THE REGIONALIST
INSTITUTE FOR REGIONAL SECURITY

CHINESE DEVICES AND THE CASE FOR TRADITIONAL RISK COMMUNICATION

Byron Nagy

SYNOPSIS

While the current approach of *Australia's Cyber Security Strategy* begins to address a number of cyber-related security threats, it fails to address the security risks inherent in devices themselves. The integrity of networking and communications equipment is a key area of concern for cyber-security, and ongoing security flaws discovered in Chinese-manufactured devices places considerable doubt over their operational trustworthiness. At a time when China produces over 90 per cent of the world's computers and over 70 percent of the world's mobile phones, the Australian government needs to be concerned about the security reliability of such devices. So far, the government has failed to develop an effective risk communication strategy to inform the public of the potential security risks posed such devices.

SECURITY CONCERNS FROM CHINESE-MANUFACTURED DEVICES

While the government must be careful not to tar all Chinese technology manufacturers with the same brush, they ought to be wary of the security of Chinese-manufactured devices. Increasing numbers of Chinese manufacturers have been revealed to have infected their devices with security vulnerabilities. In 2012, former Central Intelligence Agency chief Michael Haydon declared that Chinese-owned Huawei – the world's third largest mobile phone manufacturer – was involved in

spying operations on behalf of the Chinese government. Although the evidence for such allegations has remained classified, in 2013, the Australian government denied Huawei the right to bid for work on the rollout of the Australian National Broadband Network (NBN) on the grounds of national security. In 2014, security software company Trend Micro discovered deliberate backdoor vulnerabilities in routers manufactured by the popular Chinese brand Netcore. Also in 2014, Californian-based security company TrapX uncovered a large number of Chinese-produced logistics-tracking devices which were infected with malware at the point of manufacture. These devices were used to collect and transmit global shipping information directly to a Chinese university with a history of involvement in Chinese state-sponsored cyber-attacks.

Chinese tech companies have argued that the security concerns over Chinese-manufactured networking and communication devices are unfounded. They argue that there is no evidence to suggest that the practice of manufacturing devices with embedded malware and security vulnerabilities is widespread. Nevertheless, these revelations place considerable question marks over the integrity of Chinese-manufactured devices, of which the Australian government has so far failed to inform the public about. In 2016, Chinese manufacturers Alcatel, Huawei and ZTE accounted for 30.7 per cent of Australian mobile phone sales, with Chinese manufactured networking devices dominating the Australian market. This increasing market share of Chinese-manufactured devices is particularly concerning for Australian national security.

AUSTRALIA'S STRATEGY AND LACKING COMMUNICATION

Australia's recently-published cyber security policy document, *Australia's Cyber Security Strategy*, makes no mention of the potential cyber-security risks involved in using these devices. Although it boasts that "Australian governments and the private sector will work together to share more information, including from classified sources, exchanging information on threats and responses through joint cyber threat sharing centres," public communication of the potential risk of Chinese-manufactured mobile phones and networking devices has failed to occur. Perhaps one explanation for this glaring oversight lies in the modern risk-communication model used to inform Australian cyber-security policymakers. The current policy formation model involves shared consultation and input from a variety of sources including business leaders, individual users, and other community stakeholders. As a result, Australian cyber-security policy has become so far-reaching in its aims and objectives that legitimate cyber-security risks are being side-lined in the communication process.

This criticism of an over-broadening of security policy has been raised before. The Australian Strategic Policy Institute's International Cyber Policy Centre similarly criticised Australian cyber-security policy

for failing to communicate the relative risks facing the Australian cyber-sphere. Tobias Feakin and Peter Jennings argued that former Prime Minister Julia Gillard made a poor decision to broaden the planned Digital White Paper away from a cyber-security focus, and instead towards a "Digital White Paper [that] helps us capture some of the more profound and longer-term issues that have been brought to the table." This decision created a policy document that was rendered pointless before it was published. It simply became another "piecemeal aggregation of various cyber-related initiatives, and the promise – but no delivery – of yet more 'principles', 'guidance' and 'plans.'" This pattern has unfortunately continued with some of the policy iniatives proposed in *Australia's Cyber Security Strategy*.

Instead of remaining focused on tangible cyber-security solutions, some current policy aims and objectives have been broadened beyond usefulness, resembling a corporate buzzword dictionary more than effective public policy. One key theme to *Australia's Cyber Security Strategy* is to "work to ensure all Australians understand the risks and benefits of the Internet and how to protect themselves online." Although cyber security requires a collaborative effort by all parties – be they government, business or individual – the public needs tangible and effective risk communication from the government *in order* to protect themselves online. According to the strategy, the Australian Cyber Security Centre (ACSC) is designed to be that communication outlet. However, although well researched and written, the publications provide little in the way of ensuring "all Australians understand the risks… and how to protect themselves online."

ACSC's annual threat reports provide a comprehensive overview of the current risks faced by Australian cyber users. However, the information is targeted towards large-scale businesses, and is not useful for small-businesses and individual Australian users. The Australian government has made no mention of the security risks of Chinese-manufactured devices. For the Australian government to achieve its ambition to better 'detect, deter and respond to cyber-security threats', it needs to provide a communication outlet that readily informs the public about active cyber-security risks, such as the need to consider the security integrity of the operating hardware. The ACSC is not currently meeting that requirement.

CONCLUSION

A cyber security white paper such as the one presented by the Turnbull government presents an opportunity to communicate real strategies and areas of concern to the Australian public. The government should communicate to the public through a traditional risk communication model of top-down, expert-led information, in order to address cyber-security issues such as the potential

security exploits inherent in Chinese-manufactured devices. Australia's cyber security policy is severely lagging behind that of its Western allies. The United States has already banned the sale of Huawei and other Chinese-manufactured networking and communication devices to its government entities until the integrity of their security can be confirmed. The lack of any communication by the government regarding the security risks posed by these devices highlights a significant flaw Australia's cyber-security policy – and this is a problem for Australia's national security.