OFFICIAL

Australian Government
Australian Signals Directorate

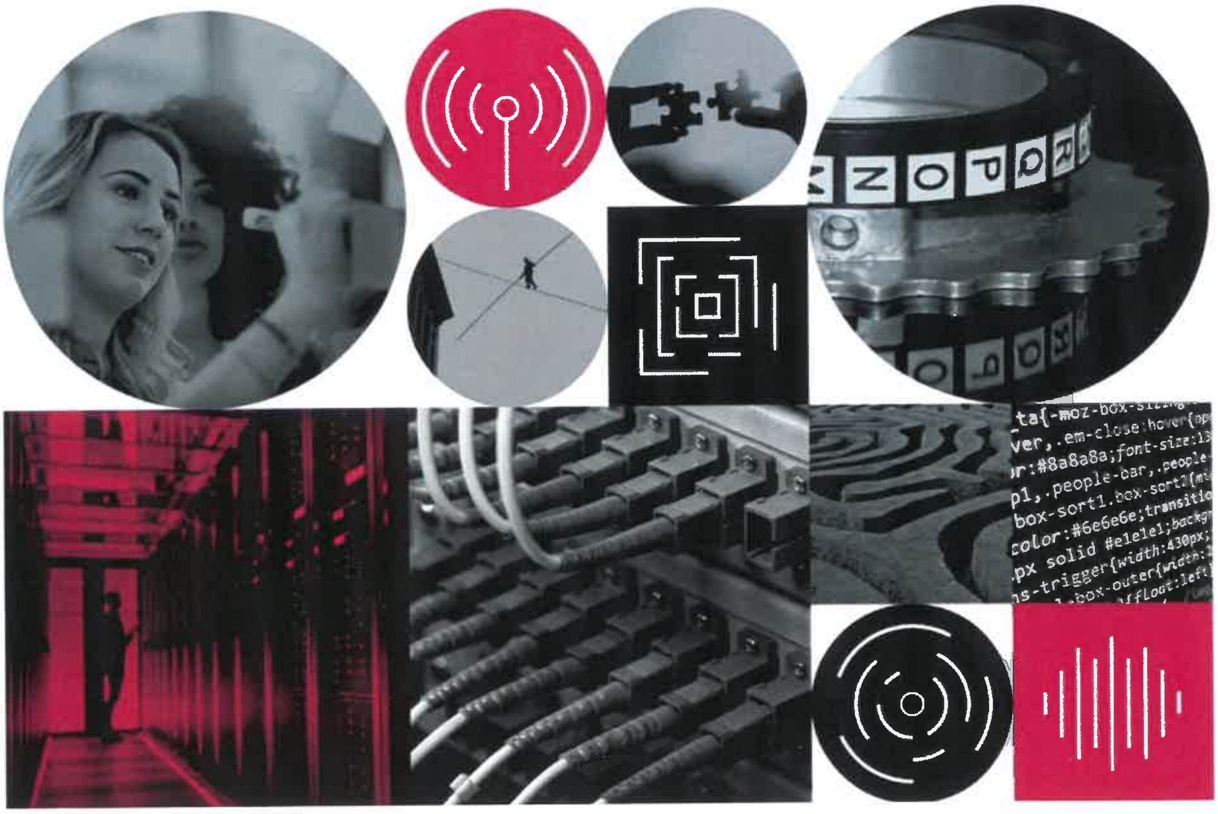
ASD

File Reference: ASD/9035/2020

SUPPLEMENTARY SUBMISSION

CYBER SECURITY

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY



Copy No: 03 of 16

OFFICIAL

Contents

HANDLING REMARKS **4**

CYBER SECURITY **5**

- The cyber threat environment 5
  - State-sponsored activity 5
  - Criminals and non-state actors 5
  - Emerging threats 5
- Overview of the activities of the computer emergency response team (CERT) 6

Handling Remarks

1. (O) This supplementary submission provides information to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on aspects of the Australian Signals Directorate's (ASD) cyber security mission. This submission addresses the Committee's terms of reference, dated 5 December 2019, which requested an overview of:
    a. the cyber security threat environment
    b. the activities of the computer emergency response team.
2. (O) This submission does not address either of the following:
    a. efforts to collaborate with the private and public sector to share information on threats and increase cyber resilience
    b. programs to increase governments, industry and community awareness of cyber security.
3. (O) Those aspects of the Committee's terms of reference have been addressed ASD's primary submission.

Cyber Security

The cyber threat environment

4. (O) Australia continues to be targeted by a range of actors conducting persistent and sophisticated cyber operations. These operations continue to pose a significant threat to Australia's national security and economic prosperity. The most concerning activity for the ACSC is the deliberate targeting of the private and public sectors for valuable intellectual property, personal information of Australians, and Australian government and Defence information.

