A whole of society approach to cyber challenges in Australia and the Pacific

WithYouWithMe submission to the 2023-2030 Australian Cyber Security Strategy discussion paper

White paper

Contents

I recently visited Australia to deliver keynote addresses on cyber resilience and workforce strategy at major events including the AISA's Australian Cyber Conference and the Department of Home Affairs' Global Marine Transportation System Cybersecurity Symposium. I also met with a number of senior Government officials, including Secretary of the Department of Home Affairs, Michael Pezzullo AO, to share insights into how Australia and the UK can learn from each other to address our shared cyber challenges.

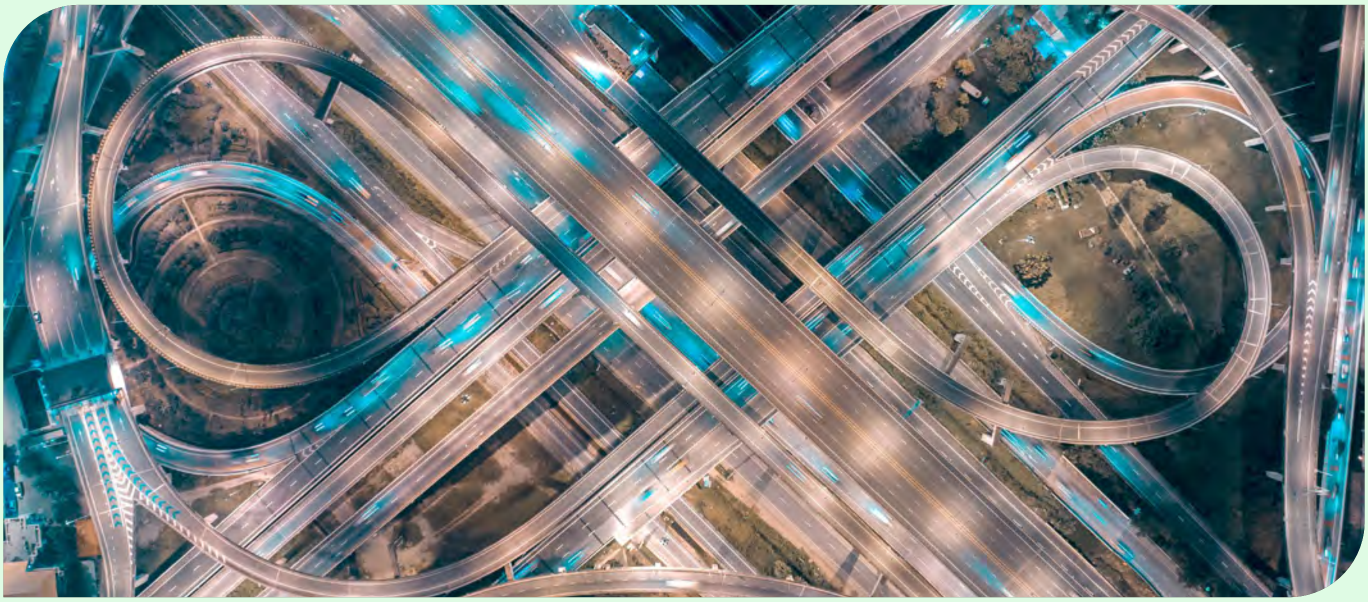
My perspective following these events and meetings is that the defining challenge of the cyber era is the recruitment of talent. Leaders often think cyber is a tech problem – but it's a people problem.

The answer to building a world class national cyber capability is in **enabling and hiring the most diverse skillset possible, using all ideas, talents and contributions, and upskilling these individuals in cyber skills**"

Sally Walker

Former Director Cyber, GCHQ

Strategic Advisor, WithYouWithMe



When the attack comes - society must prevail

Digital unity

Digital transformation, the reshaping of cybercrime, and the ongoing conflict in Ukraine have demonstrated that cyber challenges require a whole of society approach. As billions more devices are being connected to the internet and our cities become digitised, societal resilience to cyber threats must be achieved through digital inclusion, social cohesion and the seamless integration of digital technologies into a society, this includes Australia's Pacific neighbours.

Australian society is built on trusted personal networks. These networks are fragile and can be rapidly exploited to drive fragmentation of a society through social media manipulation, cyber attacks on critical infrastructure and targeted disinformation campaigns. These networks can also be the key to national cyber resilience through achieving digital unity, leading to a rapidly scaled resistance and collective ability to defend against financially motivated cyber actors, malicious information operations and hostile digital nation states.

The speed of Australia's response

The speed of digital transformation, and the protracted national response to the digital skills crisis means the Australian Government must not allow the status quo to limit the potential outcomes of this Cyber Strategy. It is clear that Australia and our Pacific neighbours now require a more drastic transformation rather than merely taking a small step away from our current position. The approach must be scalable to include our regional partners and adaptable to the dynamic cyber landscape out to 2030.

Cyber and information threats

In the information age, cyber operations are deeply connected to information operations, often being used as complimentary to each other in multi-domain digital engagements. They cannot be separated when considering the Australian Governments' holistic approach to the challenges of the future cyber threat landscape.

Scope

This white paper has considered the following questions presented in the 2023-2030 Australian Cyber Security Strategy Discussion Paper:

1. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?
2. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?
3. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?
4. What can government do to improve information sharing with industry on cyber threats?
5. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?
6. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?
7. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

Cyber resilient Pacific

Digital skills are essential to unlocking economic opportunities and prosperity, both in Australia and the neighbouring Pacific region. A digitally fluent Pacific community will significantly contribute to cyber resilience, and help to address the geopolitical challenges and power dynamics as the region adjusts to the modern digital era.

Australia must enhance its cyber cooperation to protect neighbouring countries from cybercrime and hostile cyber and information attacks originating from authoritarian states. Collaboration with Pacific Island partners will be crucial for establishing and maintaining a secure cyber environment and regional prosperity.

The Australian Government holds a respected humanitarian response track record in the Pacific and is recognised as a key contributor to the stability of the region. The government can leverage its positive standing in regional Pacific organisations, such as the Pacific Islands Forum and the Pacific Community, to lift cyber resilience by supplementing existing regional programs and providing baseline digital skills training.

In providing this training, Australia will lift the digital, data and cyber literacy of the region, building essential cyber resilience in Pacific communities at the grass-roots level by promoting safe and responsible behaviour online and providing individuals with the skills and knowledge needed to navigate the modern digital landscape. Digital, data and cyber literacy will help to reduce the risk of cyber attacks and minimise their impact when they occur.

Grey zone confrontation in the Pacific

There has been a persistent coordinated effort to influence Pacific Island populations by amplifying narratives critical of Western partners[1], recent information operations in Solomon Islands have undermined the Solomon Islands Government's existing partnerships and influenced public opinion, namely with Australia and the US.[2] Cyber operations such as DDoS attacks and website defacement have the potential to cause more than just business disruption as they can also serve as tools for disseminating fabricated news and facilitating extended disinformation campaigns, as recently demonstrated in Taiwan[3].

Providing digital skills training to Pacific Island nations will help Australia own the dominant narrative, and demonstrate the Government's eagerness to share the benefits of digital literacy and boost cyber security for the entire region.

Japan's National Institute for Defense Studies released the 2023 edition of its annual China security report, in which it detailed China's focus on grey zone operations and control of the cognitive domain[4]. Beijing is increasing its influence operations in the West through propagating the Chinese narrative in social and traditional media.

Digital, data and cyber literacy skills training provided by the Australian Government will be vital to improving Pacific citizen understanding and comprehension of the information environment in order to better combat misinformation, disinformation and propaganda.

[1] https://www.aspistrategist.org.au/understanding-chinas-efforts-to-undermine-partnerships-in-the-pacific/

[2] https://www.aspistrategist.org.au/how-the-chinese-communist-party-is-spreading-lies-in-solomon-islands/

[3] https://www.thechinastory.org/psyops-and-cyber-war-in-taiwan/

[4] http://www.nids.mod.go.jp/english/publication/chinareport/index.html

Pacific resilience project

The Pacific Resilience Project (PRP) is a proposed regional program facilitated by the Australian Government that focuses on skills mapping all citizens in neighbouring Pacific countries, with the aim of uncovering untapped potential in our Pacific community.

