CYBER NORMS

& THE AUSTRALIAN PRIVATE SECTOR

A S P I
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

INTERNATIONAL
CYBER POLICY
CENTRE

ACKNOWLEDGEMENTS

The author would like to thank Dr Tobias Feakin who was instrumental in delivering and facilitating the participant workshop and Mr Klée Aiken who at several stages provided valuable comments on the content and structure of the publication.

Finally a very special thank you to the private sector participants who enthusiastically shared their opinions and expertise and set aside their valuable time to contribute to both the workshop discussion and feedback surveys.

ABOUT THE AUTHOR

Jessica Woodall joined ASPI in April 2013. She is currently working in ASPI's International Cyber Policy Centre researching and writing on international and domestic cybersecurity issues. She specialises in Australia's international cyber engagement, global risk reduction and conflict prevention efforts, and domestic cyber policy formation and implementation. Before joining ASPI Jessica worked as an analyst in the Department of the Prime Minister and Cabinet and as a researcher in Queensland's Department of the Premier and Cabinet. Jessica holds a Master's degree in International Affairs from the Australian National University.

WHAT IS ASPI?

The Australian Strategic Policy Institute (ASPI) was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI INTERNATIONAL CYBER POLICY CENTRE

The ASPI International Cyber Policy Centre (ICPC) brings together the various Australian Government departments with responsibilities for cyber issues, along with a range of private-sector partners and creative thinkers to assist Australia in creating constructive cyber policies both at home and abroad. The centre aims to facilitate conversations between government, the private sector and academia across the Asia–Pacific region to increase constructive dialogue on cyber issues and do its part to create a common understanding of the issues and possible solutions in cyberspace.

The ICPC has four key aims:

- Lift the level of Australian and Asia–Pacific public understanding and debate on cybersecurity.
- Provide a focus for developing innovative and high-quality public policy on cyber issues.
- Provide a means to hold Track 1.5 and Track 2 dialogue on cyber issues in the Asia–Pacific region.
- Link different levels of government, business and the public in a sustained dialogue on cybersecurity.

We thank all of those who contribute to the ICPC with their time, intellect and passion for the subject matter. The work of the ICPC would be impossible without the financial support of our various funders, but special mention should go to the Commonwealth Bank, which has been a strong advocate and supporter of our work since the centre's inception.

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

CommonwealthBank

AN AUSTRALIAN PRIVATE-SECTOR APPROACH TO CYBER NORMS

The magnitude of cyberspace can confound policymakers. The cybersphere touches almost every corner of our government, has become embedded in our defence and security discourse and enables our civil society.

It emboldens free speech and drives development and education, reaching into our homes and schools. Cyberspace also underpins our business, industry and innovation environments, and is now a modern pillar of the global economy.

Since the advent of the internet, international society has struggled with ideas about how to manage this new, continually evolving, uncontrolled frontier. Domestically, nations have moved to establish legislation dictating what goes online and what doesn't, but internationally, where states have widely differing interpretations on everything from cyber arms control and freedom of speech to what constitutes cyberspace, the legislative route is filled with pot-holes.

Many have looked to cyber norms to fill the breech. Norms in their simplest form are defined as shared expectations of proper behaviour.[1] They can evolve to keep pace with technological change and have the ability to incorporate the voices of multiple actors. Currently, there's an ongoing international discussion taking place to formulate and embed norms for responsible state behaviour online. Norms, alongside international law, have emerged as the pre-eminent means to establish what's acceptable in global cyberspace, with the long-term aim of maintaining stability and preventing conflict.

Tangible international norm formation has taken place in many different forms, including academic and non-government led processes, but state-based forums such as the UN and the Shanghai Cooperation Organisation are where the most concrete norm formation takes place.[2]

Australia, and many other like-minded nations, pursue the idea of multistakeholder governance of the internet—in which the ownership and management of the internet are shared and the voices of all actors are heard and recognised.

[1] Finnemore M 2011. 'Cultivating international cybernorms', America's cyber future: security and prosperity in the Information Age, p. 90, http://citizenlab.org/cybernorms2011/cultivating.pdf.

[2] Osula A-M, Rõigas, International cyber norms: legal, policy and industry perspectives, NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) Publications, Tallinn, p. 13, https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch1.pdf p.13

As owners and operators of a large amount of the world's internet infrastructure and expertise, private-sector organisations are some of the best-placed bodies to speak authoritatively on the nuts-and-bolts functioning of cyberspace. At a practical level, the private sector also remains critical to the effective implementation of norms and ongoing compliance monitoring, which are some of the biggest hurdles on the track to the legitimisation of the cyber norm model.

