

AUSTRALIA'S 2020 CYBER SECURITY STRATEGY

Submission on the Government's discussion paper
by Ava Risk Group Limited



1st November 2019

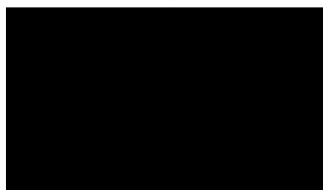
The Hon Peter Dutton MP
Minister for Home Affairs
Canberra

Dear Minister,

Ava Risk Group Limited appreciates the opportunity to provide this submission to the Australian Government in response to the call for views on the recently issued discussion paper for the proposed “Australia’s 2020 Cyber Security Strategy”.

We fully support the Government’s efforts to engage Australian industry on this important issue and would welcome further discussion to support all efforts to deliver this critical strategy document.

Yours faithfully,



Scott Basham
Group CEO



David Cronin
Chairman

TABLE OF CONTENTS

1. Introduction to Ava Risk Group Limited	3
2. Submission	4
a. What is your view on the cyber threat environment?	4
b. What threats should the government be focusing on?	6
i. Critical Communications Infrastructure	6
ii. Critical Infrastructure - Utilities	8
iii. Equipment Hardening & Certification	8
c. Do you agree with our understanding of who is responsible for managing cyber risks in the economy?	9
d. Do you think the way these responsibilities are currently allocated is right? What changes should we consider?	10
3. Ava Case Studies	11
i. Critical Military Data Network	11
ii. Critical Communications Infrastructure	12
iii. Critical Infrastructure - Nuclear Power Plant	12
iv. Banking System Continuity	13
Appendix - About Ava Group	14

1. INTRODUCTION TO AVA RISK GROUP LIMITED

Ava Risk Group Limited (Ava Group) is a market leader in the provision of risk management services and technologies. With a portfolio of security solutions including Future Fibre Technologies (FFT) and BQT Solutions (BQT), Ava Group is trusted by some of the most security conscious commercial, industrial, military and government customers in the world.

Ava Group offers a range of complementary solutions for the protection of critical infrastructure and high value assets including:

- FFT's fibre optic intrusion detection and location technology for perimeters, pipelines and data networks
- BQT's high security electro-mechanical locks, biometric and card access control, and
- Ava Global's secure international logistics and storage of high value assets and risk consultancy services.

Through decades of innovation, Ava Group continues to build on its comprehensive portfolio of premium security services and technologies for the most complex and demanding markets.

With an experienced team spread across six continents, Ava Group provides market and industry expertise directly to its customers. With its technology protecting thousands of sites, Ava Group has a proven track record in delivering first class risk solutions that surpass the expectations of its customers, end users and partners.

2. SUBMISSION

a. What is your view on the cyber threat environment?

Rapid technological innovation, global investments by foreign firms and a clear agenda by various state sponsored actors to engage in cyber activities have all created a complex and evolving threat environment. This has led a situation, we believe, that is beyond what was anticipated in the Government's *2016 Cyber Security Strategy* and exceeds the response capabilities of many departments, corporations and Australian businesses.

Evolving technologies such as 5G, IoT, Artificial Intelligence and Quantum Computing are expected to deliver massive benefits to society, while at the same time delivering a significant capability for malicious activity that is expanding our risk environment. These risks can impact individuals at a personal level through privacy breaches and identity theft, obstruct businesses at an operational level through denials of service and industrial espionage, and disrupt governments at a strategic level through cyberattacks on national critical infrastructure.

On a daily basis, we see examples in the media of the cybersecurity threat environment increasing in sophistication. At the same time, our national critical infrastructure is becoming more exposed as it continues to be digitised, integrated and networked. Our ever-increasing reliance on specialist software, computer systems and other related IT platforms to operate, monitor and maintain these vital national assets and capabilities exposes our society to new risks

Attacks on Australia's power and water utilities, telecommunications networks, major transport hubs or financial services and banking infrastructure could have dramatic and major economic and safety consequences for our society. Globally, we continue to see examples of malicious attacks on such critical infrastructure from both individual and groups of cyber "hackers" as well as highly organised state sponsored actors.

The vulnerabilities of our critical infrastructure not only include cyber-attacks that breach privacy data or steal secret intelligence, but sensitive information that may be in storage or running over IT data networks. Ava Group believes that vulnerabilities also extend to a current inability to detect and deter malicious activity through physical access to vital IT data networks and critical infrastructure in the first place. It is a well-known fact that critical communications carried on fibre optic cables can be tapped by various means if the cables are able to be physically accessed.