SFIA skills mapping

Knowing what individuals are capable of – or where gaps exist – will be crucial to ensuring project success. The Skills Framework for the Information Age (SFIA) is a globally recognised digital skills model that is used to assess, develop and manage the skills of a national workforce. Already embedded within the Australian Public Service[5], SFIA serves as a common language for describing digital skills and helping governments map competencies and identify skills gaps.

SFIA is organised into six skill categories which are then broken into seven levels of responsibility:

SFIA

Strategy and architecture	Development and implementation	Delivery and operation
Change and transformation	Relationships and engagement	People and skills

Levels of responsibility						
Level 1 Follow	Level 2 Assist	Level 3 Apply	Level 4 Enable	Level 5 Ensure, advise	Level 6 Initiate, influence	Level 7 Strategise, inspire, mobilise

SFIA overview

The Skills Framework for the Information Age (SFIA) is the industry recognised, global skills and competency framework for the digital world. It defines the skills and competencies required by technology professionals at every level to design, implement, manage and protect data and technology.

Applications

- Comprehensive, standardised and scalable skills mapping
- Clear identification of skills gaps
- Enables skill development pathways to be tailored to project goals

Benefits to Pacific nations

- Identify relevant digital skills shortages - prioritise training and education programs to address gaps.
- Improve digital workforce planning for policymakers and employers - understand the skills composition of society and plan for future national requirements.
- Highlight the strengths and areas of expertise of society - this information can be used to attract investment and create a favourable environment for the growth of the sector.
- Surge digital talent between Pacific partners to support regional resilience projects - contributing to a well networked digital Pacific community.

[5] https://www.dta.gov.au/blogs/important-step-australian-digital-capability

Benefits to Australia

- Identify individuals who have the skills to make a significant contribution to the Australian economy - fill national skills shortages through the skilled migration program.

Benefits at the individual level

- Assess current skills and identify areas for improvement - create personalised development plans that target specific skills and knowledge needed to achieve career goals.
- Move away from subjective resumes to a more comprehensive, standardised, and industry-recognised way of representing individual's skills - demonstrate competence and increase employability.
- Identify transferable skills that can be used to pursue in demand opportunities across different roles and industries - individuals can explore new career paths and opportunities for growth.
- Future-proof career by mapping skills and staying up to date with industry trends - remain relevant in the fast-changing digital economy.

Sociocultural mapping

Psychometric tests are a scientific method of measuring an individual's aptitude, learning style, personality type and potential to contribute to a project such as the Pacific resilience project. There are multiple tests in the market including the Myers-Briggs Type Indicator (MBTI), DISC, The Big 5, and Gallup Strengths Finder.

Project organisers can save valuable time and resources, and hence will be able to scale rapidly, by using psychometric testing to identify talent. According to a study by the International Journal of Selection and Assessment[6], psychometric testing is effective in identifying individuals with high potential and can reduce both hiring costs and time-to-hire. They benefit both the individual and the workforce manager by assessing:

- **Personality:** providing insights into an individual's personality traits, such as their strengths, weaknesses, preferences and behavioural tendencies. Understanding an individual's personality traits can help identify whether they are a good fit for a particular role, team or culture.
- **Skills:** mapping an individual's skills, such as verbal, numerical or spatial reasoning. These tests can help identify an individual's potential to perform well in a particular role or task.
- **Work style:** Identifying an individual's work style, such as their preferred work environment, communication style, decision-making approach and leadership style. This information can help identify whether an individual is a good fit for a particular role or team.
- **Team dynamics:** identifying how individuals work together in a team. For example, The Big 5 can provide insights into an individual's personality traits and how they might interact with other team members. This information can help identify potential conflicts or opportunities for collaboration.

[6] https://onlinelibrary.wiley.com/doi/full/10.1111/ijsa.12182

Learning style

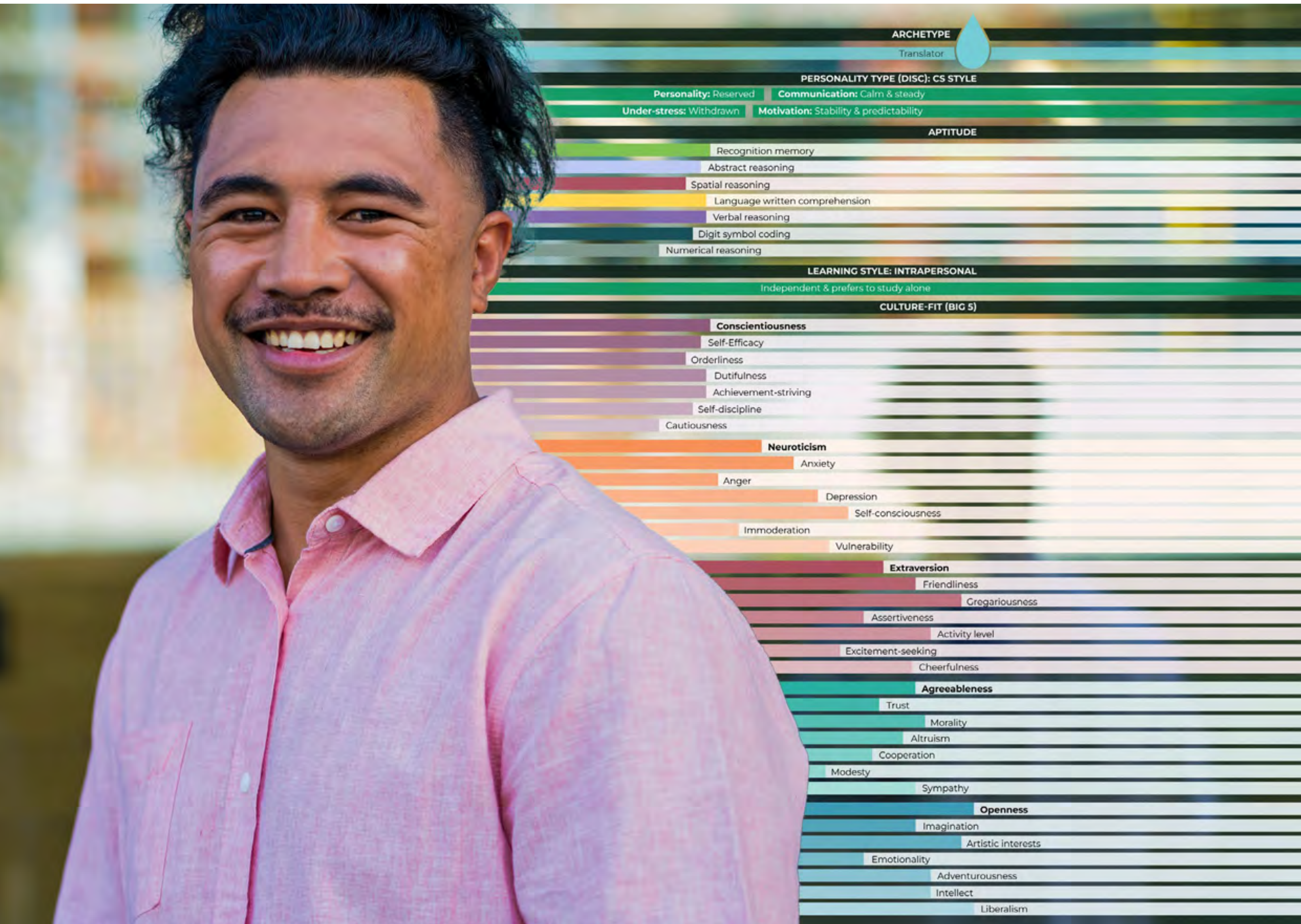
The Walter, Burke, Barbe Modality model, and the Fleming VARK model help individuals understand how they learn best and adapt their learning strategies accordingly to maximise their learning potential. Individuals may not fit neatly into one specific category or learning preference and may benefit from a combination of different strategies.

