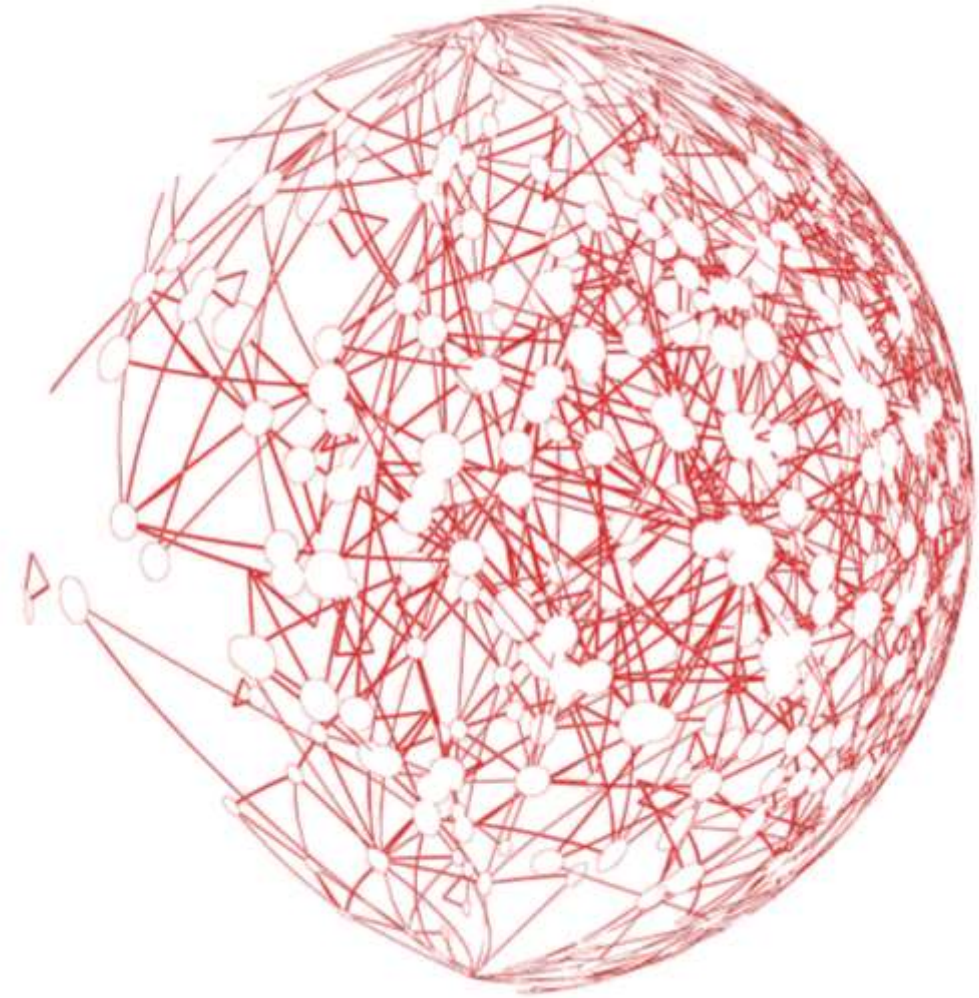

NATIONAL CYBER RESILIENCE

Is Australia ready for a computer COVID-19?

SENATOR THE HON KRISTINA KENEALLY
SHADOW MINISTER FOR HOME AFFAIRS

TIM WATTS MP
SHADOW ASSISTANT MINISTER FOR CYBER SECURITY

INTRODUCTION

The global novel coronavirus pandemic has given new focus to the importance of national resilience - our ability to respond to adverse external shocks, to prepare for risks, to minimise human and economic losses, and to bounce back from harm.

Today, cyber-attacks threaten our national resilience. Self-perpetuating malware spread in a way that is analogous to a biological virus and can do enormous damage to connected systems in short periods of time. As we have learnt first-hand in recent months, our interdependent modern society and economy rely heavily on the availability of essential services like healthcare, childcare, retail and transport logistics to function. How cyber resilient are the computer systems of our schools, our childcare centres, our GP clinics, our logistics networks, our local governments and the services they provide? How would we cope if a worm delivered malware that simultaneously brought down large numbers of these organisations for months? COVID-19 has given us a taste of how interdependent these essential services are and what our society and economy would look like in this world. We now need to confront the cyber resilience of these interconnected organisations.

