1 November 2019

Cyber Security Policy Division
Department of Home Affairs
4 National Circuit Barton
ACT 2600
Submitted via online form

Re: Australia's 2020 Cyber Security Strategy -- A Call for Views

Introduction

Access Now is an international organization that defends and extends the digital rights of users at risk around the world. As part of this mission we operate a global Digital Security Helpline for users at risk to mitigate specific technical threats. We work directly with lawmakers at national and international forums to ensure policy decisions are focused on users and those who are most vulnerable. We also host RightsCon, the world's leading conference on human rights in the digital age.

Access Now, through its Digital Security Helpline, is a member of the Forum for Incident Response (FiRST), the leading global incident response network.[1] We are founding members of CiviCERT, a coordinating network of help desks for civil society whose goal is to improve the incident response capabilities of its members and share information on threats that affect NGOs, journalists, and other human rights defenders around the world. We support emerging regional and community-based help desk efforts to further close the gap between those in need and mechanisms of support.

Over the past years we have contributed extensively to Australia's public consultations (both in writing and in person); we submitted input to Australia's International Cyber Engagement Strategy and we have been actively providing commentary and suggestions to the ongoing review of Assistance and Access Act (TOLA). We work with a network of Australian digital rights and human rights organizations that understand the critical nature of protecting the digital rights of users. We coordinate frequently with academics, technologists, and the private sector to advance Australia's human rights compliance in the digital age.

General remarks

First of all, thank you for submitting the 2020 Cyber Security Strategy up for review and public consultation, allowing all stakeholders a part in the process of shaping Australia's direction in this critical field. Australia has been an increasingly active player in the space

[1] https://www.accessnow.org/first-digital-security-helpline/

internationally, notably because of its appointment of an Ambassador for Cyber Affairs and in part as an active member of the UN's Group of Governmental Expert (GGE) on Advancing responsible State behaviour in cyberspace.

In 2017, Australia launched a new International Cyber Engagement Strategy, intended to expand on "how Australia will attain global responsibility and influence in cyberspace."[2] It includes goals in eight subject areas ranging from human rights and democracy to cybersecurity. In response, Access Now wrote to Tobias Feakin, Australia's Ambassador for Cyber Affairs, explaining that while the strategy makes mention of the rights to freedom of expression and association, it fails to show similar regard for privacy, not referring to it as a right and making reference only to "arbitrary interferences" to privacy instead of unlawful, disproportionate, and unnecessary infringements.[3]

And while many of the goals in the strategy are laudable and seek to establish Australia as a regional and global leader, it fails to recognize how the government's own current actions, including engagement in government hacking and threats to encryption under the Assistance and Access Act (TOLA), actually run counter to the commitments in the document.[4] This is an important and significant challenge for Australian public policy that must be addressed - including as part of this current consultation on Australia's 2020 Cyber Security Strategy led by the Department of Home Affairs. Additionally, there is a continued need to develop and grow the Cyber Engagement Strategy, which should be reviewed and held to a public consultation in the short-term.

In the same breath, it should be noted that the most striking change in the 2020 Cyber Security Strategy is the departure from the 2016 commitment to championing an "open and secure Internet."[5] The departure from this language, paired with the overall emphasis on government's role and authority over domestic networks and cybersecurity products and services is a shift to the detriment of Australian consumers.[6] The language of the 2020 strategy shouldn't be based on the premise that the commitments regarding championing an open and secure internet made in the 2016 plan have been met and therefore do not need to be reiterated. For consistency, both domestic and international, we recommend that the language is edited to reflect the objectives that the previous strategy held.

In our 2018 report Human Rights in the Digital Era: An International Perspective on Australia, we concluded our analysis of the cybersecurity environment with these four key recommendations:

---

[2]http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/part_6_human_rights_and_democracy_online.html.
[3]https://www.accessnow.org/cyber-engagement-strategy-australia-overlooks-threats-user-rights/.
[4]*Id.*
[5]https://www.industry.gov.au/data-and-publications/australias-tech-future/cyber-security/what-is-the-government-doing-in-cyber-security
[6] As mentioned in Appendix A, point 4, research was undertaken to better understand the cost of malicious cyber attacks to the Australian economy. This was "overtaken by a classified review." We would encourage the government to declassify this assessment in order to deepen stakeholder understanding of the threat landscape and be able to meaningfully contribute to shaping a response.

1. Commit to building cybersecurity policies and practices around central tenets of human rights, including the right to privacy. This includes compliance with the government's own Cyber Engagement Strategy commitments on human rights and democracy;[7]
2. Evaluate government hacking law and practice with the goal of either ending the practice or, at minimum, codifying statutory safeguards to protect human rights;
3. Ensure representatives from civil society and the public are meaningfully included in cybersecurity policy-making, including the ability to participate in drafting key documents; and
4. Strengthen data breach notification in Australia to ensure full compliance by the public and private sectors.