This approach to learning digital skills makes the process more efficient by helping individuals tailor study strategies to their specific needs. By identifying the ways in which an individual learns best, they can focus their time and energy on the study methods that are most effective for them, rather than using a 'one-size-fits-all' approach.

Connecting the dots

When these data points are combined, a complete picture can be built of a society, workforce or project team – pinpointing skills and abilities, learning styles, personality types and communication preferences. Once a clear community profile is created, it becomes the blueprint for the best way to connect, motivate and inspire citizens to perform to their potential.

Individuals would be provided a personalised development plan tailored to the outcomes from their sociocultural mapping and learning style.



Digital upskilling

All Pacific citizens would be provided unrestricted access to fundamental digital skills training courses (such as IT Fundamentals, Networking Fundamentals, Linux Fundamentals) free of charge. This would give a wide range of Pacific Islanders access to basic IT skills and help identify those who wish to pursue more in-depth cyber related studies.

Online course content and delivery mechanisms would be tailored to account for the unique requirements of Pacific Island trainees, such as reduced access to the internet and lower bandwidth.

A logical pathway for those completing fundamental digital skills training would be to provide access to certification pathways that align with the skills and knowledge they have acquired during their training. By aligning basic digital skills training with certification pathways, and providing access to the pathways, individuals can validate their newly acquired skills and knowledge, and have a clear roadmap for their ongoing professional development, allowing them to stay current with the latest industry trends and technologies. Additionally, access to certification pathways can increase the credibility and reputation of the Pacific training program, as it demonstrates the Australian Government's commitment to providing relevant and valuable training opportunities to individuals seeking to enter or advance in the digital workforce.

Case study

PNG's DICT expands Government cyber capabilities with first-of-its-kind training event in Port Moresby

A two-day training event run by the PNG's National Cyber Security Centre (NCSC) saw representatives from its partner WithYouWithMe (WYWM) travel to Port Moresby to facilitate critical cyber security training for Government and State-Owned Enterprise employees. The event was coordinated through the NCSC and PNG's Department of Information and Communications Technology (DICT).

Whilst the event was available online, hosting in-person was the key to a huge jump in course completion rates with 82 participants finishing their training programs armed with improved skills to combat evolving cyber threats.

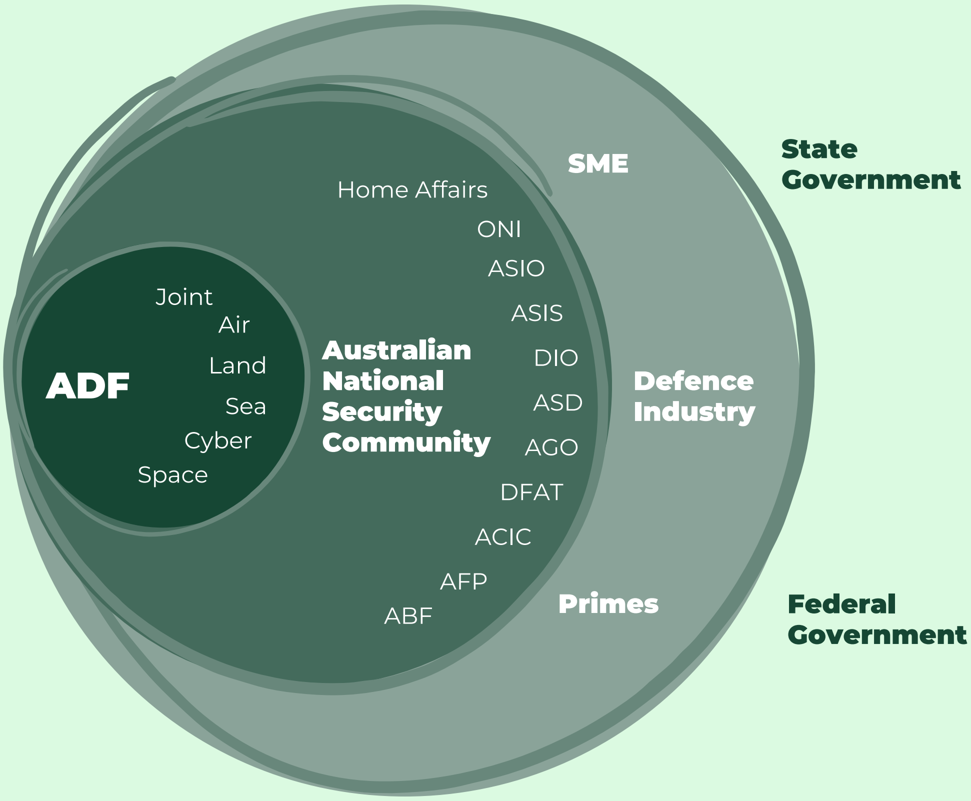
The event also allowed many to surpass common barriers to engaging in digital training including access to computers at home and consistent, high-speed internet connection.

National security ecosystem

The Australian Government can develop a best practice approach to national cyber intelligence by bringing together the interconnected network of security individuals, organisations and institutions to deliver sovereign cyber capabilities in a single ecosystem, known as the National Security Ecosystem (NSE).

Government agencies are arranged around complex, multilayered systems and processes, the Department of Home Affairs Secretary Michael Pezzullo explained that "the public service — through a lot of managerialist ideological changes made in the 1990s – has become [a] much more fragmented body". To foster cognitive diversity and the contestability of ideas, Government agencies must facilitate skills mobility. An NSE would be the next evolution of the APS Mobility Framework[7] to include a wider network of Defence and national security organisations, industry organisations, SMEs, Primes and state government.

Through the creation of an NSE the Department of Home Affairs and other relevant departments would become less fragmented and more networked. This would facilitate security cleared cyber talent exchange, rapid skills mobilisation, knowledge sharing and collaboration to allow for flexibility in the dynamic cyber environment out to and beyond 2030.



[7] https://www.apsc.gov.au/initiatives-and-programs/aps-mobility-framework

Skills intelligence

The NSE would need to embrace a universal and industry-recognised skills and competency framework to identify and evaluate the skills possessed by individuals and map the requirements of cyber roles within the ecosystem. This mapping process would provide valuable insights to workforce managers by highlighting the strengths and weaknesses of digital and cyber workforces within their organisation, other organisations, and the entire NSE. Workforce managers would be able to easily identify gaps in skills and knowledge, and develop tailored national training and recruitment strategies to meet the resourcing requirements dictated by the cyber threats Australia faces.

Cyber talent recruitment

Unrealistic experience requirements, prerequisites and credentials for entry level cyber roles has led to a skills shortage in the industry. Clearly defining the skills and competencies required for all cyber roles within the ecosystem using SFIA skills levels would remove barriers to entry for individuals without a traditional career background.

As outlined in Sally Walker's foreword, the defining challenge when recruiting for cyber capabilities is that leaders expect staff to have traditional tech qualifications, however, the answer to building a national cyber capability is hiring the most diverse minds possible, using all ideas, talents and contributions, and then providing these individuals with the necessary digital skills to succeed in a cyber team.

This recruitment philosophy would have the additional benefit of lifting the Australian Government's reputation as an employer that values individual development and growth, attracting and retaining top talent and improving the Government's brand as an employer of choice in the skills marketplace.

Security cleared cyber talent retention

The Australian Public Service is currently facing an attraction and retention crisis and continues to have vacancies in critical roles. The current people capability processes of the Australian Government mean that departments are unable to formally maintain contact with individuals when they transition to a position outside the public service. Where they go, how their careers change and what new skill sets are acquired are all unknown. By facilitating mobility within the NSE, security cleared individuals that would like to pursue another role outside their current organisation would be retained in the national cyber capability, while gaining new skills, knowledge, and experiences they are looking for in a different environment or culture.