Several large companies, including Microsoft[3] and Symantec,[4] have led the charge for private-sector engagement in the cyber norm formation, both independently and within forums such as the International Cyberspace Conference process and workshops conducted by the UN Institute for Disarmament Research.[5] Unfortunately, they and other businesses have been excluded from providing direct input to higher level norm deliberations, such as at the UN Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security (UNGGE), and have been resigned to taking part in more passive, one-way dialogues that have limited ability to influence higher level deliberations. Excluding the private sector from a process that will ultimately bind it is arguably damaging to the ultimate success of cyber norms and counter to the idea of a multistakeholder internet.

From an Australian perspective, our government has played a small but disproportionally influential role in norm formation through leadership roles in the UN and as a norms champion in the Asian region. But, similar to international experiences, the Australian private sector's involvement in this process has been largely absent.

Previously, some in government and the academic community have excused this lack of involvement by suggesting that the private sector has no interest in engaging in cyber norm formation due to a belief that it will have little success in influencing government cyber policymakers, or a fear that norm advocacy will result in increased, unwanted regulation.[6] That view is misguided and underestimates the interest, knowledge and appetite that lies in the private sector for global cyber issues and the receptiveness in government for new private-sector ideas.

[3] Nicholas P 2016. 'Cybersecurity norms: from concept to implementation, Microsoft Secure Blog, 8 February, https://blogs.microsoft.com/cybertrust/2016/02/08/cybersecurity-norms-from-concept-to-implementation/

[4] International cyber norms: legal, policy and industry perspectives, NATO CCD COE, https://ccdcoe.org/multimedia/international-cyber-norms-legal-policy-industry-perspectives.html.

[5] UN Institute for Disarmament Research and Center for Strategic and International Studies, 'List of participants', The application of international law in the context of international cybersecurity, International Security Cyber Issues workshop series, 19–24 April 2016, Geneva, www.unidir.org/files/medias/pdfs/list-of-participants-eng-0-666.pdf.

[6] American Bar Association et al. 2012, A call to cyber norms: discussions at the Harvard – MIT – University of Toronto Cyber Norms Workshops, 2011 and 2012, p. 34, www.americanbar.org/content/dam/aba/uncategorized/GAO/2015apr14_acalltocybernorms.authcheckdam.pdf.

To gain a deeper understanding of private-sector perspectives on cyber norms, ASPI conducted a workshop and survey series with experts from some of Australia's largest and most influential private-sector organisations. ASPI sought to gauge the private sector's interest in and opinions on norms, their impact on the sector, how governments can better engage with the sector in norm formation and which norms are enablers of economic growth and prosperity.

Those surveyed included representatives of the Commonwealth Bank of Australia, Telstra, Origin Energy, Qantas, Google, Fairfax Media, Macquarie Telecom, Baker McKenzie, NBN Co, the Australian Energy Market Operator and the Asia–Pacific Network Information Centre.

The goal of this paper is not to propose that the private sector can be represented by a single set of views or approaches, but to present a set of expert opinions and views that garnered broad support and consensus and those that did not.

DEFINITIONS

In the context of this paper, the term 'private sector' refers to businesses or companies that operate within national and international economies and are separate from NGOs and broader civil society.

While our focus is the private sector, the lessons learned in this study could easily support a model for the broader engagement of civil society actors.

Norms are defined as shared expectations of proper behaviour for an actor with a given identity.[7]

In traditional geopolitics, norms of behaviour were seen to largely emerge in an organic fashion, developing between states over several years, decades or centuries. However, norms for cyberspace have largely been established by states via documents and discussions that seek to codify appropriate behaviours by international agreement, in effect laying out what behaviour's acceptable before historical circumstance can decide which behaviours are appropriate and which are not.

[7] Finnemore, 'Cultivating international cybernorms'.