A widespread cyber incident that simultaneously affects large numbers of organisations in this way is not a hypothetical concern. The WannaCry ransomware worm, developed by North Korea to generate hard currency for its heavily sanctioned economy through cybercrime, infected hundreds of thousands of computers in more than 150 countries and caused $4-8 billion of losses. Most concerningly, the network of Britain's public health-care system — the National Health Service (NHS) — was corrupted during the attack, causing panic and delaying surgeries.

Soon after, Russia deployed the NotPetya malware worm against critical infrastructure in Ukraine. It crippled computer systems ranging from radiation monitors at Chernobyl Nuclear Power Plant, Ukraine's national bank, retail banks, a state power company, the postal service, the largest airport and public transport systems. Ukrainians were left unable to withdraw money from ATMs, use checkouts at supermarkets or trust that their letters would arrive at the correct destinations. This malware's effects went far beyond the intended Ukrainian target though and quickly spread around the world, crippling the systems of hundreds of businesses and governments for months. The total costs of the attacks have been estimated to be around US$10 billion.

It could have been much worse. A recent report commission by Lloyds as part of its Cyber Risk Management Project has warned that a *'global infection by contagious malware'* could cause up to US$193 billion of economic damage worldwide.

With the renewed focus on national resilience in the wake of the novel corona virus pandemic, it is timely to ask, *"Would Australia be prepared for a global malware pandemic? A computer COVID-19?"*

There's reason to be concerned with the status quo. As the former head of ASIO and current chair of the Australian Cyber Security Cooperative Research Centre, David Irvine warned late last year:

> *'Ultimately, we're not there.. we need.. to have much more effort both by the government and the private sector and individuals into developing what I'll call* ***national cyber resilience*** *to a far greater level than we have now.'*

This discussion paper explores some of the key dimensions of national cyber resilience, and how Australia stacks up. While not committing to policy positions, it points to the issues and potential interventions that Australian governments should be investigating now, to ensure that Australia is prepared for the cyber threats of the future.

THE CYBER THREAT ENVIRONMENT IN AUSTRALIA

Cyber threats are a ubiquitous part of modern life. Almost one in three Australians were victims of cyber-crime in 2018. The Australian Cyber Security Centre receives a report of cyber-crime every ten minutes. The Office of the Australian Information Commissioner received 230 notifications of malicious cyber-attacks that resulted in data breaches in the second half of 2019 (a 19.8% increase from the first half of 2019).

These attacks are a significant cost to the Australian economy and our society. The Australian Criminal Intelligence Commission estimates that cyber-crime costs the Australian economy up to $1 billion per annum in direct costs alone and up to $17 billion in indirect costs. Australian security company, Senetas, has estimated that in 2019, an average data breach cost the affected company US$3.92m. It's a worldwide trend; the World Economic Forum predicts that cyber-crime could cost the global economy US$6 trillion in 2021.

Cyber Crime in the Time of Coronavirus

Cyber criminals exploit anxiety and fear when designing cyber-attacks. During the COVID-19 crisis we have seen COVID-themed cyber crime become a common tactic across the world. In a recent 1-week period Google blocked an average of 18 million malware emails and 240 million spam emails related to COVID-19 every day.

With millions of people working from home and accessing essential services (government benefits, telehealth, online learning) via unmanaged, personal devices, the number of people vulnerable to attack has also dramatically increased. We're yet to discover the full impact, but the ACCC's ScamWatch website has reported that Australians have lost $385,510 more in March 2020 than they did in February.

CYBER RESILIENCE IN AUSTRALIA

The ability of Australian individuals and organisations to defend themselves from cyber threats is currently highly variable.

While some organisations, like our banks and national security agencies are generally relatively capable of protecting themselves against most cyber threats, the bulk of Australian organisations do not have the time, resources or capability to adequately protect themselves from even the most basic attacks.