The disruption or theft of data while potentially resulting in a financial, reputational or commercial loss to its owner, does not necessarily result in catastrophic failures and widespread impacts to the population. Interruption to the utilities network, by remote denial of service attacks or direct attack through communication systems, could cause power grids to collapse and have major impacts during extreme hot or cold weather (we already experience this regularly when utilities fail). Similarly, the loss or disruption of Air Traffic Control communications with aircraft on a large scale could potentially cause a significant loss of life.

As a subject matter expert on protecting physical data networks from intrusion and attacks, Ava Group has been successfully addressing the market needs for solutions to monitor unauthorised access and tampering of physical data network infrastructure in high security facilities and critical assets and facilities for more than 15 years. For example, you may be aware that Ava Group has already deployed its FFT physical network protection solutions for critical military data networks across the United States and has been actively protecting key data network infrastructure between a number of very sensitive and key strategic Department of Defence sites in Australia for more than a decade. Very recently, after exhaustive competitive benchmark testing by the Indian Ministry of Defence, Ava Group's FFT Secure Link product was selected to protect and provide real-time monitoring of over 40,000km of military fibre optic data network infrastructure deployed across the length and breadth of India.

b. What threats should the Government be focusing on?

Ava Group recommends that the Government broaden the scope of the proposed *2020 Cyber Security Strategy* to encompass the evolving physical threats discussed in this response. Key areas to consider are as follows:

i. Critical Communications Infrastructure

Fibre optic communications are widely deployed in government, military and commercial telecommunications networks. It is possible for relatively unskilled individuals to gain access to these cables without the knowledge of the infrastructure owner. Often done with relatively simple and easily procured equipment, these individuals are able to disrupt or tap into networks at the fibre optic level to monitor traffic without raising the alarm or leaving a meaningful evidence trail.

While encryption is obviously a significant deterrent to this activity, not every piece of data on a network is necessarily encrypted. Even if particular data is encrypted, with evolving technologies and computing power, current encryption standards may not be sufficient in the future, especially if it is possible for large dataset samples to be extracted without the data infrastructure owner's knowledge for decryption at a later time and place.

Government departments, intelligence agencies, military services, financial institutions, power and water utilities and commercial businesses with sensitive and valuable intellectual property should all have stringent measures in place to mitigate both physical and cyber threats to their networks. Yet often many appear oblivious to the danger of leaving even a closed fibre network unprotected. As such, critical infrastructure owners can potentially be exposed to the threat of state-on-state action, terrorism or industrial espionage.

Ava Group believes that the Government needs to clearly define and enforce responsibility for protecting such critical infrastructure. Whether, it is Government owned infrastructure, such as the ICON network, or non-Government owned infrastructure, like Sydney Airport or the Australian Securities Exchange, a suitable level of protection needs to be implemented.

In the case that the Government owns the infrastructure, then Ava Group contends that everything possible should be done to protect those assets from intrusion and unauthorised access. This means that the Government must fund those appropriate measures.

In August 2019, the Department of Defence in Canberra suffered from major IT outages that impacted some 60,000 Defence staff for three days. Allegedly, this outage was caused by a backhoe operator, who at some time over the course of conducting earthworks over a weekend, inadvertently cut the network cable that feeds data to and from the Defence sites in question. This event subsequently went unreported for several days. As there was no real-time monitoring of the data network infrastructure, the disruption was neither identified as the immediate cause of the outage, nor was the precise location identified so that repairs could be effected until (presumably) a physical search of the entire IT operating environment was undertaken and the root cause was identified.

Ava Group's FFT Secure Link technology has long been deployed with customers like Defence, on some very select data network linkages between certain strategic communications sites. This technology would have identified the digging activity at the precise location to within a few metres, automatically alerting the appropriate agencies prior to any damage to the cable and enabling an immediate response to the situation.

ii. Critical Infrastructure - Utilities

Attacks on Australia's utilities would have significant economic and physical safety impacts for the country. Globally, we continue to see regular examples of malicious attacks on critical infrastructure from both cyber based criminals and state sponsored actors. These events are not limited to remote cyber intrusions and include physical attacks on communications and power infrastructure.

Threats to the operations of utilities could include both cyber-attacks and potentially physical attacks by actors looking to disrupt our day to day security. Appropriate measures to counter threats from physical attack should be considered.