The 2015 report of the UNGGE explains the role of norms as follows:

> Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. Accordingly, norms do not seek to limit or prohibit action that is otherwise consistent with international law. Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development.[8]

This approach to norm formation may seem contrary to more traditional methods of international statecraft, but in the cyber policy space it's more practicable than pursuing a binding holistic cyber agreement. An overarching international cyber agreement, such as a treaty, is impractical and undesirable for several reasons. Australian Foreign Minister Julie Bishop touched on some of them at the Global Conference on Cyberspace in The Hague last year:

> It is often asserted that we need to conclude an international agreement of some kind on international security in cyberspace. Australia argues that an international agreement is premature; even the work of codifying key principles is in its infancy—the conversation has only just started and the technology is evolving rapidly. It is a challenge for policy makers just to keep up.[9]

States are extremely cautious about foregoing the use of technologies which have yet to be fully developed or exhausted. Additionally, states are wary of binding agreements that may constrain their ability to use cyber weapons or may affect their national sovereignty. The difficulty of attribution also complicates the implementation of cyber treaties, as does the role of third-party actors. The agile, non-binding, inclusive nature of norms has emerged as a realistic solution—one that seeks to embed and socialise behaviours over time via a malleable model that can change to incorporate the technological and political currents of the day.

[8] UN General Assembly 2015. 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' 70th session, item 93, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[9] Bishop J 2015. Statement for plenary session on international peace and security, Global Conference on Cyberspace, 17 April, The Hague, http://foreignminister.gov.au/speeches/Pages/2015/jb_sp_150417.aspx?ministerid=4.

EXISTING BODIES AND EXISTING NORMS

Created by the First Committee of the UN General Assembly the **UNGGE** is currently the world's most visible and pre-eminent body for the creation of cyber norms. Four UN GGEs have been established, producing three consensus reports that have helped to embed the view that international law is applicable to the behaviour of states in the online environment. Since 2012, it has conducted lengthy discussions on which norms should be applied in cyberspace, and the reports drawn from those deliberations are a strong foundation for wider norms discussions at other multilateral and bilateral discussions.

In 2011, **Shanghai Cooperation Organisation** member countries China, Russia, Tajikistan and Uzbekistan first proposed an International Code of Conduct for Information Security in a letter addressed to the UN Secretary General. The letter was the group's first high-level contribution to the emerging norms debate within the UN at the time. The code sought to establish several key principles: the primacy of states in questions of internet governance and information security policy; state sovereignty in cyberspace; and mandated international assistance to 'curbing the dissemination of information' that 'undermines other countries' political, economic and social stability'.[10] After the 2011 code failed to gain much traction, the entire membership of the Shanghai Cooperation Organisation submitted a reworked version of the letter in 2015. Beyond making reference to recent UNGGE reports and softening language on the engagement of the private sector and civil society institutions, little substantive change was made from the first letter.[11]

Several states are now working to incorporate norms for state behaviour into their **bilateral foreign and security policy agreements**. Recent high-profile examples include the US–China Cyber Agreement, which includes norms codifying information sharing and mutual assistance but also a mutual prohibition on conducting or knowingly supporting cyber-enabled theft of intellectual property.[12] This more direct approach to norm formation can be an effective means to circumvent more drawn-out and often watered-down multilateral processes.

[10] UN General Assembly, 'Letter dated 12 September 2011 from the permanent representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General', 66th session, item 93, www.un.org/ga/search/view_doc.asp?symbol=A%2F66%2F359&Submit=Search&Lang=E.

[11] UN General Assembly, 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General' 69th session, item 91, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/02/PDF/N1501402.pdf?OpenElement.

[12] The White House 2015. Fact sheet: President Xi Jinping's state visit to the United States, 25 September, www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

THE IMPACT OF NORMS ON THE PRIVATE SECTOR

As large-scale users and operators of the online environment, private-sector companies can find themselves affected by international cyber norms in three key ways:

- First, some norms directly affect business activities, including norms concerning intellectual property theft, data retention obligations, the preservation of the free flow of information online, supply-chain management, critical infrastructure protection and compliance with information control regimes.
- Second, as the main owner and operator of the internet's infrastructure and information technology expertise, the private sector may be required to alter its operations and management activities to comply with broader behavioural norms applicable to states.
- Third, norms continue to influence the shape and direction of the online environment. As private companies are key users of the internet for commerce, communications and exchange, these changes will affect them as broader internet citizens.

THE CURRENT NORMS DISCUSSION

Given its built-in expertise, size and capacity, the private sector is a logical contributor to cyber norm formation; however, to date, most influential norms discussions have taken place exclusively among governments.

