Defence White Paper 2015 Submission
A National Cyber Resilience Blueprint
Tim Scully*

Executive Summary

Governments world-wide have struggled to address the cyber threat to public and private sectors. They have applied traditional policy and capability development measures to the problem with no avail. The 2015 Defence White Paper will perpetuate this failure if it does not treat the threat as one that transcends traditional Defence policy and capability settings. This submission recommends that the White Paper initiates a tried but true, expansive model that moves beyond the usual interagency and departmental remits to develop a National Cyber Resilience Blueprint.

A Defence White Paper cannot, by itself, articulate the long-term policy settings and capability needed to achieve national cyber resilience. But it can lead the charge.

Australia has so tightly embraced the Internet that it is now indispensable to the conduct of public and private business at all levels – individual, small, medium and large. It will remain critical to our economic prosperity and, therefore, to our national security.

But this irrevocable online dependency also makes us highly vulnerable to malicious actors and other digital catastrophes. The Defence White Paper 2015 will not be able to address this complex vulnerability as it can only argue the case for ‘Defence’ policy settings and capability with token observance of whole-of-nation needs. And the cyber threat will pale in the shadow of grander, traditional defence challenges to be considered in the White Paper, even though it is intrinsic to all of those challenges.

Any public discussion of ‘national security’ inexorably gravitates towards military and intelligence cyber operations and those departments most interested in them, such as the Department of Defence and the Attorney-General’s Departments. Consequently, the other half of our national interest, our economic prosperity, is sidelined along with key stakeholders including, for example, the Departments of Communications, Industry and Foreign Affairs and Trade, who are deeply engaged in growing and sustaining our economy.

Significantly, our industry stakeholders are also sidelined. They are consigned to the role of product and service providers to Government rather than being engaged as equally capable, if not leading, partners in achieving national cyber resilience. Academic and research institutes are also sidelined as bit players rather than partners as they struggle to gain relevance.

The 2009 Defence White Paper first addressed cyber operations as a Defence capability and spawned the Cyber Security Operations Centre (CSOC). This was laudable, but subsequent funding was allocated to Defence alone, leaving other Government stakeholders bereft of resources to develop their equally important cyber resilience
roles. Not surprisingly, the 2009 White Paper focussed on ‘Defence’ cyber operations capabilities, rather than on national, strategic policy settings and capabilities.

The 2013 Defence White Paper heralded the yet-to-appear Australian Cyber Security Centre (ACSC) – with no additional funding – that will draw in essentially the same Government players, but will add some industry players to the mix. Apart from a move to the new ASIO building, the only tangible difference between the CSOC and ACSC – as far as publicly available information goes – appears to be the addition of these industry stakeholders. Yet once again, without funding allocated, even this may turn out to be a pipe dream.

Many questions are unanswered about these industry players in the ACSC. How will they be selected to join this elite, classified enclave? What will their role be? Will it be ‘invitation only’ for select companies who can afford or already have security-cleared people and who also have an entrenched military, operational mindset? Will all industry users of cyber security services be represented, not just owners and operators of critical infrastructure? And how will industry-at-large gain confidence in what remains a reticent, classified, Defence-dominated centre?

This domination by Defence in both leadership and resources in this ‘new’ arrangement will likely perpetuate the status quo, thereby leaving efforts to stimulate national cyber resilience in the doldrums while our economy continues to be exploited by malicious actors whose pace of innovation is faster than that of our cyber defenders.

The cyber domain comprises two main capability areas, namely offensive and defensive measures (cyber “effects” is also considered by some commentators to be a separate capability set). While offensive measures will not get much airing in the unclassified version of the White Paper, the defensive measures should. The problem is that cyber resilience is clearly not just the responsibility of Defence, so the required policy settings and capabilities extend beyond the remit of a Defence White Paper.

Defence’s cyber security role and functions, through the Australian Signals Directorate (ASD), should not be over-estimated. ASD’s cyber operations functions include offensive capabilities, but its defensive responsibilities are restricted by law to providing material, advice and assistance for the protection of government information and networks – it can help industry, but only through other government departments, and it still cannot provide sustained assistance to government let alone industry. And it is not clear if the establishment of the ACSC will allow ASD’s technical capabilities to be brought to bear more broadly upon industry generally.