Currently, there are particular vulnerabilities within resource constrained small businesses and government entities.

THE CYBER RESILIENCE OF AUSTRALIAN SMALL BUSINESSES

The frequency and severity of cyber incidents on Australian small business is increasing. One in four Australian small businesses were victims of cyber-crime in 2017 (up from one in five in 2016). Among victims of cyber-crime who lost data in the attacks, the financial losses of these incidents increased to an average of $10,299 in 2017 (up from $6,591 in 2016).

This increasing victimisation mirrors low levels of cyber security capability among Australian SMEs. A 2017 MYOB survey found that 87% of Australian SMEs reported believing that their business was safe from cyber-attacks because they use antivirus software alone.

In a similar vein, Chubb's 2019 SME Cyber Preparedness report found that only 43% of Australian SMEs were investing in better cyber security training for their staff, only 29% checked employee compliance with cyber security policies and only 20% were implementing internationally recognised information security standards. Worryingly, only 49% of Australian SMEs do not have a data breach response plan, significantly impacting their ability to respond to a cyber incident. These findings echo a 2017 Norton SME survey found that while 37% of Australian SMEs didn't believe they could operate for more than a week without access to critical information stored on their IT systems, only 32% of businesses were continuously backing up their data.

The results of the ACSC Small Business Survey, launched in June 2019, will provide further important insight into the cyber resilience of Australian SMEs when it is released by government.

CYBER RESILIENCE IN COMMONWEALTH GOVERNMENT ENTITIES

A further, concerning example of uneven cyber resilience is the Commonwealth government itself.

Despite the Australian Signals Directorate's 'Top Four' strategies to mitigate cyber security incidents being made mandatory in April 2013, by late 2019 it was reported that nearly four in ten Australian government entities had still failed to implement these basic cyber security measures (61.7% compliance) six years later. A succession of ANAO reviews have found continuing failures of Commonwealth agencies to implement basic cyber resilience measures without consequence or accountability.

The Commonwealth Cyber Security Posture in 2019 report confirmed that implementation of the ASD's 'Top Four' cyber security mitigations *'remains at low levels across the Australian Government'*. Extraordinarily, of the 25 Commonwealth entities that were prioritised for improvement as part of the Morrison government's 'Cyber Uplift', none were assessed by the

ACSC to have achieved their recommended cyber security maturity level. As a result, the report concluded that *'these entities are vulnerable to current cyber threats targeting the Australian government'.*

CYBER SECURITY SKILLS

An underlying factor to Australia's uneven cyber resilience is a persistent and growing shortage of cyber security professionals.

A 2016 Australian Information Security Association survey found that 78% of respondents agreed there was a shortage of qualified cyber security workers for available positions in Australia. The survey also found that these shortages were most acute across local, state and federal government and in public services like healthcare and education.

In 2018, AustCyber (the Australian Cyber Security Growth Network) estimated that there were currently 2300 fewer cyber security professionals in Australia than required by the industry. It further forecast that increasing demand for cyber security skills would see the industry require nearly 17,000 additional cyber security professionals by 2026. Austcyber expects that Australian cyber security graduates will quadruple by 2026, but even this level of growth would fall short of the growing requirements of industry. While we saw a flurry of new cyber security courses being launched at Australian universities and TAFEs around 2016, it's unclear how many new graduates have been produced as a result. Just 14% of respondents to a 2019 ISACA Technology Landscape survey of cyber security professionals believed that we would bridge the skills shortage in our region in the next decade. 37% believed the skills shortage would worsen in our region compared to other parts of the globe.

In the past, Australia has relied on migration to fill this skills shortage. But the COVID-19 crisis highlights the limitations of relying on global supply chains during a crisis. The shortage of cyber security skills is a global issue. According to the World Economic Forum there is a current global cyber skills gap of 4 million. According to a report by cyber security certification firm ICS2 the global cyber security skills shortage is as much as 4.07m professionals and the total workforce needs to increase by 145% to meet current requirements.