This knowledge transfer would benefit the entire ecosystem, as the individual can share new ideas and approaches that enhance national cyber capabilities. Ecosystem mobility would also strengthen relationships between organisations and foster collaboration and a shared understanding of each other's operations, leading to innovation opportunities and operational efficiencies.

The Australian Government would additionally gain the agility to adapt to changing strategic requirements by effectively allocating human assets during times of national crisis. Increased staffing flexibility through NSE talent mobility would allow organisations to temporarily loan talent to other organisations, manage workload fluctuations and avoid the need to hire additional employees.

Addressing skills shortages in the National Security Ecosystem

Australia is facing a digital skills shortage, but the Australian Government can lead the effort to address this. If we are to equip our workforce with the skills to meet a rapidly changing, technological future, we must define a new path.

Ensuring the Australian Government has a pipeline of cyber talent to meet the demand for cyber skills both now and into the future will require a multi-faceted approach. Through the combination of external recruiting of individuals from diverse backgrounds and internal upskilling programs of the current workforce, the Australian Government's cyber workforce will be more reflective of the broader community it serves.

Cyber uplift pathways based on potential

Upskilling of existing staff within the National Security workforce will play a crucial role in addressing future cyber workforce requirements, as all roles will be affected by digital automation and augmentation in the coming years.

This can involve testing of employees potential to identify digital skills aptitude, implementing streamlined training programs and mobilising employees to transition into roles that support cybersecurity. Additionally, internal mobility opportunities can be identified by using SFIA to map the current skills gaps within the APS and the skills employees currently have. In doing so, the Australian Government can make the most of its existing human assets, by unlocking untapped talent that currently lies dormant within the APS workforce

National Security Ecosystem skills mobilisation

Connecting demand and supply across organisations within the NSE can achieve more scalability and a faster return than repeatedly recruiting and making career placement decisions to fill vacancies and administering HR applications. Empowering National Security organisations and their workforces to self-organise can lead to improved outcomes without the bureaucracy overhead.

Mobilisation is achieved by enabling NSE leadership to directly resolve capacity and capability shortfalls, as they are best placed to judge their operational gaps or opportunities and make appropriate decisions. Additionally, the cyber workforce can be given more freedom to apply for diverse roles across the NSE, allowing them to apply their skills, gain new experiences and demonstrate their potential in different contexts. These outcomes create value for both the national cyber capability and the individual employees – a win-win situation.

Skills mapped immigration

Skills mapped immigration offers a simplified, repeatable alternative to skilled immigration, allowing the Australian Government to identify the specific skills and expertise required for a particular digital project, and recruit individuals who possess those skills. This approach is more targeted and efficient than traditional skilled immigration, which focuses on individuals who meet broader criteria such as education level or work experience. As mentioned previously, unrealistic experience requirements, prerequisites and credentials for entry level cyber and digital roles have led to a skills shortage, and these requirements are almost never met in the regions that Australia opens for immigration, such as the Pacific Engagement Visa (PEV).

With skills mapped immigration, the Australian Government can (in consultation with sovereign organisations) identify gaps in the domestic workforce and target recruitment efforts towards individuals with the specific skills needed to fill those gaps. This would result in a more diverse workforce that is better equipped to meet the needs of a dynamic cyber threat environment, while addressing the broader problem of meeting skilled worker targets for national projects.

While increasing the intake of cyber skilled migrants is an option, the difficulty of attaining security clearances for foreign-born Australians is one to consider. Declassifying the information these individuals will be in contact with will need to be considered for this programme to be successful.

Cognitive diversity

Cognitive diversity encompasses a range of factors including personality, experiences, perspectives, skills and knowledge. The more diverse a team is, the higher their level of collective knowledge processing (the extent to which individuals prefer to consolidate and deploy existing knowledge, or prefer to generate new knowledge) and better ability to employ perspective (the extent to which individuals prefer to deploy their own expertise or prefer to orchestrate the ideas and expertise of others) is when facing new situations[8]. Cyber teams of the future will require the ability to respond to evolving challenges as they appear, hence, these teams will require cognitive diversity to succeed.

Recruiting from diverse and underrepresented segments of society will result in cognitively diverse cyber teams who often have unique perspectives and experiences that can help to generate new ideas and approaches to cyber challenges. When teams are composed of individuals with different backgrounds, experiences and ways of thinking, they are more likely to be able to identify and solve complex problems and are more resilient in the face of unexpected challenges.

For example, individuals from underrepresented segments of society may have different cultural backgrounds, language skills and life experiences that provide alternative perspectives on cyber threats and solutions. This can help to broaden the team's understanding of the problem space and increase the likelihood of identifying new and innovative solutions.

In addition, diverse teams help to avoid groupthink, a phenomenon where team members tend to conform to a dominant viewpoint and ignore alternative perspectives. By including individuals from cognitively diverse backgrounds, cyber teams can increase the likelihood of challenging assumptions and questioning the status quo, which leads to more effective decision-making and problem-solving.

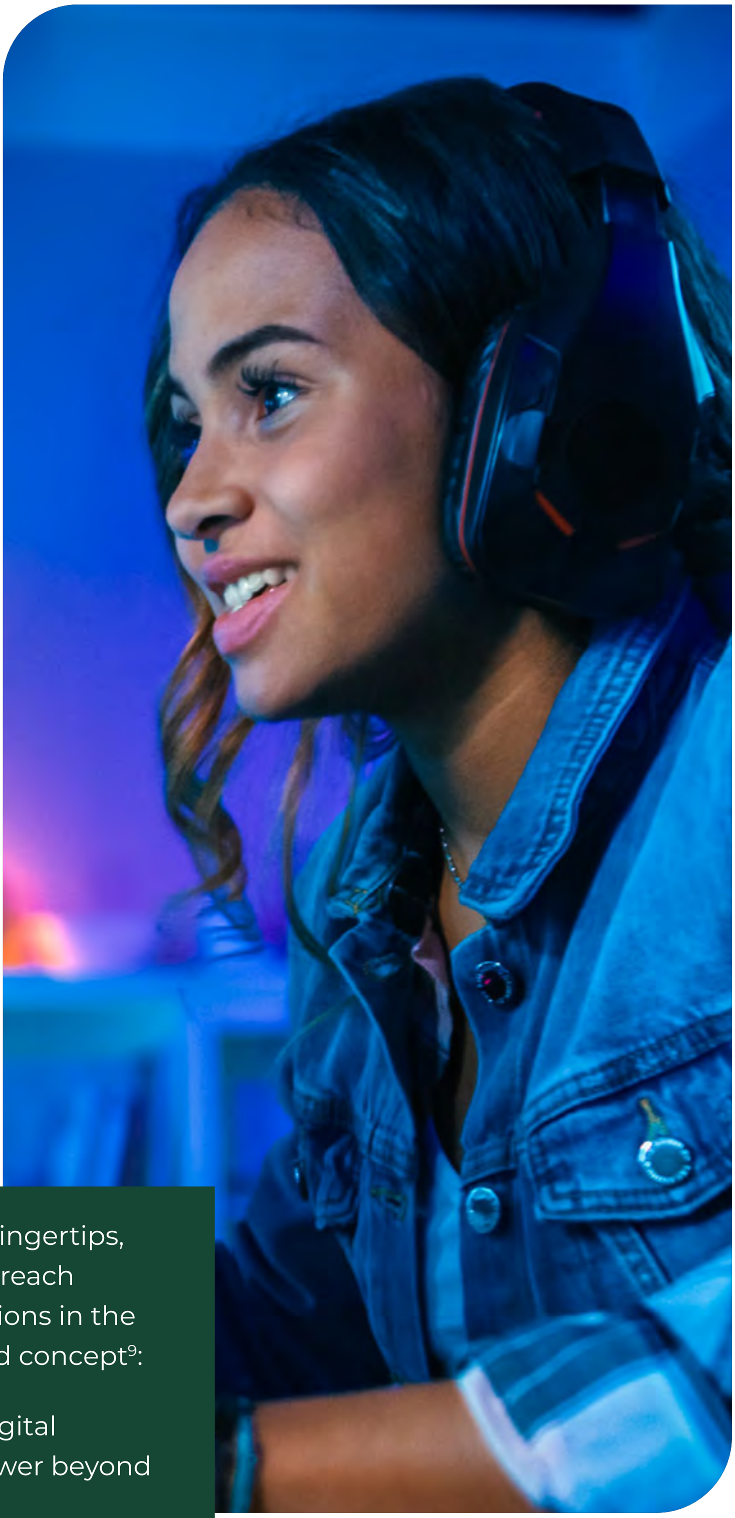
[8] https://hbr.org/2017/03/teams-solve-problems-faster-when-theyre-more-cognitively-diverse

Digital natives

Digital natives are individuals who have grown up in a world where digital technologies, such as computers, smartphones, and the internet, have always been a part of their lives. They tend to have shorter attention spans compared to previous generations, likely due to the fast-paced, highly stimulating nature of digital technology.