Below we will develop this position to reflect the narrative and concerns laid out in the 2020 Cyber Security Strategy discussion paper.

Analysis: Cyber Security Strategy 2020

1. What is your view of the cyber threat environment? What threats should Government be focusing on?
2. Do you agree with our understanding of who is responsible for managing cyber risks in the economy?
3. Do you think the way these responsibilities are currently allocated is right? What changes should we consider?

The numbers presented in the discussion draft suggest that Australia is currently lagging behind in cybersecurity.[8] Identity theft in Australia alone bears a similar cost as in the UK, even though the UK has three times the population. What are the reasons behind these disparities? The government's strategy must be to assess this against global indicators and then to address these issues systematically; starting with critical infrastructure and the security of the government's own publicly facing services. This approach should be guided by a cybersecurity audit of past and present government programs, ranging from healthcare databases and previous breaches, to the myGovID and any other programs which aggregate individuals' data.[9] Without proper cybersecurity practices, these programs expose individuals to the very risks enumerated at the introduction of this section.[10] Due to the complexity and cost of maintaining such connected government services, in the future a cybersecurity risk assessment by the Australian Government should preclude any such program or database from being undertaken, with a special focus on potential risks to minority and marginalized

[7]https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/part_6_human_rights_and_democracy_online.html
[8]https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-strategy-2020-discussion-paper.pdf
[9] Interestingly there is an ongoing consultation of the ACCC Report on Digital Platforms which makes extensive note of the need to further (re)define various data categories and ensure they are subject to robust safeguards according to those levels. Several of the recommendations made by the ACCC would ensure privacy and security for users, and should be considered by the Home Office.
[10] https://www.businessinsider.com.au/victoria-drivers-licence-facial-recognition-2019-9

populations. A cybersecurity review and audit by an independent body, and through an independent process, will ensure that best security practices are upheld and followed regardless of where the governance body of the program is located.

Furthermore, while cybersecurity maintenance is best left to industry and business, the government has to play a regulatory role in making sure that consumers are adequately protected, informed and supported. In this respect, the government has two key responsibilities:

1. Set baseline rules (through regulation/law) for businesses to abide by and,
2. Provide clarity to individuals on how the government enables and supports them.

In the current environment, there is a notable lack of clarity on both. The government should focus on developing a cybersecurity framework which would give clarity and define responsibilities for the private sector -- not unlike the EU's Network and Information Security (NIS) Directive and the EU Cybersecurity Act -- the latter of which introduces a certification framework for connected services and products.[11]

The current allocation of responsibility is with the end-users who are carrying the burden of responsibility and are not guaranteed any rights or remedy when their security is compromised. Aside from giving individuals power to challenge and file complaints when the private sector fails to uphold government-defined rules, the government should work together with its law enforcement to make sure that individuals are given an adequate toolbox to deal with cybercrime. The issues enumerated in the introduction (such as ransomware and phishing) are surmountable through education and provision of public resources.

Individual-oriented initiatives such as the European "No More Ransom" campaign, provide an open resource to individuals as well as SMEs and empower them to take action when they are targeted by cybercriminals.[12] Providing readily available support and education resources is a key government role in mitigating cybersecurity threats in their jurisdiction.

Additionally, the security space would be well served by a clearer separation of powers between bodies responsible for signals intelligence, and those responsible for information assurance (the latter being those trusted with cybersecurity). Such a conflation is not a unique challenge to Australia, but it often results in a more stressful, higher stakes environment for the entire agency. A clear definition of critical infrastructure assets from a cybersecurity priority perspective would also facilitate this clarity.

---

4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?
5. How can Government maintain trust from the Australian community when using its cyber security capabilities?

[11] https://www.accessnow.org/eu-cybersecurity-directive-finalised-the-knights-who-say-nis/
[12] https://www.nomoreransom.org/en/index.html

To elaborate on the above comments, we do acknowledge that there may be situations where law enforcement investigations and intelligence operations face challenges as users and industries shift to more secure online tools, the most common example being encrypted communications. Securing the infrastructure individuals rely on is a net positive for cybersecurity, but it may add complexity to investigations of criminal activity (cyber or not). In reaction to this need to update existing legislative frameworks (as identified in the discussion paper), we developed a human rights respecting approach which should govern government activity in this space entitled *A Human Rights Response to Government Hacking*.[13] We published this report in the hopes that it would give governments a blueprint to pursue regular operations without compromising internationally recognized human rights. We remain convinced that while this is a complex issue, human rights respecting solutions do exist without compromising the integrity of our overall communications security, which is currently sought by haphazard legislative amendments like Assistance and Access Act.[14]

At this point, the discussion paper seems to take a placative tone in saying: “Government’s activity is also regulated strictly by law and subject to extensive external and independent scrutiny to protect the privacy of Australians.”[15] We respectfully submit that this does not reflect the problems caused by the current legal framework and the need for urgent reform flagged by many stakeholders. While certain updates to legislative instruments should be made (we’ve outlined several at this stage), there is no justifiable reason that such measures should come at the expense of good policy making and continued scrutiny to protect the rights of users.