A global crisis means global demand for essential goods and services, as we're seeing now with awful international shortages of respirators and personal protective equipment for medics. We've seen major cyber incidents have global effects before. The 2012 'Shamoon' wiper attacks on Saudi Aramco forced the company to urgently replace 50,000 hard drives, drying up world supply for the better part of six months. A global cyber incident that hit large numbers of organisations around the world wouldn't just effect hardware supplies though, we would see a similar international competition for human capital - cyber security incident responders. In such a contest, Australia would start from a position of acute disadvantage.

NATIONAL CYBER RESILIENCE – WE'RE NOT THERE YET

To date, Australian cyber security strategy has largely been framed through the prism of defence and national security. Focused on addressing the most sophisticated threats to the most sensitive organisations. At protecting sensitive targets within government from the significant challenge of well-resourced, persistent state backed adversaries. Focused on developing offensive cyber capabilities to deter attacks on valuable Australian targets. Focused on protecting critical infrastructure from a 'cyber Pearl Harbour'. This is a major challenge and while there is still a lot of work to be done to ensure our critical infrastructure is secured, the technical capabilities Australia has developed in government in this space compare well with the best in the world.

However, when it comes to building cyber security capability outside the defence and national security sphere, Australia's track record is much patchier. Responsibility for cyber security is fragmented within the current government. Home Affairs currently retains responsibility for policy making. The Australian Signals Directorate, and the Australian Cyber Security Centre that sits within it, is home to the bulk of Australia's technical cyber security expertise and sits within the Defence portfolio. While there are excellent technical skills and expertise within these agencies, they lack the resources, experience and perspective needed to engage with the broader Australian business community, particularly the small business sector. There is no dedicated Ministerial role to liaise between government and the private sector.

Government policy initiatives designed to engage the Australian business community to improve their cyber resilience have failed to gain traction. Many of the business and community facing initiatives of the 2016 Commonwealth Cyber Security Strategy have now fallen by the wayside. Despite being intended as a 'baseline' for measuring cyber security in corporate Australia, the 2017 ASX 100 Cyber Health Check ended up being a one off. It's the same story for the promised annual cybersecurity meetings between leaders in government, the private sector and the research community chaired by the Prime Minister–we haven't seen one since 2017 . The Joint Cyber Security Centres, established in capital cities between 2017 and 2018 to facilitate collaboration between government and business, are widely seen to have failed in this objective. Aside from a few start ups, small businesses have next to no presence in these centres.

Perhaps the best example of the disconnect between Australian cyber security policy makers and small business was the $10 million 'Cyber Security Small Business Program' which offered small businesses $2100 to cover half the cost of a Council of Registered Ethical Security Testers (CREST) accredited cyber security health check. Given that the bulk of small businesses spend less than $500 a year on cyber security in total, it's not surprising that only 35 small businesses took the government up on the offer of spending $2100 on testing alone (somewhat less than the 5400 checks the government forecast would occur). Only 181 Australian small businesses undertook the free, self-assessed health check offered under the program.

The current paradigm of Australian cyber security policy is not succeeding in engaging organisations and individuals outside the traditional defence and security community.

To build national cyber resilience in Australia, we need to consider new approaches.

Image by Abraham Pena, used under Creative Commons Attribution 4.0 International License via the Hewlett Foundation Cybersecurity Visuals Challenge

NEW APPROACHES TO BUILDING NATIONAL CYBER RESILIENCE

Strengthening Australia's national cyber resilience requires re-conceptualising the role of government in cyber security policy. Just as public health experts recognise that there are collective benefits from improving the overall health of a population, so too do government cyber security authorities need to recognise the collective benefits of interventions to lift the baseline cyber security capability throughout a nation. Hardening up the cyber security of vulnerable Australian organisations will encourage opportunistic cyber criminals to look elsewhere for targets. Lifting the overall level of cyber hygiene on the Australian internet will reduce the ability of malware to spread between Australian organisations.