Unsurprisingly, state-centric discussions produce state-centric outcomes. This is not ideal, given that the optimal vision for the internet is one that is multistakeholder, open and inclusive. Whilst this mantra was born in the in the realms of the internet governance debate, it now is being embraced across a number of thematic cyber topics. International norm formation should be no different.

Most existing high-level norms are structured and worded in such a way as to limit the behaviours carried out by or between states. This is problematic, as many of the actions or threats posed in cyberspace are generated by non-state actors, and their remediation is led by private-sector actors. Nationless 'hackers for hire' who target governments, businesses and individuals also challenge this state-led approach. The field of actors in cyberspace is more crowded than in traditional security fields, and the language attached to high-level norms should diversify to present the same limiting conditions, protections and opportunities that are afforded to states online.

WHY INVOLVE THE PRIVATE SECTOR?

According to Martha Finnemore of George Washington University, norms often fail, not necessarily because actors don't like them or there isn't a consensus around them, but because there's a lack of enthusiasm to implement them.[13]

The benefits of opening up the high-level norm formation process are far from one-sided. The private sector, with its reach and influence, should be a key ally and 'norm champion' in the push to embed positive behaviours.

While private-sector capacity building will more often than not be carried out with an eye to broader economic outcomes, a more stable online ecosystem serves all actors, benefits are not constrained to private-sector environments and the goals of governments and the private sector are often intersecting.

Private-sector engagement can assist with the establishment, socialisation and implementation of norms among businesses' customers, other companies and governments. The private sector can lend expertise in the norm formation process to help identify what's achievable, realistic and practicable, help monitor norm compliance and assist in building capacity and creating national environments that are able to adhere to global norms.

To achieve its buy-in, the private sector must be engaged at key points in the norm formation process. This includes but is not limited to: helping to articulate the behaviours norms are trying to prevent, the specific wording of certain norms and the promotion of norms. This will allow states to directly articulate why certain norms are needed and help to achieve broader investment from the private sector in norm implementation.

AUSTRALIAN PRIVATE-SECTOR POSITIONS ON KEY QUESTIONS OF INTERNATIONAL NORMS

ASPI posed a series of questions related to norms to a group of private-sector industry leaders. The questions were separated into three parts:

- Part 1 sought to establish the views of the group on the impact of cyber norms on the Australian private sector.
- Part 2 gauged how to better engage the private sector in norm formation.
- Part 3 assessed opinions on existing and new norms.

[13] Finnemore, 'Cultivating international cybernorms'.

In total, 31 statements were put to the group. The participants were asked to rank their agreement or disagreement with each statement on a scale of 1 (‘strongly disagree’) to 5 (‘strongly agree’). They were also asked to elaborate by providing comments, several of which are included in the analysis of the results below. A full list of the survey questions and the scores received is in the appendix to this paper.

The analysis below is based on the surveys and an in-person workshop discussion held in Sydney.

Part 1: What is the impact of norms on Australian businesses and industries in addition to regional and global stability, and does the private sector have a role in their development?

First and foremost, our discussions and survey sought to gauge the relevance of cyber norms to the Australian private sector. There was consensus among the group that ‘cyber norms have the potential to affect the private sector’ (20% agreed with the statement and 80% strongly agreed). Organisations that had a strong existing or growing regional footprint were particularly cognisant of the impact that norms could have on their operations. One participant neatly summed up the feelings of the group, saying ‘The rules of the road in cyber will affect the private sector as much as any other stakeholder.’

Beyond sector-specific implications, as users of the ‘interconnected ecosystem’ of the internet the group recognised that even norms that aren’t directly relevant to the private sector could affect the ‘functioning of the internet as a whole’ and therefore have secondary consequences for their companies and industries.

Interpretations differed as to whether norms would inhibit or enable economic security and growth. Some experts showed concern that heavy-handed norms proposed by some countries and groups such as the Shanghai Cooperation Organisation could have wide-ranging impacts by ‘disrupting innovation and production, stifling broader economic growth to inhibiting opportunities for companies to grow and expand new markets’.

That said, 80% of the group agreed that ‘on the whole’ norms improved behaviours across a broad range of thematic cyber issues, such as defence and security, economic prosperity and innovation; 20% were uncommitted either way. 70% of the group agreed that norms could help contribute to the formation of uniform approaches to cybersecurity practices across the region and act a useful enabler for business. Again, 30% were unconvinced either way.