Digital natives are an essential group to target for cyber roles because they possess valuable technology fluency, innovative mindsets, adaptability, collaboration skills and diversity, making them a valuable addition to cybersecurity teams. Additionally, their high preference for flexible and remote work arrangements make them a great target for remote work and ad hoc work opportunities.

Digital natives are a valuable source of talent for government organisations looking to expand their cyber talent workforce. Digital natives are comfortable using digital tools and platforms, making remote work a natural fit for them, and allowing for greater flexibility in terms of working hours. Government organisations can tap into their skills, attitudes and perspectives by offering job opportunities that align with these preferences, such as part-time or full-time remote work options or flexible work schedules. Further exploration on these opportunities are examined later in this document.



Growing up with technology at their fingertips, digital natives take much less time to reach digital wisdom than previous generations in the workforce. Digital wisdom is a two-fold concept[9]:

- Wisdom arising from the use of digital technology to access cognitive power beyond our usual capacity
- Wisdom in the use of technology to enhance our innate capabilities

[9] Shing Cheong, M. (2023). Digital Natives and the Path of Digital Wisdom: Practical Implementation of Digital Security Education – The Techducator. The Techducator. https://munshing.com/tech/digital-citizenship/digital-natives-and-the-path-of-digital-wisdom-practical-implementation-of-digital-security-education

Citizen baseline digital literacy

As digital technology becomes increasingly embedded in our daily lives, citizens are more likely to encounter threats from cyber criminals such as phishing attacks and malware, and influence operations through the manipulation of information by nation states. Basic digital literacy can help citizens identify and mitigate these threats, reducing the likelihood of successful attacks that can compromise personal or sensitive information, critical infrastructure, or even national security.

Citizens with a basic understanding of cybersecurity can help to strengthen the overall security posture of the country by reporting suspicious activity or vulnerabilities they encounter and identifying misinformation and disinformation - increasing the visibility and responsiveness of cyber threats for Government agencies.

National defence against information operations

Hostile nation states have shown their ability and willingness to manipulate information in the cyber domain, to influence public opinion, conduct psychological operations and pressure legal and political systems[10]. Generating a baseline of national digital literacy will help individuals be more discerning consumers of information online, enabling citizens to critically evaluate the information they encounter and make informed decisions about what to trust and what to dismiss.

Identify citizens for further cyber training and employment

Baseline digital literacy testing of citizen volunteers can be used to identify individuals with talents that are relevant to a cybersecurity profession. The testing can highlight an individual's strength in areas such as digital tools, programming languages, or network administration. Additionally, the testing can identify individuals with an analytical and problem-solving mindset, which are crucial qualities for a career in cybersecurity.

Furthermore, the testing can identify individuals with strong communication and collaboration skills, which are necessary for cybersecurity professionals who need to work effectively with others. Overall, Citizen baseline digital literacy testing can provide a useful starting point for identifying individuals with the potential to pursue a career in cybersecurity, by evaluating their digital literacy, problem-solving mindset, and communication and collaboration skills.

Integration to current pathways

The Australian Government has allocated funding to support cybersecurity education and training initiatives, such as the Cyber Security Cooperative Research Centre, the Cyber Security Skills Partnership Innovation Fund, and apprenticeship programs with industry partners, however, these individuals are not skills mapped, nor are they held on a National Security Ecosystem database.

Investing in education and training is a good foundation[11], however, the location of individuals and level of their skills need to be captured. A skills mapped database of all citizens will support the Australian Government's integrated industrial base by providing a comprehensive overview of available skills and expertise of the Australian community, enabling a targeted recruitment campaign to meet the needs of the cybersecurity industry.

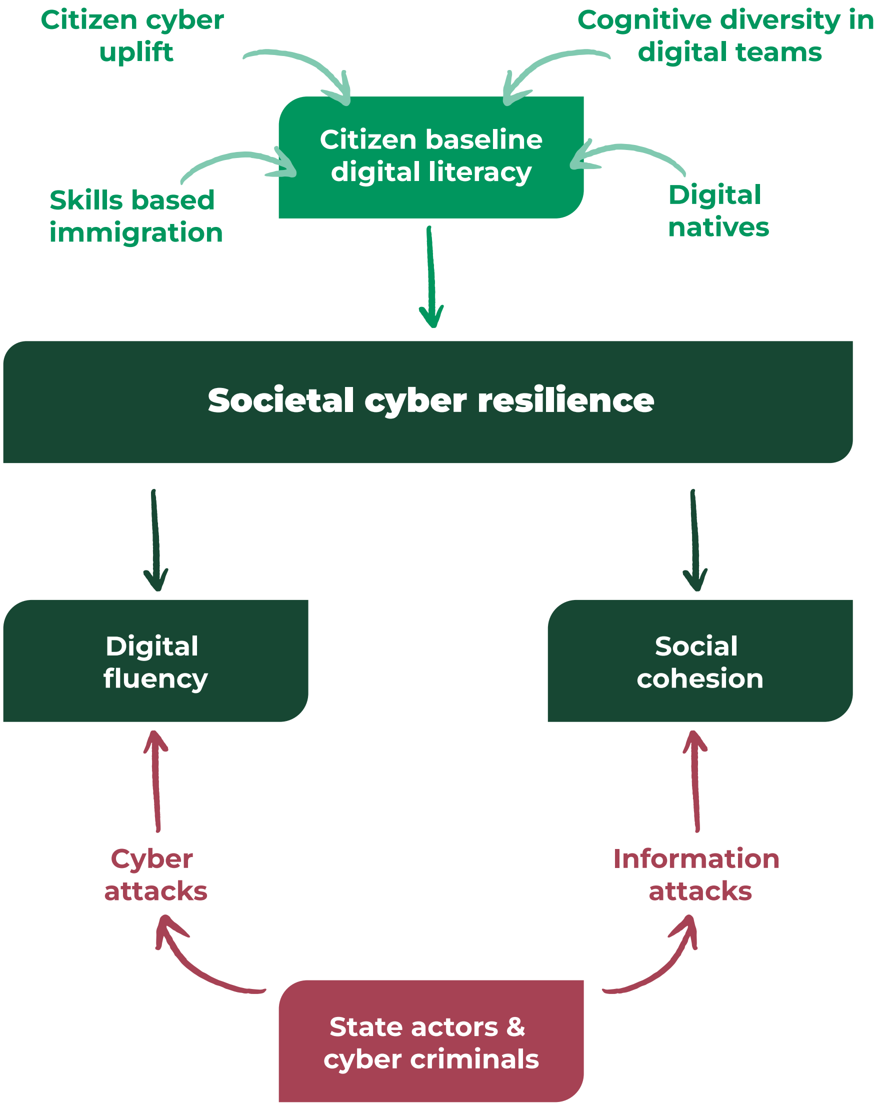
[10] Fritz, Jason R. (21 March 2017). China's Cyber Warfare: The Evolution of Strategic Doctrine. Lexington Books. p. 70. ISBN 978-1-4985-3708-7.