Not to diminish ASD’s superb track record of ‘making a difference’ behind Defence’s firewalled zones, it is by no means the master of the cyber security/resilience domain. Industry has a significant and rapidly growing capability. What’s more, ASD is an operational capability with a unique capacity to build a comprehensive picture of the threat we face. But cyber policy and coordination, responsibility for which rests with the Department of Prime Minister and Cabinet, seems to be in stasis. The one and only attempt at a Cyber Security White Paper fundamentally failed to produce any tangible outcomes and left a leadership void in this domain. It must also be recognised that ASD is first and foremost an intelligence agency, a fact that circumscribes its ability and
desire to engage more fully in the discourse on national cyber resilience across all sectors. It needs to embrace cultural change if it is to improve its engagement in the discourse on national cyber resilience.

The Defence Science and Technology Organisation (DSTO) is increasing its efforts in cyber security capability development, and the Chief Defence Scientist’s intent to engage more deeply with industry is a positive development, but I would contend that DSTO has yet to realise the full extent of its role as the national S&T security requirements coordinator – it still focuses mainly on the Australian Defence Organisation’s needs.

In the absence of any other suitable instrument, including the 2009 National Cyber Security Strategy that lacks innovation and is now irrelevant, the Defence White Paper could be the catalyst for a National Cyber Resilience Blueprint. This would be developed by a combined government-industry-academia group using the Cooperative Research Centre (CRC) Program as its business model - and it would not necessarily be led by a Government official. The Blueprint would dissect and scrutinise the roles, functions and structure of our existing national cyber security institutions and infrastructure, including policy and regulatory frameworks. It would lay the foundations for a world-leading, tripartite collaboration to build cyber resilience for all Australian interests. And it would do so using a tried but true, expansive model that moves beyond the usual interagency and departmental remits.

My proposition is that the Defence White Paper should recommend using the CRC model to develop the national policy settings and capability requirements for four reasons.

First, given the CRC Program’s proven, 25 year track record of success, its independent, collaborative and transformative problem-solving model is needed to bring together the three tribes of government, industry and academia to create an innovative Blueprint to address the cyber threat as a national hazard. The Blueprint would capitalise on the Government’s focus on the public good, industry’s necessity to be innovative and profitable, and academia’s raison d’être to research and develop real solutions to real problems.

Second, it is generally assumed, particularly in Government, that the current government policy making and operational (i.e. implementation) architecture is capable of dealing with the cyber threat to our national security and economic viability. However, for over ten years that architecture has consistently failed to develop effective policy and capability for national cyber resilience (the fact that it is still referred to as ‘security’ underscores this point). This assumption should be vigorously and independently tested.

Third, the CRC Program’s emphasis on ‘transformative’ problem solving is critical because we need to look at cyber resilience with fresh, innovative eyes without the inherent constraints of government policy-making bureaucracy or the fickle ‘bottom line’ focus of industry. Nor should it reflexively draw from international models; they have failed too. The CRC model is able to overcome such inherent bias and constraints to discover ‘what is possible’.
Fourth, an independent review could help articulate who all the stakeholders are in this domain and where responsibility and accountability should lie. In other words, it could overcome the prevailing learned helplessness in dealing with the matter and firmly embed the notion that it is not just the Government which is accountable and responsible for cyber resilience.

The Government is currently reviewing the CRC Program (the Miles Review) and it is possible the Program will be subsumed into a new “Industry Growth Centre” model. Nonetheless, the key elements that have driven the success of the CRC model, especially industry’s commitment and collaboration with research bodies to solve real problems, will very likely be retained.

The 2015 Defence White Paper’s role will not be limited to cyber support for military operations alone; it will also cover ASD’s responsibility to provide advice and assistance to government department and agencies. But that’s about as far as it can go given its scope. To make a serious impact on national cyber resilience, the Defence White Paper should promote the establishment of an independent, cooperative body to review existing national arrangements and develop the whole-of-nation policy settings and capability requirements that we are currently lacking. Its product would be a National Cyber Resilience Blueprint. All players with skin in the game – industry, academia and government - should play an equal role and share the burden to develop the Blueprint. The 2015 Defence White Paper could be the catalyst for this innovation.

I provide my consent for the Department of Defence to publish this paper in its entirety.

**Tim Scully**  
October 2014

---

* Tim Scully is a senior leader with over 30 years experience building and leading operational responses to national and international intelligence and security challenges. He is the Chairman of the Data to Decisions Cooperative Research Centre and a Director of Stoneleigh Consulting. Tim was previously CEO Stratsec & Head of Cyber Security Capability at BAE Systems Australia. In government, he served as the inaugural head of Defence’s Cyber Security Operations Centre; Head of the Defence Security Authority; Assistant Secretary Support to Military Operations; and Assistant Secretary Analysis and Production. He remains a strong contributor to protective security policy development and thought leadership, and is a strong advocate for improved cyber security awareness among Australian industry leaders. Tim is also a PhD candidate at the Strategic and Defence Studies Centre, Australian National University.