When asked whether the private sector should have an opportunity to contribute to the international norms debate, 10% of the group agreed and 90% strongly agreed. Many of the experts argued that the private sector is far from a passive actor in cyberspace and, as a key owner of much of the internet's infrastructure and expertise, has much to offer to this process.

This role was seen to involve three parts:

- advocating in support of existing norms that already align with wider corporate positions
- lending expertise in the shaping and implementation of current high-level norms
- helping to establish new norms, both at the universal level and for behaviours within the private sector.

Existing information-sharing arrangements in the private sector concerning both threats and best practice were highlighted as useful examples that could help inform state-level international discussion. This would in turn lead to norms that were more relevant, more achievable, easier to implement in the long term and 'fit for purpose'. Sixty per cent of respondents agreed that de facto norms that exist in the private sector could be drawn upon to either help shape existing norms or help formulate new ones.

One expert highlighted a spin-off benefit: private-sector contributions to norm formation 'could improve acceptance of norms by the greater private sector community', even if the sector were not directly involved in the norm formation process. There was also 100% consensus among the participants that the Australian and broader private sector could also lend assistance in assessing compliance with international norms.

The statement that 'Governments should lead discussions on international norm formation' elicited the widest disagreement among the group in this section of the survey. Several participants (40%) wished to see the private sector as an equal leader in norms formation, while others (40%) were more circumspect about the ability of the sector to take up such a principal role, instead pointing to the existing expertise, financial backing and diplomatic experience in government as justification for a state-led process.

This view came with the caveat that the private sector should still have an established mechanism for direct input to and influence on norm formation (in effect, 'an equal seat at the table' where businesses' views are recognised and represented). The UNGGE received special attention in this respect: many experts recognised its primacy as the most important global norms formation body, and 90% called for its 'more systematic engagement of the private sector'.

Some participants acknowledge that private-sector involvement could come with some baggage, including the pursuit of 'impractical and unrealistic norms' and the display of overt 'self-interest from larger companies'. While similar critiques could be made of all nation-states in modern international diplomacy, many participants considered that the creation of a complementary and balanced role alongside governments within a well-defined framework was the best means to mitigate this risk for businesses.

Summary of Part 1 positions

Part 1 of the survey established that the private sector:

- sees value in norms formation
- appreciates that norms can affect the global online environment
- wishes to engage in norms formation
- believes that private-sector expertise can help strengthen and implement norms
- seeks to have a voice in discussions at high-level forums, such as the UNGGE.

Part 2: What actions need to be taken to better engage the private sector in the norms formation process, and how can we as a nation best leverage the process?

The second component of our survey sought to establish how difficult it is for the private sector to engage with the concept of cyber norms, and how steps could be taken to simplify and demystify this process.

Most of the expert group (70%) believed that clearer definitions of 'norms' would aid understanding beyond legal and diplomatic practitioners. Ninety per cent believed that a stronger narrative explaining why we're pursuing certain norms would broaden understanding of those norms and aid their implementation. In additional comments, it was suggested that this could be achieved by laying out how norms differ from existing policies, treaties and agreements and what tangible outcome they sought to achieve. Several participants proposed that a conceptual framework presented alongside norms could assist in this respect, particularly one that spoke to the 'value proposition' of norms. Certain participants (20%) argued that the definition of a norm was quite clear, but that more effort was needed to explain norms' significance to the private sector.

Many participants (70%) believed that more clarity could be gained by breaking norms down into the thematic cyber areas that they are targeting, such as cybercrime, cyber espionage or conflict prevention. However, some participants (30%) argued that higher level, broader expectations were more useful in initiating a quicker take-up of responsible behaviours. There was a certain amount of agreement (50% agreed, 20% strongly so) that attaching specific expected behaviours to norms could assist in their quicker, more immediate and uniform implementation. Some participants shared reservations about this measure, as they believed that it's the role of individual states to best determine how they will implement agreed norms.

The expert group was strong (70%) in its opposition to a leading role for the International Telecommunication Union in the internet governance agenda, and was only a little more receptive to the idea of a broad universal regulatory binding instrument housed in the UN (50% against, 20% undecided, 20% for). Several participants suggested boosting direct law-enforcement-to-law-enforcement links as a more effective and preferable route to a binding UN-level treaty. Others also suggested boosting resources and expertise at INTERPOL and working to increase the adoption of the European Convention on Cybercrime (the Budapest Convention).