Reflected Phishing

A common technique used by commodity attack phishers that many people will have seen themselves is known as 'reflected phishing'. Once attackers secure access to an initial email account (through phished credentials or credential stuffing), the contacts list of that compromised account is then used to phish their contacts. Because they come from a legitimate email address from someone they know, these reflected attacks attract a higher click rate than bulk spammed attacks. In this context, preventing the original attack would

The Conservative UK government conceptualised cybersecurity in this way in 2016. As the CEO of the United Kingdom National Cyber Security Centre (NCSC), Ciaran Martin, set out in a 2019 speech, in a modern economy *'there are some market failures where the Government needs to intervene if there is to be an acceptable level of national cyber security hygiene.'* As a result, in order to promote national cyber resilience, Martin argued that government needs to make *'more fundamental interventions'* to *'improve the digital homeland'*.

The Director of the UK's Government Communications Headquarters (GCHQ), Jeremy Fleming argued in a speech in the same year that the UK aims to make its cyber security strategy *'more citizen facing and more citizen relevant.'* Fleming explained how the NCSC sought to *'take the burden of cyber security away from the individual'* by *'expand(ing) the cyber security ecosystem.. taking a bold interventionist approach to involve a wider set of stakeholders in protecting the nation's cyber security'*. Or as the Technical Director of the NCSC, Ian Levy memorably put it *'getting off our backsides and doing something.'*

One of the principal tools the UK government has used to implement this interventionist strategy is what it calls Active Cyber Defence (ACD).

ACTIVE CYBER DEFENCE

The UK's Active Cyber Defence framework is designed to *"take away most of the harm from most of the people most of the time."* The NCSC seeks to identify the most common threats facing UK government entities, and UK citizens interacting with them, and to develop scalable, automated interventions to mitigate those threats. In the words of Jeremy Fleming, its goal is *'to make the Internet automatically safer for people to use.'*

Since it was adopted in 2016, the NCSC claims that its Active Cyber Defence program has prevented millions of cyber attacks.

Active Cyber Defence isn't a silver bullet. It can't prevent innovative or sophisticated attacks. It's not useful for preventing Advanced Persistent Threats attacking critical infrastructure or sensitive government targets. Instead, it's designed to harden the UK against high volume, low complexity attacks.

Dr Ian Levy, the Technical Director at the NCSS says, ACD aims to *'raise the cost and risk of mounting commodity cyber attacks against the UK, thereby reducing the return on investment for criminals.. if we can affect that, we can demotivate attackers from targeting the UK.'* In this way, researchers at King's College London have said that the results of ACD may constitute an 'emergent public good delivering significant socioeconomic benefits' for everyone in the UK.

A principal aim of the NCSC's ACD programme has been to prevent cybercriminals from leveraging UK government networks and brands to launch their scams. Cyber criminals often exploit public trust in institutions to convince individuals to click on malicious links or undertake other risky behaviours. The ACD programme seeks to stop cyber criminals from exploiting UK government brands by using a range of automated tools designed to close off basic government vulnerabilities exploited by cyber criminals in these attacks including:

- **Takedown Service:** Asking hosting providers to remove websites and content impersonating the UK government and others;
- **Mail Check:** an automated scanning tool designed to identify vulnerabilities in UK government email systems that make it easier for cyber criminals to produce emails impersonating a government agency;
- **Web Check:** an automated scanning tool to identify common security issues in government websites;
- **Protective Domain Name System (DNS):** Blocking government users' access to bad websites, such as those known to distribute malware.

ACD doesn't solve all problems, but it seems to have achieved real success in the areas it has intervened. In mid-2016 Her Majesty's Revenue and Customs (HMRC) was the 16th most popular brand globally for phishing bait – the theme or narrative used to elicit certain behaviours from victims – but by the end of 2018 HMRC has dropped to 146th. The continued

disruptive activities of ACD reduced the effectiveness of using the HMRC brand and subsequently drove cyber criminals to other, less effective brands.

In its first year of operation, by disrupting the activities of cyber criminals the ACD programme was able to assist in halving the UK's share of global phishing attacks, taking down almost 140,000 UK-hosted phishing sites. During this period the Web Check system was able to use the same automated reconnaissance tools used by malicious actors to scan the UK government's digital infrastructure and identify over 2300 urgent issues for remediation.