The protection of critical infrastructure must include a wholistic approach of both cyber security and physical security. This approach has long been adopted by regulatory bodies internationally, such as the USA CFATS and NERC regulations which explicitly incorporate physical security requirements within their standards. While it can be argued not all of these regulatory environments have been entirely successful from day one, it is clear that in developing these frameworks, a broad range of threats were considered.

iii. Equipment Hardening & Certification

Cyber hardening of technologies is essential to combating the threat environment.

Government can play a key role in this area via the promotion and implementation of appropriate standards. It can also drive market changes in a commercial sense through demanding certain specific requirements of technology products during the normal course of the Government procurement process.

Federal and State Governments should collaborate to present a unified policy for the purchase of IT, security system and other related technology to a set of Australian Standards, similar or the same as certain international standards such as the US National Institute of Standards and Technology (NIST) or Underwriters Laboratories (UL), which would require

equipment to be cyber hardened. This could also be extended to commercial entities which are deemed critical to Australia's national security and economic interest.

This approach will drive commercial decisions for local manufacturers to make compliant products here in Australia, which will also help to develop local anti-sovereign cybersecurity "risk mitigation" capabilities which will also help to develop the local Cybersecurity Industry - in the same way that we have a local Defence Industry to support Defence projects around the country. Government should similarly mandate that any new projects they initiate must have a percentage of local Cybersecurity "content" in the same way they might stipulate for a new Airforce plane project or Navy shipbuilding project.

c. **Do you agree with our understanding of who is responsible for managing cyber risks in the economy?**

Ava Group agrees with the observation made in the discussion paper, that in the current regulatory environment, end-users carry a significant portion of the risk of cyber protection, and that Government currently has a limited role in protecting a large number of systems critical to our way of life.

Furthermore, as businesses are only required to self-report on significant compromises of personal information, it would seem reasonable to suspect that there is an increased likelihood that non-personal data related breaches or otherwise significant network hacking incidents which may have the potential to threaten our national security or national economy go under reported. Typically, it is only due to the public visibility of some of these major outages that they come to light. How many others have occurred that are significant and out of sight?

The Australian Government's *Security of Critical Infrastructure Act 2018* which came in to force on 11 July 2018 was a step forward in establishing a framework to take a leading role in the protection of our critical infrastructure assets. While the scope of the Act appears to provide for

discretionary powers to direct the owner or operator to remedy security risks, it is unclear to what standards and requirements should be adhered to.

Ava Group contends that this is a key area of future endeavor for the Government to firm up the understanding of the standards and requirements that critical infrastructure operators need to meet to deliver better outcomes in physical and cyber security.

d. Do you think the way these responsibilities are currently allocated is right? What changes should we consider?

End users need to take responsibility for the management of their own security. However, Government has an important role in establishing and maintaining the regulatory framework and standards which can cater for the diversity of end user requirements and skills.

To assist end users to improve security, Ava Group suggests that the Government considers the following possible activities or changes:

- The Government owns and manages an extensive communications facility, supporting many departments. Standards and manuals such as the *Australian Government Information Security Manual* provides valuable recommendations on establishing and managing IT systems. Given the sensitive nature of such communications, Ava Group recommends the review and update of manuals to include more focus on the physical protection of these critical communications links.
- While the Government's *Security of Critical Infrastructure Act 2018* provides a mechanism for information gathering powers, and Ministerial directions power, Ava Group believes that the Act should enforce more rigorous requirements to report threat incidents (both cyber and physical) as well as being more prescriptive on the standards and requirements for physical security systems to be employed by critical infrastructure.
- Equipment utilised in the core networks and access points (e.g. IoT) can introduce weaknesses in the security of critical infrastructure. Cyber hardening to certain standards (NIST or UL) should be a mandatory requirement in the case of critical infrastructure. Ava Group

recommends that the Government should enforce this requirement on manufacturers through the greater use of its procurement power, as well as expanded requirements defined via the *Security of Critical Infrastructure Act 2018*.

- While Australia's capabilities may be limited by our access to resources, our adversaries are highly skilled and well-funded. The Government should consider a framework where it can act, in real time, against serious cyber and physical threats against critical infrastructure that is owned and managed by commercial and state based enterprises.