ASPI next sought to establish how the experts believed Australia should engage in global norm formation. Some participants (20%) agreed that we should pursue our own set of norms that serve our national interest; 40% disagreed, arguing that, while we should look to our national interest, we shouldn't do so to the extent that consensus decisions, broader norm adoption and international cooperation are abandoned.

Dovetailing with this point was 100% agreement that establishing a clear outline of Australia's national objectives in cyberspace will aid the formation of norms that are well suited and relevant to our goals.

The recently announced Australian Cyber Security Strategy includes an undertaking to create a stand-alone international cyber strategy, which with any luck will fulfil this role and assist in the consolidation and dissemination of thinking on our ambitions for cyberspace.

Also mentioned in the cybersecurity strategy was the creation of a new 'cyber ambassador' position within the Department of Foreign Affairs and Trade. The survey group welcomed this announcement; most recognised the role as an easy, high-profile and practical means to engage with the government on norms formation and broader international cyber issues. A participant commented that a 'logical and important first step [of the role will be] reaching out to the private sector'; 100% of participants agreed with that sentiment, and specifically that the new ambassador should work to include the private sector in the government's norms formation process.

Summary of Part 2 positions

Part 2 of the survey established that the private sector:

- believes that clearer definitions, frameworks and narratives attached to norms will assist the private sector to engage with them
- considers that attaching expected behaviours to norms will aid their implementation
- are against a leading role for the International Telecommunication Union in the internet governance debate
- prefer practical law-enforcement-based cybercrime fighting efforts to universal binding treaties at the UN
- deem the pursuit of our national interests in cyberspace to be important, but not at the expense of stifling larger progress in norms formation
- think that we need to establish an understanding of what Australia as a nation wants to achieve in cyberspace
- wishes to engage with Australia's new cyber ambassador on norms formation and broader international cyber issues.

Part 3: What are Australian private-sector opinions on specific emerging and established norms? And what impact would they have upon operations and management?

ASPI sought the group's reaction to a series of specific norms at different levels of acceptance and adoption to gauge participants' general reactions but also to establish how those norms could affect the Australian private sector.

There was 100% support for norms that allow the **free flow of information across borders**, uninhibited by states or other organisations. There was also backing (90%) for norms that **prohibit the use of information security issues as artificial barriers to trade**—specifically, those that present as 'an excuse for anti-competitive behaviour'.

The group was widely supportive (80%) of the norm, backed by the Netherlands Government, that the **internet's public core—its main protocols and infrastructure—should be considered a neutral zone and safeguarded against unwarranted intervention**. Suggestions were made that this norm could be strengthened by altering its wording to include actors other than governments.

Unsurprisingly, there was also relatively strong support (90%) for the norm championed by the US that **'governments should not conduct or knowingly support cyber-enabled**

theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors'. Encouragingly, recent reports indicate that this norm may well be a contributor to a downturn in attacks launched from China against commercial sectors in the US.[14]

Next, ASPI sought to gauge the group's views on three norms specific to the private sector. The first related to the **mandatory incorporation of 'backdoors' into IT products**. There was strong opposition from a majority (80%) of experts to any form of backdoor, and several argued that this would lead to a fundamental weakening in the security of their products. Others accepted that some flexibility on this approach may be necessary for national security reasons, but that such instances 'needed to be carefully managed and the reasons carefully articulated'.

The second private-sector norm posed to the group concerned **private-sector autonomy in supply-chain management**. Fifty per cent of respondents agreed that the private sector should maintain control over its own supply-chain integrity, while others argued that at the consumer product level responsibility must be shared with government. One participant highlighted a stronger role for government in critical national infrastructure oversight, particularly given the dramatic consequences of overlooking assurance processes in favour of less costly alternatives in those sectors.

The last of the private-sector-specific norms posed to the group concerned the **right of companies to 'hack back' following infiltrations of their networks**. This question generated the largest amount of written feedback in our series of surveys. Many participants (60%) were against the right of business to hack back, pointing to problems of attribution and the risks posed to innocent third parties. One simply elaborated that 'You don't respond to a crime by committing another.' Some, while not aggressively advocating for this right, saw the opportunity for future discussion, particularly if the organisations in question 'were better equipped than some governments to investigate an attack on their own networks'. Several participants suggested that the right to hack back could be established alongside a legal framework that considered proportionality, risk, oversight and due diligence processes that allow for zero collateral damage to be tolerated and provide no right to indemnity. Another suggested that perhaps this right could be established and managed in a similar manner to the Australian Government's declared offensive cyber capability; that is, subject to stringent legal oversight and consistent with the international rules-based order and obligations under international law.