[11] https://www.digitalprofession.gov.au/career-development/aps-career-pathfinder-tool#individuals

Whole-of-country approach required to meet future challenges

Achieving an integrated digital base for the 'whole of country' approach to meet future challenges relating to the progression of cyber and emerging technologies will require a coordinated effort between government, industry and education and training providers to upskill and reskill Australian citizens to meet workforce skills demand effectively.

A multi-pronged approach including digital skills uplift of all citizens, migration based on skills mapping (and potential to gain skills rather than qualifications), cognitive diversity through removing the biases associated with traditional recruiting, and providing a workplace that appeals to digital natives will organically lift the cyber resilience of Australian society. With skills nurturing, this approach will lead to systematic defence against cyber and information attacks on the Australian community.


Citizen cyber uplift
Cognitive diversity in digital teams
Citizen baseline digital literacy
Skills based immigration
Digital natives
Societal cyber resilience
Digital fluency
Social cohesion
Cyber attacks
Information attacks
State actors & cyber criminals

Digital volunteers

Scalable remote workforce

Australia is at a juncture where the pace of change is colliding with the development of skills. New technologies are reshaping existing industries and creating new ones. Workplace cultures are shifting. Higher productivity is being achieved through remote-work arrangements and the fast-growing 'Gig-Economy' is quickly disrupting and transforming the skills ecosystem.

Last generation's workforce technologies were built for last generation's economy. As the Gig-Economy continues to grow, a new generation of tools and technologies is taking root and the Australian Government must maintain a technological edge to capture its share of the workforce. Today's workforce is different in nature from previous generations, seeking tech-enablement, virtual-connection and the ability to self-organise through better access to the demand for skills.

Rapid changes in demand will require an equally agile and adaptive supply. The foresight required to build the Australian Government's cyber workforce exceeds the available time and concurrently reduces organisational agility. This could be considered the biggest strategic risk facing the Australian Government's cyber people capability - being unable to accurately anticipate the needs and requirements of the National Security Ecosystem during a crisis, especially given the grey zone nature of current geopolitical competition and the enduring risk of black swan events in the Indo-Pacific.

By embracing data, technology and flexible and responsive workforce models – the Australian Government can deploy skills, expertise and talent to where it is needed to deliver the outcomes that the Government and Australians expect.

The National Digital Emergency Service

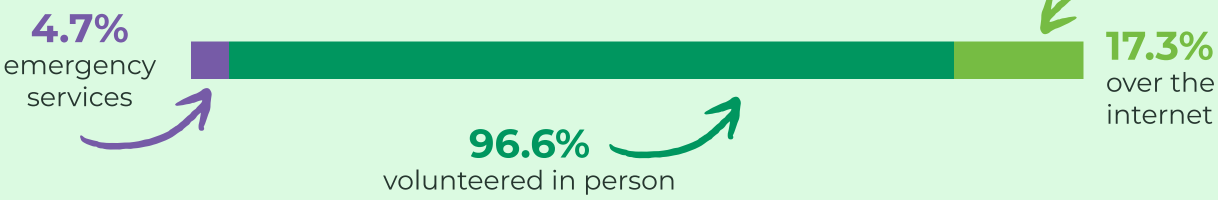
Just as citizens augment the government's response and recovery capabilities during natural disasters, digital volunteers can remotely offer their time, skills, and expertise to help organisations and communities respond to and recover from cyber incidents.

Natural disasters and cyber events share similarities such as the need for volunteers with specialised skills and training, operating in high-pressure environments, and relying on collaboration and coordination to be effective in their efforts to help those affected by a crisis.

Natural disasters cost the Australian economy **$38 billion** per year on average[12]

Cybercrime cost the Australian economy an estimated **$42 billion** every year[13]

Over 5 million (5.025 million) people volunteered through an organisation or group in 2020[14]



What can we learn from recent natural disasters to inform a cyber crisis response?

Findings from the Royal Commission into National Disaster Arrangements highlight that consistent, timely and actionable data are key to enabling effective national coordination against future crises.

In the Royal Commission into National Natural Disaster Management, it was identified that emergency organisations and Defence currently have minimal data insights leading to poor visibility on the skill set, location, availability, and physical and mental attributes of their volunteer and fulltime workforces.

Royal Commission into National Natural Disaster Management[15]

[12] https://www.iag.com.au/newsroom/community/natural-disasters-estimated-cost-australia-73-billion-year-2060

[13] https://www.unsw.adfa.edu.au/newsroom/news/cybercrime-estimated-42-billion-cost-australian-economy

[14] https://www.volunteeringaustralia.org/wp-content/uploads/VA-Key-Volunteering-Statistics-2022-Update.pdf

[15] Royal Commission into National Natural Disaster Management, Interim Observations, (Commonwealth of Australia, August 31, 2020), https://naturaldisaster.royalcommission.gov.au/publications/interim-observations-1#a-shared-responsibility

The National Digital Emergency Service (cont)

Not only are there growing concerns about the sustainability of volunteer workforces that support emergency services across Australia as numbers continue to decline[16], but even the Defence Force (who is utilised as the contingency force in natural disasters) doesn't have an accurate picture of skills and locations of personnel willing to assist in a crisis. It has been argued that there is a need for a nationally coordinated strategic approach to manage volunteer response workforces and enhance the resilience of communities and the emergency services that respond to natural disaster events.

A trained and actively managed civilian emergency response force is currently being considered as a potential solution to augment the emergency services and Defence Force in natural disasters, however, there is no discussion regarding a civilian cyber service to support the Australian Cyber Security Centre (ACSC) during cyber events. Volunteering Australia states that information technology is providing new opportunities for people to find a volunteering opportunity that suits their interests and circumstances, and to volunteer in different ways.[17]

The changing demographics of volunteers and improved citizen access to digital technology present the Australian government with an opportunity to leverage the rapid scalability and efficiency of new types of volunteerism such as virtual volunteering and micro-volunteering, and enhanced data-driven decision-making to prepare for cyber incursions within our sovereign borders.

What volunteer force supports the cyber first responders?

"the excellent work done by, for instance, the Australian Signals Directorate, which is a Defence portfolio agency, and the centre within ASD known as the Australian Cyber Security Centre is the equivalent of the initial first responder: make sure everything's safe, make sure that lives are being saved and all the rest of it, in the same way that our firefighters and emergency services personnel would undertake."

Department of Home Affairs Secretary Michael Pezzullo[18]

[16/17] https://www.volunteeringaustralia.org/wp-content/uploads/VA-Key-Volunteering-Statistics-2022-Update.pdf

[18] https://www.themandarin.com.au/213703-cybersecurity-crowded-pitch-creates-complexity/

In today's world, cyber must be seen more like a traditional tradecraft than a theoretical one – unfortunately the traditional education methods used by tertiary and vocational education providers to develop digital talent has resulted in programs that cannot evolve fast enough to keep pace with both market demand and the evolution of technology.

The establishment of a part-time, volunteer National Digital Emergency Service (NDES) under the jurisdiction of the National Cyber Security Coordinator (supported by a new Cyber and Infrastructure Security Group), would provide the government with increased cyber security capabilities, including preparation against cyber attacks, training for members and incident response surge capacity. The NDES would have a clear remit to provide cyber security uplift for government, organisations, non-profit entities and the community. It would offer training and accreditation to members similar to the State Emergency Services (SES) or the NSW Rural Fire Service (RFS) and provide surge capacity for widespread cyber incidents. The objective of the service would be to enhance the Australian cyber security workforce and would address the practical skills gap commonly cited by recruiters requiring more formal cyber security education and experience.

Civilian mobilisation through levée en masse

The levée en masse strategy was first applied in a French revolutionary context, employing education and ideology through mass forms of communication to stimulate an inspirational uprising, driving young men to the Army.

