NYMAN GIBSON MIRALIS

Defence Lawyers and Advisors
est. 1966

1 November 2019

The Hon Peter Dutton MP
Minister for Home Affairs

By submission via Home Affairs online link

SUBMISSIONS TO THE DEPARTMENT OF HOME AFFAIRS ON ITS CALL FOR PUBLIC VIEWS REGARDING AUSTRALIA'S 2020 CYBER SECURITY STRATEGY

Nyman Gibson Miralis

1. This submission is made to the Department of Home Affairs ('**Department**') with respect to its call for public views regarding Australia's 2020 Cyber Security Strategy ('**Strategy**').

2. Nyman Gibson Miralis is a leading Australian criminal law firm specialising in international criminal law and has acted and advised in a vast array of matters involving cyber technology in Australia and abroad. Our work in this regard is increasingly for persons who are victims of malicious cyber activity.

3. Nyman Gibson Miralis has also engaged with various Australian authorities and departments concerning cyber matters on behalf of individuals and companies.

4. In particular, our submission will focus on the interests of persons affected by bad actors in cyberspace.

Introduction

5. As acknowledged by the Department, the growth of cyber-crime affecting Australia and Australians is rapid, with significant effects on those individuals and businesses with the misfortune of falling victim to this offending.

6. Given the rapidly evolving nature of cyber-crime, in our view it is right that the Department is at this time re-evaluating the Government's strategy in this area.

7. In recent times, Nyman Gibson Miralis has increasingly acted for individuals and businesses that have been victims of criminal activity in cyberspace and are seeking redress through the legal system. It is this work and experience in the field of cyber-crime that has informed our submissions below on the 2020 cyber strategy.

Observations on victims' experiences

8. Our experience is that victims of cyber-crime engage our services because traditional methods of reporting criminal activity are not resulting in responses and outcomes seen as satisfactory by such persons.

9. In particular, the following three issues are frustrations commonly felt by these victims.

10. *First*, victims of cyber-crime are experiencing a lack of Police responsiveness to reports of this activity along with an apparent lack of willingness to devote resources to investigating same.

11. The reasons provided for such responses vary, but in certain matters have included jurisdictional constraints, difficulties obtaining necessary digital evidence, and complexity of cases vis à vis prospects of successful outcomes. As a result, we have been contacted and engaged by a multitude of persons who, following what they perceive as an inadequate response by law enforcement, wish to seek to explore engagement with the criminal justice system through private representation.

12. *Second*, the lack of capacity for law enforcement to respond quickly to incidents of cyber-crime is often allows the proceeds of this activity to be disbursed offshore. This essentially means that victims of such malicious activity are left without any realistic option for pursuing an effective remedy.

13. Of course many more 'traditional' crime types involve dealings with – and challenges for law enforcement in tracing – money. However, there is an inherently enhanced speed at which proceeds of crime that are obtained in cyberspace can be sent through cyberspace to locations out of the reaches of Australian law enforcement. Accordingly, delays in the investigation of such offences are acutely damaging to the prospects of success for such investigations.

14. *Third*, limits in law enforcement resources and the specialist evidence needed for cyber-crime investigations has, in our experience, regularly resulted in the need for individuals to employ significant private resources in investigations prior to law enforcement progressing publically funded investigations.

15. These private resources include briefing lawyers to take statements, collect evidence, and prepare briefs for Police to act upon. Such resources are also regularly devoted to having private IT experts collect and analyse digital evidence relating to the alleged offending.

16. The need for victims of crime to invest substantial resources in getting investigations off the ground prior to Police being in a position to act would not be seen as an acceptable state of affairs in any other crime type, let alone other forms of fraud. It should not be the case that the prospects of effective public investigation and prosecution of this conduct is so largely dependent upon the capacity of the victim to fund and resource the beginnings of such investigations.

Submissions on strategic areas to address

17. Our submissions below are tailored to specific questions posed by the Department in its Strategy Discussion Paper.

What is your view of the cyber threat environment? What threats should Government be focussing on?

18. As outlined above, incidents of financial crime in cyberspace are increasing at an exponential rate. It goes without saying that not only does this represent potential enormous harm to the Australian economy at large, but also presents devastating effects to the individuals who fall victim to this activity.

19. Whilst this is occurring largely away from the eye of every day public view, under a cloak of cyber anonymity, the scope of its impacts cannot be overstated. If this rate of crime increase was occurring in any other area of human activity, the concerns of the public would, understandably, be significant.

20. In our submission, Government should focus on the threat posed by malicious cyber actors carrying out financial crimes by targeting Australians who may be naive or vulnerable to these risks.

What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

21. Although prevention is always better than a cure, in our submission Government should address the most serious cyber threats by developing a legal framework – both in terms of legislation and resource capacity – that is equipped to deal with these malicious actions when they occur.

22. Dealing with cyber-crime involves both prosecuting those responsible and enabling effective remedies be provided to victims.

What changes can the Government make to create a hostile environment for malicious cyber actors?

23. As indicated above, our opinion is that a hostile environment for malicious cyber actors is best made through ensuring that Australia's legal system is positioned to respond with strength to such activity.

24. This firstly involves substantially increasing the resources available to law enforcement to investigate and prosecute these often complex cases. As we have noted, the capacity of law enforcement to

respond speedily is critical to the effectiveness of such actions. It is also important for public agencies to be equipped with resources to commence and carry out though investigations and prosecutions of criminal conduct in cyber space.

25. It is also essential that Australia has the legal tools at its disposal to create this desired hostile environment.

26. In this regard, Australia should work with international partners to increase the visibility and traceability of international money flows, along with seeking to ensure that arrangements exist whereby funds taken out of Australia through cyber-crime can be repatriated to victims.

27. Further, Australia should also ensure that there is clarity in criminal legislation concerning the reach and presence of jurisdiction in cyber-crime cases. As this type of offending often involves few conventional ties to physical territory, legislation should make clear the extent to which conduct occurring in cyberspace but producing effects in Australia can be caught by Australian criminal laws.

28. In our view, it is in Australia's interests to cultivate and preserve a reputation as a jurisdiction with the means, will, and practice of strongly responding to manifestations of cyber-crime that touch Australia.

Conclusion

29. We thank the Department for the opportunity to make submissions on this important topic and hope that our observations above can contribute to a productive Strategy moving forward.

30. Thank you for your consideration of our submissions.

NYMAN GIBSON MIRALIS

[redacted]

Dennis Miralis
Partner