[14] FireEye Inc. 2016. 'Redline drawn: China recalculates its use of cyber espionage', FireEye iSight Intelligence, June, www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

The final set of questions posed to the group related to two prospective norms: that **governments should ensure their territories are not used as a base for the unlawful use of ICTs,** or **by terrorist groups to radicalise, recruit and conduct online activities**. Feelings towards these norms were divided, mainly due to global variations in what could be considered 'unlawful use' of ICTs and the use of these norms to crack down on internal dissent and opposition movements. One participant suggested that the UNGGE's use of 'internationally wrongful acts' in place of 'unlawful use' was a more palatable means of dealing with this issue, as it 'clarifies that this norm applies specifically to international law rather than national laws'.

Summary of Part 3 positions

Part 3 of the survey established that the private sector supports norms that:

- encourage the free flow of information across national borders
- prevent the use of information security concerns as artificial trade barriers
- protect the public core of the internet
- prohibit the theft of intellectual property
- prevent the mandatory insertion of 'backdoors' into IT products
- compel countries to crack down on criminal and terrorist use of the internet.

There was an appetite for further discussion on norms relating to:

- the legal right of businesses to 'hack back' following infiltrations of their networks
- the private sector maintaining control of its own supply-chain management.

SUMMARY

Through this discussion workshop and survey series we have established that key Australian private sector actors understands and are interested in the cyber norms formation process. Our expert group had a well-developed understanding of how cyber norms could affect the operations and management of their organisations and the larger online ecosystem as a whole.

In addition, many participants identified opportunities for private-sector collaboration and sharing of best practice when forming, refining and implementing new norms. In this regard, the role of Australia's new cyber ambassador was highlighted as a key means to facilitate engagement with the private sector on international cyber issues.

Finally, the group provided useful insight into which norms participants saw as enablers of economic growth and prosperity and the broader wellbeing of the interconnected online ecosystem.

RECOMMENDATIONS

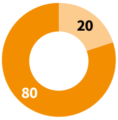
National governments, including the Australian Government, should take the following steps:

- Proactively engage the private sector to gauge businesses' feelings on different behavioural cyber norms and work to create 'norm champions' where interests intersect. Particular areas of focus should be information sharing, critical infrastructure protection, supply-chain management, intellectual property, privacy and data protection plus privacy.
- Identify key stakeholders for specific norms and engage with them to enable better norm formation and implementation. For example, for information-sharing norms, engage with the Forum of Incident Response and Security Teams; the Asia Pacific Computer Emergency Response Team; and financial services and critical infrastructure organisations and companies.
- Assess how international bodies tackling other cross-cutting issues, such as the Financial Action Task Force, have worked to integrate the private sector into their deliberations.
- Provide a direct feed-in route at the UNGGE for private-sector contributions, for example by having the UNGGE invite private-sector organisations to contribute directly to meetings, convene advisory workshops or accept written submissions.
- Foster discussion within industry to establish, within individual business sectors, what responsible private-sector behaviour online looks like.

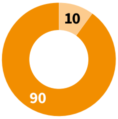
APPENDIX

PART 1 QUESTIONS

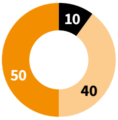
Norms have the potential to affect the private sector.



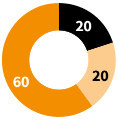
The private sector should have the opportunity to contribute to the international norms debate.



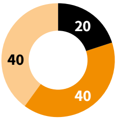
Vocal private sector support of certain state–state norms could help influence their acceptance and implementation.



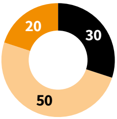
Raising the visibility of cyber issues will help to engage the private sector in norm development.



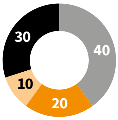
Norms can help to improve behaviours across thematic cyber areas, such as security, economic prosperity and innovation.



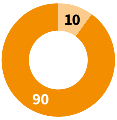
Norms can help establish uniform approaches to cybersecurity practices and regulations across the region.



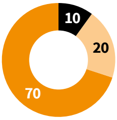
Governments should lead discussions on international norms.