The example used by the discussion paper of the 2019 BlueKeep vulnerability illustrates the need to mainstream information and scale communication to the public about cybersecurity incidents. Ultimately, the responsibility sits with private providers (such as Microsoft, in this illustration) to inform its users through the products they make available (e.g. - the Windows Operating System) and roll the appropriate patch out in a security update. The government should not seek to “proactively identify” any vulnerable systems through technical means, but instead research into which enterprises are most likely to be impacted, paired with a coordinated outreach to inform them of the situation and how to remedy it, is a suitable solution. There are too many potential side-effects from scanning networks, including causing damage to others' systems and networks, to infringing on their privacy. Rather, further to our earlier recommendation, a healthy cybersecurity framework should seek to create a well resourced government office to make sure that individuals and industry have continuous access to an accessible, trusted and well integrated government entity focused on information assurance as a part of a diverse digital security ecosystem, an entity which can support them in time of their need and at their own behest.

[13] https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf
[14] https://www.accessnow.org/tag/assistance-and-access-bill/
[15] Available on pg. 9 of the 2020 discussion paper: https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-strategy-2020-discussion-paper.pdf

That said, the focus on handling vulnerabilities is timely.[16] Vulnerabilities are common and will always exist; the important thing is how we respond when we discover them. Several large-scale attacks over the past few years, such as the devastating WannaCry attack, were conducted by leveraging vulnerabilities that governments already knew about but kept secret, to stockpile for use against strategic targets. We can help stem the tide of attacks like this, but only if governments make a stronger commitment to a vulnerability disclosure process that appropriately prioritises defense of our digital security, vital systems, and infrastructure.[17]

At Access Now, we advocate that governments not only have a vulnerability disclosure process for when they find or become aware of technology flaws, but also that governments facilitate coordinated vulnerability disclosure (CVD) for industry.[18] The latter approach is systemic, responding to the issues that create a less secure environment for everyone. It includes making changes that support disclosure and patching of vulnerabilities, such as avoiding criminalizing security research (like Argentina tried to do)[19] and instead giving leeway to prosecutors in related cases (the way the Netherlands have).[20]

We therefore recommend that the Australian government implement a vulnerabilities equities process for its own operations as well as a vulnerability reporting policy for government provided services and own institutions. The latter should be supported by clear language protecting the rights of security researchers (as opposed to treating them as a malicious actor), tempered with a clear delineation of the reporting process and responsibilities. In order to achieve its cybersecurity objectives, we further recommend that the government promote and support the development of coordinated vulnerability policies for all entities operating in its jurisdictions, making sure that it promotes and protects a culture of cybersecurity research and community cooperation.

---

6. What customer protections should apply to the security of cyber goods and services?
7. What role can Government and industry play in supporting the cyber security of consumers?
8. How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?
9. Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?
10. Is the regulatory environment for cyber security appropriate? Why or why not?
11. What specific market incentives or regulatory changes should Government consider?

[16] Similar conversations have been advanced in the US and EU both at the institutional and national level: https://www.accessnow.org/the-eu-needs-to-get-serious-about-fixing-vulnerabilities/
[17] https://www.accessnow.org/wannacry-shows-need-cybersecurity-defense-not-offense/
[18]https://www.accessnow.org/meltdown-spectre-need-better-vulnerability-disclosure-stronger-u-s-cyber-framework/
[19] https://www.accessnow.org/argentina-dont-criminalize-security-research-e-voting/
[20] https://www.ncsc.nl/english/security

Cybersecurity is a multi-faceted, broadly defined subset of digital security that, according to multi stakeholder and standard setting bodies, encompasses "the availability, confidentiality, and integrity of information and its underlying infrastructure."[21] Governments around the globe have increasingly framed privacy and other human rights as antithetical to public safety and national security, stigmatizing valuable digital security tools. As a result, cybersecurity laws and policies often interfere with human rights or adversely undermine the security they seek to improve.