State-sponsored activity

5. (O) State actors are best characterised by their persistence. They will spend considerable time and effort to compromise their targets where they have a particular intelligence requirement. But adversaries are constrained by resources too. State actors continue to achieve success with basic cyber espionage techniques – such as spear-phishing – but, if necessary, are capable of using far more effective and covert means against high-priority secure targets.

6. (O) The Australian Government, key government organisations, contractors and the academic sector continue to be perennial targets for state actors. They are almost certainly seeking intellectual property relating to defence capabilities and other cutting-edge research. They may also want access to the personal information of employees for subsequent intelligence targeting.

7. (O) However, the ACSC is seeing an increase in Australian entities being compromised simply because they are running vulnerable software, which is targeted in large-scale global reconnaissance operations. Only after exploiting the target will an actor assess the value of the compromise.

8. (O) The precise intent of sophisticated state actors is difficult to determine, but the targeting of the Department of Parliamentary Services and political parties in February 2019, so close to the federal election, is of concern. The security of elections was a priority for the ACSC in the reporting period, with a number of state and federal elections occurring.

9. (O) The number of states that have developed or bought cyber espionage capabilities is increasing. Not all will have an ongoing intent to target Australia, but may target Australians incidentally or in response to topical issues.

10. (O) State actors will attempt to obfuscate their covert cyber operations, but the ACSC, in partnership with like-minded countries, has demonstrated its ability to attribute unacceptable cyber activity to Russia, China, and North Korea, in order to hold these states accountable for their actions.

Criminals and non-state actors

11. (O) Cybercrime is also a pervasive and endemic threat to Australia's economic and social prosperity. Cyber criminals are following the money, and Australia is an attractive target due to its wealth and widespread internet connectivity. They operate at scale with the principle of quantity over quality. They usually target individuals and organisations by exploiting poor cyber-hygiene practices, including the use of default, simplistic, or generic passwords. In the future, we expect to see more phishing campaigns, business email compromises, cryptocurrency mining, credential harvesting and ransomware.

12. (O) Terrorist organisations possess rudimentary cyber capabilities and will probably remain limited to low-capability operations, such as defacing poorly secured websites, stealing personal information from poorly secured systems and conducting unsophisticated phishing operations. They will claim to have greater cyber capabilities than they possess.

Emerging threats

13. (O) In many ways, the current cyber environment is more secure than it ever has been, specifically where endpoint security services are concerned. The baseline level of security for

many consumers has risen as the default security of mobile phones and computers, running the latest software, has improved. Many consumers also benefit from large technology firms making security improvements in their products. However, at times we are our own worst enemy with many cyber compromises enabled by poor cyber security and unpatched networks. The ultimate aim of good cyber security is to avoid compromises. One way to help achieve this is to raise the cost to adversaries, which, depending on the adversary, could result in fewer compromises.

14. (O) Now is a pivotal time to get systemic cyber security right for the next generation of infrastructure crucial for future economic development in Australia. Cyber targeting of critical infrastructure is an increasing area of concern. Despite the many benefits that internet and information technology connectivity provide, administrators of critical infrastructure need to remain alert to, and protect against, adversaries seeking to interfere with the networking which supports these systems.

15. (O) New information technology platforms will underpin categories of technology that are significantly different from what has come before. For example, the fifth generation (5G) mobile phone network will be faster and provide more bandwidth to allow low latency, increased device density and higher speeds. However, to achieve this, fundamental changes are required in how a telecommunications network operates, and this raises questions about how to best secure it.

16. (O) Enabled by 5G will be a large-scale deployment of Internet of Things (IoT) devices that store their data and do most of their processing in the cloud. Billions of these devices installed worldwide will expand the options for hackers looking to compromise networks or steal personal data if security is not prioritised.

17. (O) The supply chain for software and services and, to a lesser extent, hardware, will be a key target for malicious cyber actors looking for a weak link in an organisation's security, or seeking to exploit devices at scale. In 2018, the ACSC saw the Chinese compromise of Managed Service Providers (MSP) as a means to exploit the trusted access of MSPs into customer networks.

18. (O) There have also been examples of malicious actors compromising developer systems and placing unauthorised code into legitimate software that was sent out to customers via automatic updates. An example of this was when Russia compromised software used in Ukrainian businesses to spread the destructive NotPetya malware.

19. (O) Australian organisations need a better understanding of the security of cloud computing and online storage. Inadvertent data spills and malicious data breaches from cloud storage or unsecured databases can expose sensitive information about Australians. These breaches are often due to access control misconfiguration. The trend towards increased usage of cloud storage will require clear understanding of the vulnerabilities and security options available. Further, there must be a clearer delineation of responsibility between the cloud provider and the customer regarding the implementation of security.

Overview of the activities of the computer emergency response team (CERT)

20. (O) In 2018–19, ASD continued to manage a broad range of cyber security incidents, responding to 2164 incidents, including Australia's first national cyber crisis. This crisis saw the ACSC operate at a heightened state of activity to provide advice and assistance to Australia's major political parties and government agencies after they were targeted by a sophisticated state actor.