Other initiatives as part of ACD have also paid dividends including a government wide Vulnerability Disclosure Platform through which users and security researchers can safely alert government to security vulnerabilities and a Suspicious Email Incubator that enables members of the public to report suspicious emails to enable automatic protective action to be taken.

These first-year results demonstrate that an ACD programme can be deployed on government systems and begin producing scalable results in a relatively short period.

The World Economic Forum recently cited the UK's Active Cyber Defence Model as a potential tool for addressing the 'cyber poverty gap' through the pursuit of a 'cyber version of the NHS' to address the uneven spread of cyber security capabilities. Similarly, the recent US Cyberspace Solarium Commission report made a number of recommendations (e.g. 4.5.1-4.5.3) calling for analogous actions in the US.

More ambitiously, the UK government is now seeking to expand the impact of ACD by making its automated tools available to businesses and charitable organisations. As Jeremy Fleming told CYBERUK 2019,

> *"For our next chapter, we want to ask what happens when the big communications service providers start to introduce our blocking techniques at scale? What happens when retailers take up some of the security indicators we've been developing with DCMS and use them to promote safety and security? Or when large corporates really get on board with anti-spoofing?*
>
> *So today, I would like to encourage businesses in all sectors to work with us to find new ways of incorporating these automated services. And if enough do, the results could be truly transformational - a whole-of-nation, automated cyber defence system."*

GCHQ has already made interventions of this kind. Fleming outlined one instance in which the agency identified over 1200 websites being operated by small businesses that were serving malicious code that collected the details of credit card transactions undertaken with the businesses. GCHQ's intervention enabled the small businesses to fix the issue, benefiting their reputation and protecting their customers from fraud. Last year, NCSC released 'Exercise in a box', an online tool that enables organisations, including small businesses, to test and practice how they would respond to a cyber incident. The NCSC has also increasingly sought to

cooperate with ISPs on network level interventions to block malicious traffic associated with known malware attacks. As a result, 86% of the members of the UK Internet Services Providers Association are now implementing, or will soon be implementing, ACD interventions.

An independent assessment of the ACD programme undertaken by the King's College London Cyber Security Research Group has foreshadowed the potential expansion of the ACD programme beyond government entities:

> *'There are no significant technical obstacles to extending these protections beyond the public sector and no fundamental reasons why ACD tools and techniques should not be tested and deployed as appropriate. Indeed, individual firms and trade bodies are already engaged in developing capabilities and best practice frameworks that build on ACD knowledge and experience.'*

While expanding the ACD programme beyond the public sector would face new obstacles and would require careful engagement with potential partners, such an initiative has the potential to make the broader online ecosystem in the country safer. It could reduce the overall number of attacks on vulnerable organisations like small business, and free up the resources of larger organisations to focus on sophisticated attackers.

The ACSC Commonwealth Cyber Security Posture 2019 outlines a number of discrete activities that the ACSC is already undertaking that are a conceptual fit with ACD. There is significant potential in expanding these activities within a coordinated framework for automated, scalable interventions targeting commodity cyber-attacks.

DEVELOPING AND ORGANISING AUSTRALIA'S CYBER SECURITY SKILLS

Developing and organising the domestic skills required to respond to the potential for large scale cyber incidents is an important part of building Australia's national cyber resilience.

There is wide recognition that a core part of this task will be growing the pipeline of Australians studying cyber security qualifications through our education system over time. Addressing the gender imbalance in the industry is also critical to expanding our cyber security skills. When 89% of your human capital is being drawn from one gender, you're effectively fighting with one hand tied behind your back. Creating more mid-career pathways for general IT professionals, developers and systems administrators, to transition to cyber security roles will also be crucial.

However, another important part of the puzzle is the organisation of Australia's cyber security human capital. Given the global shortages of cyber security skills, a number of countries have sought to improve their ability to respond to large scale cyber incidents by building institutions to engage the broader community in the task and to allow people working outside government to apply their cyber security skills in the national interest on a part time, auxiliary basis.

The two principal models for these auxiliary cyber security capabilities that deserve further consideration from government in Australia are *Civilian Cyber Corps (C3)* and *Cyber Reserves Corps* within defence forces.

