but I certainly would not support the Chinese government. It is not democratic, it is not transparent and it is certainly not accountable. I have had business dealings with the Chinese. Getting money from them is like getting blood out of a stone. My contribution is much more at street level than the polished speeches from the previous two speakers. We sent a Chinese company a bill for $50 000, and after 90 days of phone calls and letters, we had to wait another month, and then we could put a bluey on them to bring them to court to explain why they were not paying the bill. However, a month before the court hearing, they paid us $25 000 of that bill, which took us right back to the beginning, and we had to put another bluey on them for $25 000.

We cannot believe anything that comes out of China. Countries all over the world have stated that we cannot rely on any of the information about the coronavirus. This is a government that has a history of lies, facades and smoke and mirrors. Members may remember, for example, the 2008 Olympic Games, when the little girl who sang the song for the opening ceremony was actually lip-syncing. The reason was that the young girl who was actually singing was deemed too ugly to appear before the cameras. This is the calibre of the people to whom our government wants to hand over all the data of our transport network. Some of us sitting in the chamber today would chant, "Go Perth! Go WA!" The Premier and his government sit in Chinatown and they chant, "Go China! Go Wuhan!"

HON STEPHEN DAWSON (Mining and Pastoral — Minister for Environment) [10.39 am]: I rise to make some brief comments on behalf of the government about this motion. I have to say that Hon Robin Scott has made a couple of contributions this week that have skirted very close to racism. I urge the member to keep that in mind when he speaks in this place.

I refer to the radio systems replacement project. In July 2018, following an independent tender process that began in February 2017, the Public Transport Authority awarded a contract to design, build and maintain the new digital radio system to a joint venture comprising Huawei Technologies Australia and a leading engineering company, UGL. Throughout 2017 and early 2018, the Department of the Premier and Cabinet and the Public Transport Authority repeatedly engaged with federal security agencies and were ultimately advised by the federal agency that there was nothing in the information we had advised them of that would cause them to look more closely at the project for their purposes. The contract delivers a closed, private voice and data network, with use restricted to the transmission of operational data to support the PTA's passenger rail services. Huawei's involvement in the PTA's digital radio system is consistent with the New South Wales government's decision in 2010 to engage UGL and Huawei to design, supply, install and maintain a digital radio system for Sydney Trains and the Queensland government's willingness in December 2019 to engage Hitachi with Huawei to deliver a radio signalling system for its Cross River Rail project. Huawei has not been excluded from participating in the open 4G and 3G Australian mobile telephone networks. We are advised that it has had longstanding partnerships with Singtel Optus and Vodafone Hutchison Australia, helping build their 3G and 4G mobile networks. Security-based restrictions by the Australian government on Huawei's activities have been confined to the NBN and the new 5G mobile network.

As I have said before, as a precaution during procurement, and again prior to contract award, the relevant state government agencies double and triple-checked with the relevant commonwealth security agencies, including the Department of Home Affairs, that they had no objections or concerns with the state progressing with the project. Like any significant information technology project for any enterprise, the specifications and delivery arrangements for the project put the appropriate cybersecurity protections in place to ensure that the system is not liable to be hacked. These deal with generic cybersecurity issues, which are unrelated to issues of national security.

HON CHARLES SMITH (East Metropolitan) [10.42 am] — in reply: There is not much more to say. We have highlighted the issues, which are to do with the equipment that is used. History tells us that equipment cannot be trusted. I will briefly conclude this motion by saying that I strongly urge the Western Australian state government to tear up this contract and ban Huawei from entering Western Australia. As former Labor Senator Stephen Conroy said —

> … it is not possible to mitigate the risk of China's ability to penetrate, spy and surveil on a network that is built with Chinese kit.

To bring this debate to a close, I will quote my friend Professor Clive Hamilton. If any members here have not read his book *Silent Invasion*, I strongly urge them to do so. It is even in our Parliamentary Library. Professor Clive Hamilton states —

> When I began undertaking the investigation that led to the book, the critical question was—you could look at what's happening in Australia, but you have to ask why. Why has the PRC developed this elaborate mechanism of foreign interference—not just in Australia; exactly the same kinds of issues are coming up in Canada, New Zealand, the United States and, of course, throughout South-East Asia. China in recent

> times, and particularly under President Xi Jinping, sees itself as the emerging hegemonic power. It's a totalitarian state that operates exceptionally close control over its domestic population, and it plans to extend its influence throughout the world, and particularly in the Indo-Pacific region. It has a long history of United Front operations—it emerged, actually, in the 1930s. The Chinese Communist Party has been refining these techniques for a very long time and is now applying them, as one intelligence officer said to me, in a way that can be regarded as a full-court press. I had to look that up; it's a basketball term. It means, basically, an 'all-out assault', and I think that's what's happening. The objective is to, essentially, pacify other nations, particularly in the Indo-Pacific region, so that China can become the hegemonic power, and to edge or indeed drive the United States out of this region and replace it.

The question remains: why did this government, despite national and international security concerns, award a contract to this company?

Motion lapsed, pursuant to standing orders.