As mentioned in the first section of our response, the government should not proceed with its 2020 Cyber Security Strategy without committing to a full audit of existing legal instruments and programs which may be perpetuating a systemic insecurity to the Australian digital environment. This system insecurity would be in addition to the cost that such instruments and programs bear on the reputation and trust of Australian cybersecurity services and products abroad.[22]

---

12. What needs to be done so that cyber security is 'built in' to digital goods and services?
13. How could we approach instilling better trust in ICT supply chains?
14. How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?
15. Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

N/A

---

16. How can high-volume, low-sophistication malicious activity targeting Australia be reduced?
17. What changes can Government make to create a hostile environment for malicious cyber actors?
18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?
19. What private networks should be considered critical systems that need stronger cyber defences?
20. What funding models should Government explore for any additional protections provided to the community?
21. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

[21] https://freeandsecure.online/definition/
[22] https://www.itnews.com.au/news/australias-anti-encryption-laws-ridiculed-on-world-stage-520197

“Between those two ends of the spectrum lie a range of actions – mid-level capabilities. Such measures can include gathering information on actors targeting Australia, sharing advice on hostile activity between entities involved in defending networks or blocking known malicious actors. Australia already works closely with international partners to share information and build support for international rules and norms to govern the responsible use of cyberspace.”[23]

Several of the largest breaches of the integrity of global cyber systems have been traced to government operations -- whether an intelligence agency was reckless and did not disclose a vulnerability or a government seemingly knowingly made a decision to undermine hardware.[24] Governments should work together, and with other stakeholders, to publicly condemn government hacking, especially hacking that implicates critical infrastructure or the building blocks of connected systems. They should commit not to engage in government hacking of internet infrastructure and use diplomatic pressure to get other governments to do the same, subject to meaningful accountability mechanisms. Where government hacking is already taking place,governments must ensure it is subject to a law with affirmative safeguards, the deliberation of which legislators should take up promptly.

As noted previously, governments should also pledge to notify impacted users when attacks like this are discovered. This is precisely why Coordinated Vulnerability Disclosure (CVD) or processes like the Vulnerabilities Equities Process (VEP) in the U.S. exist. People cannot be incidental damage in online battles between governments. User-centric vulnerability disclosure policies should be referred to and supported in all Australia cyber dialogues, cyber capacity building with states, work in Indo-Pacific region and other key allies and partners.

It is not likely that we will see commitments like these arise in the cybersecurity processes that are led in silos by military interests. Governments should therefore lead an open and pluralistic discussion on appropriate limitations to cyber operations. Moreover,governments should mandate civilian agency leadership on government cybersecurity policy. While some refer to attacks on companies as “cyberwar,” this military framing can only lead to even more harm to users.[25] It suggests solutions ought to be led by the military and driven by conflict, but it is essential to avoid militarization of the internet to promote and protect the rights of users.

Importantly, while we haven’t yet established these global commitments and norms, we are seeing steps in this direction. Bodies at the United Nations have addressed government interference with hardware supply chains. The U.N. General Assembly adopted a report by a U.N. Group of Governmental Experts on Information Security (GGE) that condemned interference with the supply chain and the use of harmful hidden functions.[26] While the GGE

[23] Available on pg. 14 of the 2020 discussion paper: https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-strategy-2020-discussion-paper.pdf

[24]https://www.accessnow.org/hardware-questions-about-government-hacking-what-if-the-bloomberg-story-is-true/

[25] https://www.accessnow.org/cms/assets/uploads/2018/08/DGC-tech-accord-human-rights.pdf

[26] http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

was unable to reach consensus on its last report, the new Group of Governmental Experts - as well as the work of the Open Ended Working Group that was initiated - holds great promise. Regardless of the result, it is essential that a continued consultative engagement with civil society is maintained to ensure that the resulting measures work for the security of individual users.

In addition, global consensus on the specific harm of government hacking is growing; at the 39th session of the United Nations Human Rights Council, a resolution on the safety of journalists identifies government-sponsored hacking as a threat.[27]

Companies have internal responsibilities too. They must evaluate the risks of their operations to human rights and take measures to prevent and mitigate any harms. For hardware vendors, those harms can range from labor abuses and environmental damage in their supply chains to "value chain" abuse, such the theft of intellectual property and the pilfering of users' data. The U.N. special rapporteur for freedom of opinion and expression has brought attention to contracts between the companies, to ensure "all parties uphold their human rights responsibilities."[28] Likewise, once they identify risks, companies should develop rights-respecting policies, use their business relationships to ensure suppliers uphold principles protecting users, and, through human rights due diligence, reduce opportunities to subvert product security. This may mean that more companies move their supply chains out of jurisdictions where threats of interference or manipulation are high.
In order to ensure respect for user rights, companies should commit to conduct regular audits that cover supply chains across the sector. Those commitments should be backed by strong global norms and national laws that protect user data and ensure corporate accountability.

---

22. To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?
23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?
24. What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?
25. Would you like to see cyber security features prioritised in products and services?

N/A

[27] http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/39/L.7
[28]https://freedex.org/recommendations-to-companies-in-the-internet-and-telecommunications-access-industry/