Civilian Cyber Corps (C3)

The Cyber Civilian Corps (C3) are civilian organisations that professionally engage volunteers in public interest cyber security work. These organisations would allow experienced cyber security professionals to build the capabilities of people outside the sector in the broader community. In this way they are akin to a Cyber CFA/RFS or Cyber SES - professionally led, volunteer driven organisations though which people give their time to improve the collective safety of their community.

US Think Tank, New America has argued that Cyber Civilian Corps could be used to augment government interventions to lift cyber resilience in three areas:

- **Education and outreach**: offering cyber security awareness talks and training for not for profit community organisations and local businesses, offering basic cyber security training for community members;
- **Testing, assessments and exercises**: preventative interventions to deliver basic testing, assessment and incident response exercises for time and resource poor local organisations that lack cyber security expertise.
- **On call expertise and emergency response**: C3 volunteers would be available to undertake necessary activities on public or private networks in response to a significant or wide spread cyber incident.

These functions map closely to those of the CFA/RFS – community engagement, preventative action and crisis response surge capacity. The community engagement and preventative intervention functions of a Cyber Civilian Corps would complement any Active Cyber Defence interventions to lift the baseline of cyber resilience in the community. It's likely C3 members would be able to have a far greater impact at a community level than any government bureaucrat too. C3 members who know and understand their communities are far more likely to be able to gain traction in engaging local groups on these issues.

A Cyber Civilian Corps also offers mutual benefits to both volunteer participants, and larger, more capable cyber security organisations. Volunteers could be incentivised to join C3 groups to gain practical experience, access hands on training and certification, and network with others working in the industry while receiving a sense of satisfaction from having discharged a civic duty.

C3 groups could be a particularly beneficial for young people interested in a career in cyber security, providing access to real world experience and industry mentors and a pathway into a high paying pathway. There's real potential in creating an official youth wing of a C3 group. It's easy to imagine the kinds of collaborations schools, TAFEs and universities could engage in with C3 groups.

Finally, C3 offers real benefits to industry participation. Beyond the collective benefits of improving the baseline of cyber security capability in Australia, C3 would offer industry participants a valuable new source of recruits and a new channel for professional development opportunities, particularly in leadership and management. There are strong reasons to expect that well designed C3 organisations would attract significant in kind industry support.

There have been a number of proposals for Cyber Civilian Corps style organisations in Australia in the past with varying degrees of formality and ambition. Establishing an organisation of this kind in Australia would require careful consideration of the Australian context and the experiences of operational C3 groups around the world. To this end, we may be able to learn from the experiences of Cyber Civilian Corps in operation in Estonia and the US State of Michigan.

Estonian Cyber Defence Unit

The Estonian Cyber Defence Unit comprises around 200 volunteer personnel within the 15,000 strong Estonian Defence League, a paramilitary organisation that reports to the Commander of the Estonian Defence Forces.

As US Cyber Security researcher, Monica Ruiz describes it, the Cyber Defence Unit *'is made up of average citizens outside of government, who are specialists in key cyber-security positions, patriotic individuals with information technology skills, and experts in other fields (e.g., lawyers and economists) who wish to volunteer outside of their daily jobs to protect Estonian cyberspace.'*

The core tasks of the Cyber Defence Unit are:

- **Education and training**: training members in their skills and educating the public on good cyber hygiene practices, including seminars for government staff.
- **Strengthening and ensuring the security of the population**: supporting government entities (including schools and hospitals) with threat assessment and mitigation, as well as securing critical infrastructure. Private entities may also request the assistance of the Cyber Unit through the State Information System's Authority.
- **Crisis Response:** responding to a major or widespread cyber incident at the request of the government.

Michigan Cyber Civilian Corp

The Michigan Cyber Civilian Corps (MiC3) is an group of just over 100 civilian cyber security professionals who volunteer their time for 10 days a year *'to provide rapid response assistance to the State of Michigan in the event of a critical cyber incident'.* Members also engage in training and certification and seek to *'raise the security culture throughout the state'.*

Media reports indicate that the MiC3 has helped respond to three cyber attacks on local government in the state in the last 12 months and has made vulnerability scanning tools available to Michigan businesses to identify potential security risks.