3. AVA CASE STUDIES

The following case studies are provided to provide a context of potential data network protection capabilities for further consideration by the Government:

i. Critical Military Data Network

A large military site including operations control room, equipment staging sites, security response teams and several critical launching facilities needed to be able to detect and respond to any unauthorised access to its fibre optic network in under three minutes. The challenge was that all secure communications was through the site's underground fibre optic network which had dozens of access points that were only protected by manhole covers.

The military group had experience with fibre optic cable intrusion techniques and selected Ava Group's FFT Secure Link data network protection solution as met all required security performance criteria.

1. FFT Secure Link can monitor over 40km of fibre and therefore able to monitor required distances with a single system.
2. FFT Secure Link could provide advance warning of any attempted access to the fibre network, as well as the precise location, well in advance of the intruder gaining access to the sensitive data flow - allowing a response action to occur before any impact on operations could occur.

3. FFT Secure Link had no impact on the operation of the existing network as it did not operate on the confidential data and therefore did not impact data latency or data throughput.

ii. Critical Communications Infrastructure

Submarine communication cables are most exposed to interference near the onshore landing station where the depth of water and depth of burial provide limited protection from deliberate access.

A government agency required monitoring of its critical submarine cable from the operations rooms located near the landing station through to the first offshore seabed infrastructure point. Sensitive defense related data was being passed through the fibre cable, which could not be physically protected by any other method.

FFT Secure Link was able to provide constant situation awareness of activity on the cable and early warning of any attempts to access the cable and compromise the data by tapping or restricting the data flow. The early warning, and location information, was integrated into the operational protocols for the site.

iii. Critical Infrastructure - Nuclear Power Plant

A newly constructed Nuclear Power Plant required protection of its perimeter from intrusion, but also required protection of internal data communications from the control room to all facilities within the site, including the reactors. The site was subject to high temperature extremes and dust storms.

FFT's Aura Ai-2 and Secure Fence fibre optic solutions could provide reliable early warning of attempts to intrude the perimeter fences, as well as deal with the significant environmental challenges that would defeat other fence mounted sensor systems. In addition, FFT Secure Link was able to monitor all internal critical internal fiber optic links for any attempt of interference, including both accidental (maintenance) or hostile sources.

1. Ava Group's FFT solutions were able to monitor both perimeter and the communications network with only a few systems.
2. FFT Aura Ai-2 and Secure Fence provide advance warning of any attempted access to either the perimeter or fibre network, as well as the precise location, in advance of any impact to the operation of the facility.
3. Ava Group's FFT solutions have no impact on the operation of the existing network as it does not operate on the control data, and therefore, did not impact data latency or data throughput.

iv. Banking System Continuity

An international bank had its trading, operations rooms and a data centre spread over several different floors in a multi-story city skyscraper. Other building tenants also leased floors between the trading and operations floors of the bank and the data center. Communication cables ran through shared services ducts between all the floors of the building. However, the bank had no ability to physically separate their data cables to protect their confidential data communications.

Ava Group was able to install its FFT Secure Link solution on a single fibre optic cable which then provided an alert, and the location, of any activity within the bank's network.

APPENDIX



About Ava Group

Ava Risk Group Limited (Ava Group) is a market leader of risk management services and technologies, trusted by some of the most security conscious commercial, industrial, military and government customers in the world.

Ava Group offers a range of complementary solutions including:

- › intrusion detection and location for perimeters, pipelines and data networks.
- › electro-mechanical locks, biometric and card access control.
- › secure international logistics and storage of high value assets, and risk consultancy services.

Through decades of innovation, Ava Group continues to build on its comprehensive portfolio of premium security services and technologies for the most complex and demanding markets.

With an experienced team spread across six continents, Ava Group provides market and industry expertise directly to its customers. With its technology protecting thousands of sites, Ava Group is proven to deliver first class risk solutions that surpass the expectations of its customers, end users and partners.



Operating across two divisions, Ava Group brings together three highly compatible security related entities (Future Fibre Technologies, BQT Solutions and Ava Global Logistics), each with world leading technology, services and exceptional people.

Technology Division

Future Fibre Technologies (FFT) manufactures a complete portfolio of fibre optic intrusion detection and location products for the protection of high value assets and critical infrastructure.

BQT Solutions (BQT) is a specialist in the development, manufacture and supply of high quality, high security card and biometric readers, electromechanical locks and related electronic security products.

Services Division

Ava Global Logistics provides secure international logistics of high value assets on a fully insured door-to-door basis. This includes armoured vehicle collection and delivery at origin and destination, secure storage, commercial and chartered air and sea freight and customs brokerage services.

Locations