Global cyber conflict has seen this strategy reimagined in Ukraine, where the 'IT Army of Ukraine' mobilised 184,000[19] civilians to a common cause in wartime, and in China where a civilian 'guard force' of white hat hackers[20] defended networks during a major national event.

Cyber mobilisation through the levée en masse strategy works – and can also significantly influence the broader social, ideological and political elements of a nation state in a digital crisis.

[19] https://techcrunch.com/2022/02/27/ukraine-takes-the-resistance-to-cyberspace-assembling-an-it-army-to-hack-sites-from-russia-and-its-allies-calls-on-tech-leaders-to-get-involved/

[20] https://web.archive.org/web/20220109024711/http:/bj.people.com.cn/n2/2022/0105/c82840-35082965.html

There are two approaches to the scalable remote workforce:

Standby (proactive):

A nationally managed, commonwealth-funded civilian cyber contingency reserve of paid and unpaid digital volunteers who are regularly trained to enhance community cyber resilience, response and recovery.

Emergency (reactive):

Rapid mobilisation of unpaid civilian cyber volunteers to support the Australian Government in an information and cyber warfare scenario by providing a robust, whole-of-country mechanism.

Standby Digital Corps

The NDES would have a similar model to the SES and RFS in that it would be a majority volunteer organisation with a small group of full-time staff to organise and administer the organisation. It would not only prepare for and respond to cyber events, but it would have the ability to provide a 'on call' red team to facilitate scenario-based exercises for government, business and not for profit organisations.

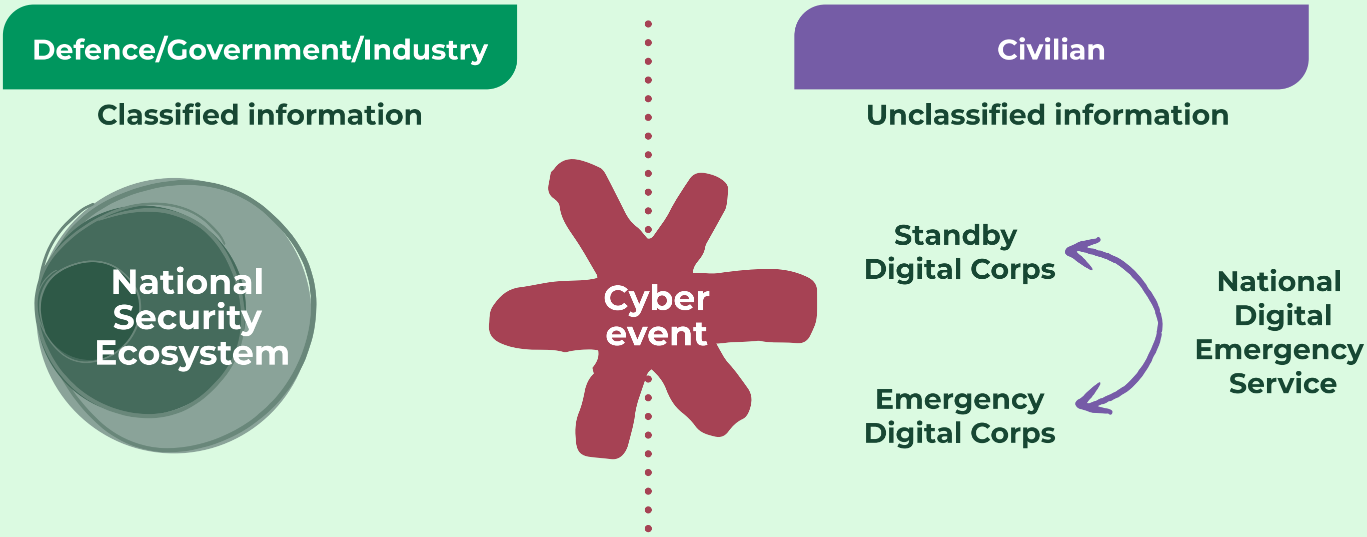
Although the NDES could be developed around major cities and leverage existing Joint Cyber Security Centre infrastructure, the benefit of having a digital citizen force would be the ability to scale a remote capability at speed.

NDES members would deal with unclassified information, negating the requirement for protected networks. There's also often a long tail to cyber incidents that is beyond the initial technical breach, the NDES would be a good option for ASCS and the proposed NSE to shed non-classified tasks that bleed resources.

NDES members could help public sector companies improve their security posture through bug bounties, a way of incentivising ethical hackers to find vulnerabilities in a company's systems and report them to the company. This saves costs and builds a more transparent and collaborative culture.

Emergency Digital Corps

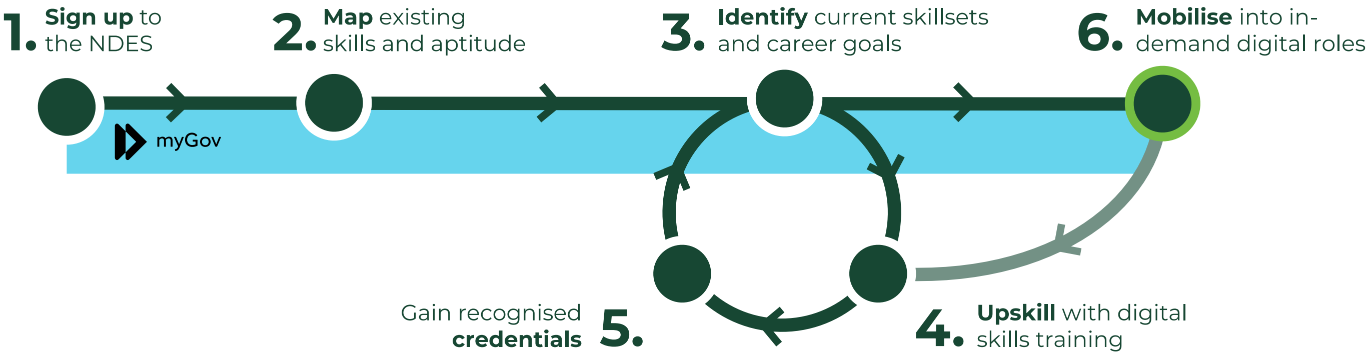
Rapid mobilisation of civilian cyber volunteers would support the Australian Government in an information and cyber warfare scenario by providing a robust whole-of-nation mechanism to facilitate citizens defending their own personal data, countering the spread of misinformation and disinformation, and providing a civilian cyber show of force. Maintaining the ability to rapidly scale a civilian cyber workforce will also reduce the cyber capability overmatch favouring nefarious state and non-state actors, both in the size of their cyber forces, and their capacity to build the cyber warriors that make up their organisations.



The National Digital Emergency Service Platform

To enable this standby and emergency ‘cyber levée en mass’, a database would be required to hold the details of cyber volunteers, a skills mapping capability to identify and collect individual's skillsets, a platform on which to deliver training and provide micro credentialling, and a mechanism for command, control and communication.

This database and platform solution(s) would need to be unclassified, secure and mobile-enabled, enabling accessibility to all Australian citizens. Integration into the MyGov platform would facilitate a seamless opt in method to capture individuals' personal data and provide a secure database to hold citizens digital skills credentials.


1. Sign up to the NDES
2. Map existing skills and aptitude
3. Identify current skillsets and career goals
6. Mobilise into in-demand digital roles
myGov
Gain recognised credentials 5.
4. Upskill with digital skills training

Step 1: Sign up

Upon signing up to the NDES, individuals onboard to the platform by providing basic details and uploading their resume which is skills mapped to the SFIA skills framework through AI.

Step 2: Map

Sociocultural and learning style mapping (such as described in the proposed Pacific Resilience Project) is completed to understand an individual's aptitude and potential for learning digital skills. A comprehensive ‘skills potential’ profile is provided to the individual.

Step 3: Identify

Based on an individual's current skillset, digital literacy (skills mapping), sociocultural testing results, and their career goals, training pathways will be customised through stacking micro-credentials aligned to the SFIA framework.

Step 4: Upskill

Practical, low cost and high-quality digital skills training enabling all individuals to complete training around their own schedule, which is ideal for the remote standby and emergency volunteer models.