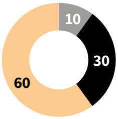
Australia's new cyber ambassador should work to include the private sector in the government's norm formation process.



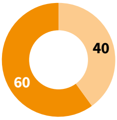
The private sector should have input into international norms discussions such as the UN Group of Governmental Experts.



De facto norms that already exist between private sector businesses, could serve as a model for international norms.



Expertise in the private sector can be used to aid in assessing compliance with international norms.



PERCENTAGE WHO

Strongly agree 🟧

Agree 🟨

Neither agree nor disagree ⬛

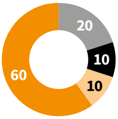
Disagree ▩

Strongly disagree ⬜

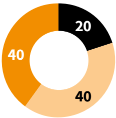
APPENDIX

PART 2 QUESTIONS

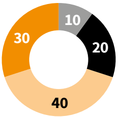
There needs to be clearer definitions around what a norm is to aid understanding and engagement.



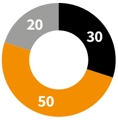
The private sector will be able to better engage with norms if they are presented alongside a clear conceptual framework.



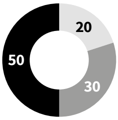
Norms should be broken down into thematic areas such as cyber crime, conflict prevention, online safety, espionage etc. to enable better implementation and comprehension.



If specific expected behaviours are attached to norms, it will enable their quicker immediate implementation.



Australia should work primarily to support and implement norms put forward by allies.



PERCENTAGE WHO

🟧 **Strongly agree**

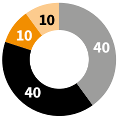
🟨 **Agree**

⬛ **Neither agree nor disagree**

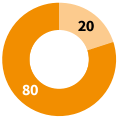
▩ **Disagree**

⬜ **Strongly disagree**

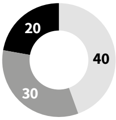
Australia should work to create and implement our own set of norms that serve our national interest.



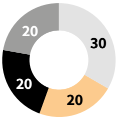
A clear outline of the objectives that we as a nation are trying to achieve in cyberspace will assist in the formation of well-defined and relevant norms.



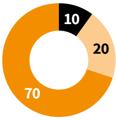
The International Telecommunication Union should be at the centre of the internet governance agenda.



The UN through a broad international universal regulatory binding instrument should have responsibility for combating the use of ICTs for criminal purposes.

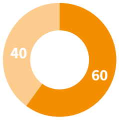


A stronger narrative explaining why certain norms are required will more easily facilitate their implementation and broader comprehension.

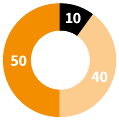


PART 3 QUESTIONS

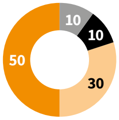
Information must flow freely across borders, uninhibited by states or other organisations.



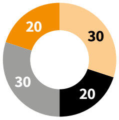
Information security issues should not be used as an artificial barrier to trade.



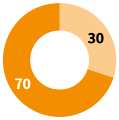
The private sector should not be forced to insert mandatory 'backdoors' into products.



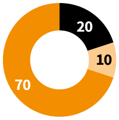
The private sector should manage its own supply chain integrity processes.



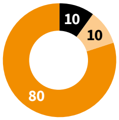
Governments should work to improve transparency around national IT policies and regulations.



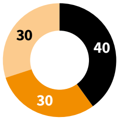
The internet's public core – its main protocols and infrastructure – should be considered a neutral zone, safeguarded against unwarranted intervention by governments.



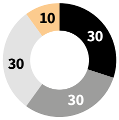
Governments should not conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.



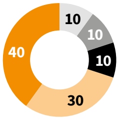
Governments should ensure that their territories are not a base for the unlawful use of ICTs.



Businesses have the right to 'hack-back' following an infiltration of their networks.



States should seek to ensure that their territories are not used by terrorist groups to radicalise, recruit, and conduct terrorist activities using ICTs. States must not knowingly allow terrorists groups to radicalize, recruit, and conduct terrorist activities using ICTs in their territories.



ACRONYMS AND ABBREVIATIONS

NGO	Non-government organisation
UN	United Nations
UNGGE	UN Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

ASPI
Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au
Blog www.aspistrategist.org.au
Facebook.com/ASPI/.org
@ASPI_ICPC
www.cyberpolicy.aspi.org.au

ASPI

AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

INTERNATIONAL
CYBER POLICY
CENTRE