Avantgard Pty Ltd
31a Copeland Rd
Beecroft NSW 2119
Australia
ABN: 99613466292

31 Oct. 2019

Australia's 2020 Cyber Security Strategy - Submission

To whom it may concern.

I am writing to express my views on the importance of active cyber defence in Australia's cyber security strategy.

My company Avantgard has focussed for the past three years on transplanting Israeli active cyber defence skills, capabilities and technologies into the Australian environment. We strongly support Maj Gen Marcus Thompson's publicly expressed views on the importance of active cyber defence measures, including actively working to identify intrusions and threats, for Australian civilian organisations and agencies. Australia is lagging USA and Israel in the adoption of active defence measures including cyber deception.

It is our view that Australia's 2020 Cyber Security Strategy should call out active cyber defence as a critical area for focus and resourcing in cyber defence plans.

1. Active cyber defence by Cyber Deception

Cyber deception is complex, but the basics can be summed up thus: While attack tools change, the attacker does not. Methodologies remain the same. Therefore, attackers are predictable. As attackers will search for our own information (credentials, shared, cookies) to understand how to build their operations, and we control that information -- we control them. By leaving a piece of data, a breadcrumb if you will, on an endpoint, the attacker can no longer rely on the data collected. You incept attackers straight through the OODA loop. They can no longer just enumerate through the data and pivot. For the first time, they must tread carefully. It's no longer about them needing to succeed only once. If they make a wrong move and follow a breadcrumb to a fully instrumented decoy machine -- they are done. The operation is blown, and their toolset has been taken.

Stuxnet had code in it which was 12 years old. Imagine yourself as the head of a threat actor organization. After 12 years of running successful intelligence operations, in one day -- your capability is destroyed. Assuming a threat actor runs 2500 operations a year for intelligence gathering, which in turn support more operations generating yet more intelligence, and of course your inability to launch new collection operations for a while, you are facing strategic damage.

This is the power of cyber deception. It changes the attackers' whole game plan. From budget to KPIs, they are now slower, and their overall economic cost is increased exponentially.

Over the past five years cyber deception has demonstrated the ability to detect national state attacks and the catch the same attacker across multiple targets using the same techniques. (attackers have not worked out how to avoid detection)

Cyber deception is proving to be an effective defence measure, however Australia lags USA, Israel and Europe in the adoption of cyber deception measures.

It is our view that Australia's 2020 Cyber Security Strategy should call out cyber deception as a critical area for focus and resourcing in cyber defence plans.

In support of this view I enclose a case study of the efficacy of a contemporary cyber deception solution in NATO cyber wargame exercises. In the interest of transparency, I advise that Avantgard Pty Ltd is the Australian representative of cyber deception specialist Cymmetria (cymmetria.com).

Should you require further information I can be contacted directly using the details below;

Sincerely,

[redacted]

Andrew Cox

CEO
Avantgard Pty Ltd
T: [redacted]
E:
31a Copeland Rd
Beecroft
NSW 2119
Australia