Step 5: Credentials

Upon meeting the course requirements individuals would be issued with industry certified credentials. This not only benefits the individual in their professional development and competitiveness in the skills marketplace, but would enhance the standing of the Australian Government as a legitimate training provider, facilitating digital skills for free.

Step 6: Mobilise

Through a mobilisation platform, the supply and demand requirements of the Australian Government would be fulfilled by the merging of a social network, marketplace and innovative technologies. By combining these three development and retention strategies, the NSE could benefit by improving demand resolution and increasing talent supply.

Crowdsourced analysis

A scalable remote workforce would be an effective way to deliver crowdsourced analysis of threats during a cyber event. Crowdsourcing is a method of gathering information or resources from a large group of people over the internet, to solve a problem or complete a task. In the case of a cyber event, crowdsourcing could be used to gather information about potential threats or to analyse data to identify patterns or vulnerabilities. The problem set could be compartmentalised by a command and control entity to remove security classifications, removing the requirement for AGSVA clearances.

Crowdsourced response

This approach could also be employed to provide a crowdsourced response to cyber events. A platform could be rapidly created to track and manage the progress of response efforts in real-time, including identifying and prioritising tasks, assigning responsibilities, and monitoring the status of ongoing activities.

Scalable remote workforce benefits include:

1. **Faster response times:** With a remote workforce, government agencies can quickly mobilise personnel to respond to cyber threats. Remote workers can be activated quickly and can begin working on the problem from their own locations, without the need for physical travel.

2. **Increased flexibility:** A scalable remote workforce allows government agencies to scale up or down their response efforts depending on the severity of the cyber threat. This flexibility can help agencies to better manage resources and respond more efficiently to threats.

3. **Cost savings:** Remote work can reduce costs associated with travel, equipment and office space. With a remote workforce, government agencies can save money on these expenses and redirect those funds to other important areas of their cyber operations.

4. **Improved collaboration:** Advances in technology have made it easier for remote workers to collaborate and communicate with one another. This can help government agencies to work more effectively as a team, even when individuals are in different locations.

National Security Ecosystem collaboration

The platform that facilitates the crowdsourcing process would be designed to allow remote workers to securely access and analyse data in real-time, collaborate with each other, and communicate with emergency responders or other relevant stakeholders.

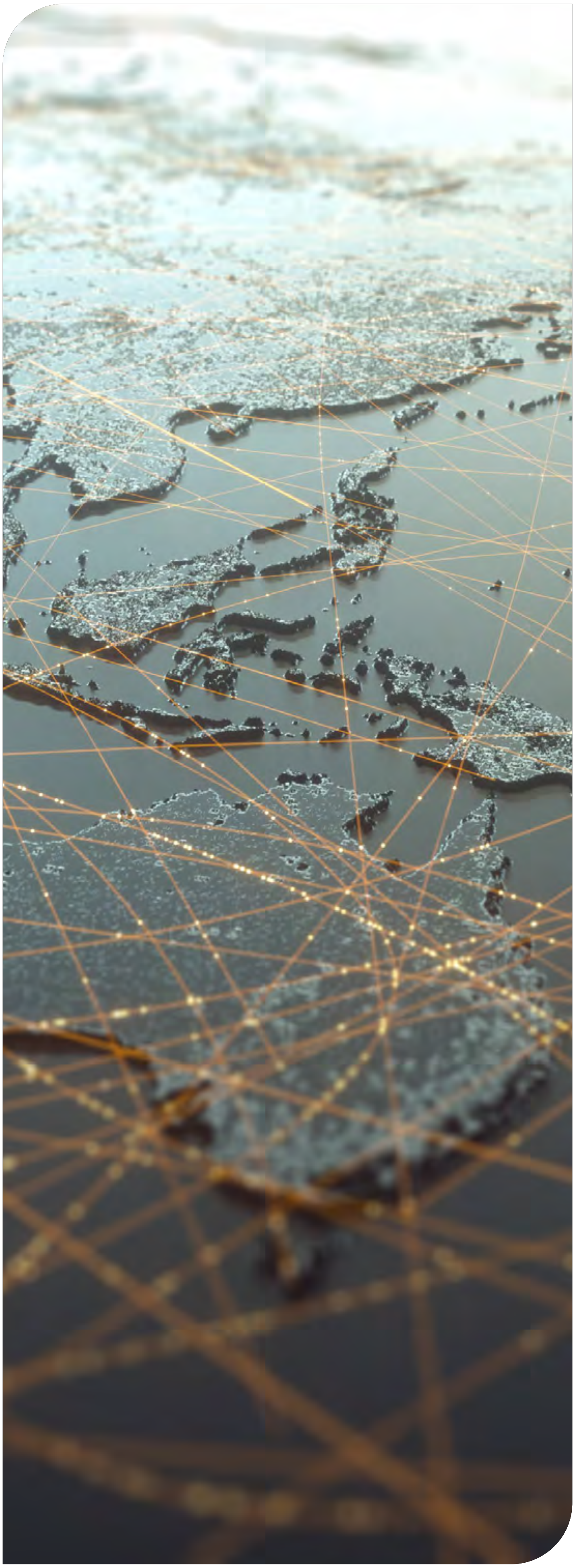
To ensure the quality and accuracy of the crowdsourced analysis and response, guidelines and protocols would be established for individuals to follow, including best practices for data analysis, threat identification and information sharing.

Removing barriers to entry

Skills underpin all work. They are the driving elements in all industry and individual enterprise – and they are always evolving. Cyber skills development must transform in order to be ready for the future of work after a fourth industrial revolution: where learning is no longer separate from doing; where we immerse learning in work environments.

NDES members would be encouraged to express interest in available projects and tasks based on their skills, availability, lifestyle and circumstance. Success would be measured on work quality, productivity and outcome, not attendance. This initiative would aim to improve the utilisation of time, enabling the ability for tasks to be generated and completed in a decentralised 'gig-economy' structure and capitalise on recent market changes caused by disruptive technology platforms.

The Australian Government can develop an NSE, bolstering our ability to respond to evolving challenges as they appear. The skills ecosystem concept emphasises the inter-dependency of component actors when getting the skills equation right – representing a shift in focus from positions, vacancies and employment to tasks, outcomes and projects.



About WithYouWithMe

WithYouWithMe (WYWM) was founded in 2016 with the vision to solve veteran underemployment by providing free up-skilling opportunities and job matching aligned with in-demand digital careers, without the need for a university degree or job experience. This vision has evolved to a point where we now help thousands of veterans, military spouses, neurodivergent people, women in technology, and Indigenous Peoples around the world to find meaningful careers. We offer training pathways to members of these communities for free, funded by our client engagements which provide organisations with access to our workforce insights platform and talent mobility solutions.

Working with Defence and Government across the Five Eyes, WYWM's world-class and industry-leading training Cyber Academy and talent platform has been designed from the ground up to meet the needs of Five Eyes Governments and defence forces. Known as Potential, WYWM's platform is designed to discover untapped human talent and rapidly enable them to become cyber warriors. Potential can be used by nations in times of cyber emergency or urgent need to quickly mobilise cyber recruits.

Potential is the world's only complete end-to-end talent identification and training platform, rapidly reducing the amount of time it takes for a cyber operator to reach a minimum viable operational state. Our sociocultural mapping is proven to reliably predict which skills an individual has the strongest propensity to learn and then then providing those candidates with a guided training pathway and allowing those who wish to learn the ability to become basic cyber warriors in weeks and months instead of years... and for those with even greater aptitude, Potential offers advanced training opportunities to train them for more senior offensive cyber roles. There is nothing out there comparable to rapidly build cyber attackers and cyber defenders.

Details of the respondent as applicable:

Tom Larter
WithYouWithMe
Alexandria, NSW 2015

Registration date: 31/10/2016

ACN: 615621577

ABN: 70615621577

ASIC: 615621577

WITHYOUWITHME