Cyber Reserves

Defence forces have a long history of relying on part-time soldiers, militias and conscripts to increase available manpower in times of crisis and need. The modern iteration of this tradition is known as Reserves. These men and women undertake part-time military training and are available to be called up to active duties if needed, and will often balance their military service with a full-time civilian career.

Cyber Reserve forces sit within the existing branches of the defence forces and comprise are part-time personnel trained to engage in cyber operations with these organisations. Cyber Reserves provide low-cost channels for skills development and maintenance along with the surge capacity necessary to respond to any significant crises. Many basic cyber security tasks can be performed with relatively straight forward training that can easily be delivered in a military environment. In this way, Cyber Reserves could be a big vocational training opportunity. Regardless of the specific organisational model Cyber Reserves generally allow governments to access cyber skills without having to compete with full time private sector wages.

United States Cyber Reserve

The US military, similar to the UK model, has four service-specific cyber components that operate under the US Cyber Command. After a string of early successes demonstrating the effectiveness of Cyber Reserve forces against full-time cyber forces, US Cyber Command stated an aim of 15% Reserve component in the new 6000 cyber personnel recruitment, highlighting the appeal of Cyber Reserve personnel.

RAND has suggested that reservists are not only effective for cyber operations but in some ways are more effective than regular cyber operators in the defence forces. Firstly, cyber reservists have reduced training time and costs compared to other reservists, due to the significant overlap of skill requirements for Defence and non-Defence cyber security roles. Secondly, cyber reservists have reduced on-going training requirements as they get significant training from their regular employment. This ongoing training is referred to as the 'keyboard time' required to keep cyber security experts up to date with common tactics, techniques and procedures (TTPs) and maintain their skill levels. This is also referred to as 'cyber flight hours', analogous to how aircraft pilots gauge experience and capability by measuring flight hours on specific aircraft.

Singapore Cyber Specialists

In 2018, Singapore's National Service scheme began allowing National Servicemen to train to become Cyber Specialists during their two years of mandatory service. Upon completion of their mandatory service, Cyber Specialists are then given the option of continuing in paid service while they complete part time training that earns

Cyber Reserves have been highly efficient and effective in various iterations. But the main limitation of Cyber Reserves is the same as their main strength. It's an issue that was identified in an analysis of the Estonian Defence League *"In the event of a major cyber incident or crisis,*

the members of the Cyber Defence Unit are likely to have urgent tasks and responsibilities at the organisation where they hold their 'day job'". When a crisis hits, Reserve members can't be in two places at once. Calling them up for military service will mean that they are not able to perform the cyber security role they were formerly undertaking.

Israeli National Service

The Israeli Defence Forces have long streamed its best and brightest national service recruits into cyber security units where members receive intensive and highly specialised training. In addition to providing a continuing pipeline of cyber security talent, this model is widely regarded as a major contributor to Israel's status as a start-up power house in this space.

Australia currently has a nascent Cyber Reserve capability, with the latest figures indicating that the Australian Defence Forces had filled 77 Cyber Reservist positions out of 110 designated roles. There are currently no targets for further personnel recruitment. Expanding this Cyber Reserve capability would be a straightforward option for a government to build Australia's National Cyber Resilience.

CONCLUSION

The opening months of 2020 have changed the way Australians think about our national resilience.

First the fires, now an unfolding crisis on a global scale. The pandemic has raised challenging questions about the systemic weaknesses of modern, densely interconnected societies — and it's forced Australians to confront some tough questions about our domestic capability to respond to global tumult.

But we should not wait until another crisis mugs us before improving our vulnerabilities. We know what those vulnerabilities are *now*. We know the centrality of cyber networks to our society, and we know that they remain vulnerable.

In the wake of the COVID-19 pandemic, we will see this new perspective brought to debates about Australia's sovereign capability, our industry policies, our strategic policy and the health of our democratic institutions.

National Cyber Resilience will be crucial part of this discussion.

Authorised Tim Watts, Australian Labor Party, Footscray, Victoria.