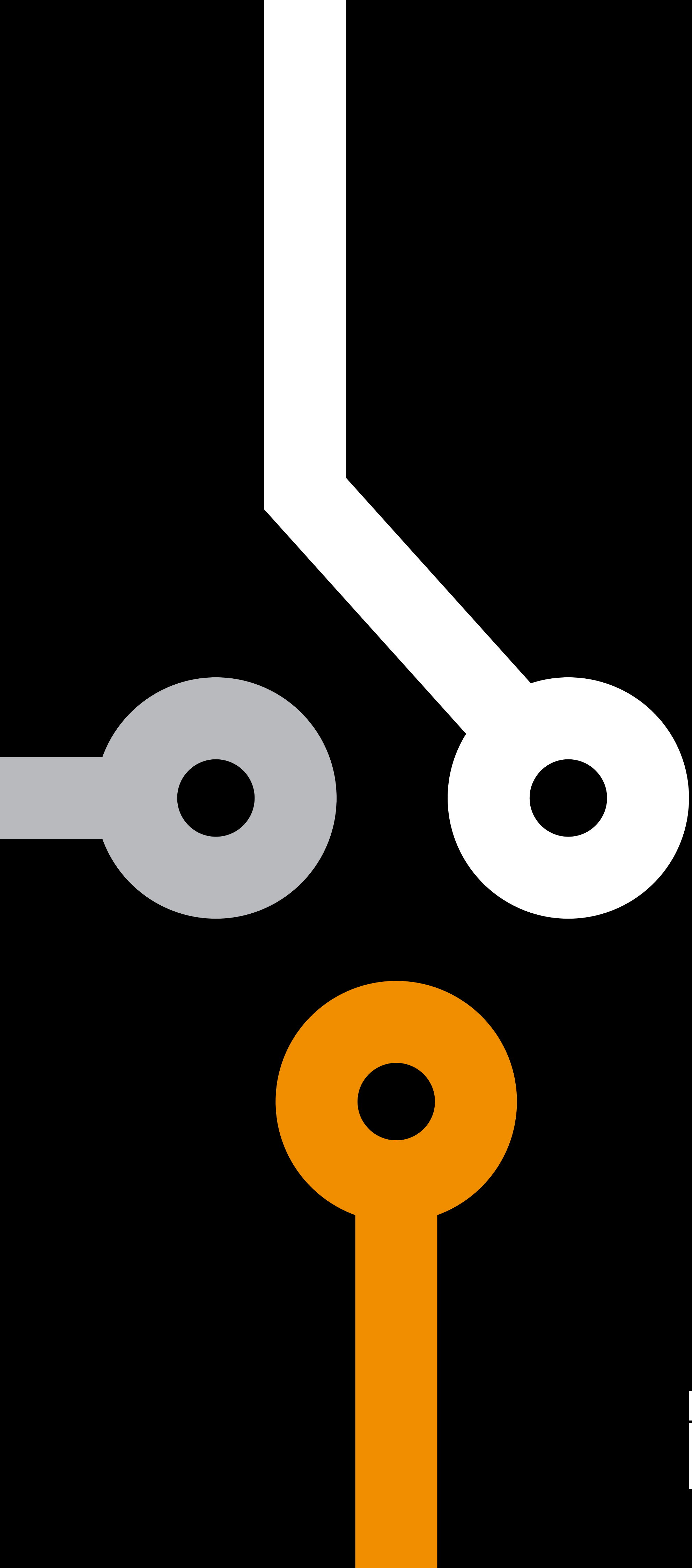


POLICY BRIEF:

AUSTRALIA'S OFFENSIVE CYBER CAPABILITY

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

INTERNATIONAL
CYBER POLICY
CENTRE

ABOUT THE AUTHORS

Fergus Hanson

Fergus is the Head of International Cyber Policy Centre. He is the author of Internet Wars and has published widely on a range of cyber and foreign policy topics. He was a Visiting Fellow at the Brookings Institution and a Professional Fulbright Scholar based at Georgetown University working on the uptake of new technologies by the US government. He has worked for the UN, as a Program Director at the Lowy Institute and served as a diplomat at the Australian Embassy in The Hague. He has been a Fellow at Cambridge University's Lauterpacht Research Centre for International Law and the Centre for Strategic and International Studies, Pacific Forum. He has published widely in Australian and international media.

Tom Uren

Tom is a Visiting Fellow in the International Cyber Policy Centre. He has worked in various analytical and operational areas in Defence and has diverse expertise across internet and cyber issues. Tom researches and writes on international and domestic cyber issues. He has a BSc(Hons) in Molecular Biology and previously worked for CSIRO in research on forest tree molecular genetics.

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's mission is to shape debate, policy and understanding on cyber issues, informed by original research and close consultation with government, business and civil society.

It seeks to improve debate, policy and understanding on cyber issues by:

1. conducting applied, original empirical research
2. linking government, business and civil society
3. leading debates and influencing policy in Australia and the Asia–Pacific.

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 sponsors but special mention in this case should go to the Australian Computer Society (ACS), which has supported this research.

A S P I
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

INTERNATIONAL
CYBER POLICY
CENTRE

acs

POLICY BRIEF:

AUSTRALIA'S OFFENSIVE CYBER CAPABILITY

FERGUS HANSON AND TOM UREN

CONTENTS

FOREWORD

The reality of the world we live in today is one in which cyber operations are now the norm. Battlefields no longer exist solely as physical theatres of operation, but now also as virtual ones. Soldiers today can be armed not just with weapons, but also with keyboards. That in the modern world we have woven digital technology so intricately into our businesses, our infrastructure and our lives makes it possible for a nation-state to launch a cyberattack against another and cause immense damage—without ever firing a shot.

ACS's aim in participating in this policy brief is to improve clarity of communication in this area. For Australia, both defensive and offensive cyber capabilities are now an essential component of our nation's military arsenal, and a necessary step to ensure that we keep up with global players. The cyber arms race moves fast, so continued investment in cyber capability is pivotal to keep ahead of and defend against the latest threats, while being able to deploy our own capabilities when and where we choose.

So, too, is ensuring that we have the skills and the talent to drive cyber capabilities in Australia. This means attracting and keeping the brightest young minds, the sharpest skilled local talent and the most experienced technology veterans to drive and grow a pipeline of cyber specialists, and in turn help protect and serve Australia's military and economic interests.

Yohan Ramasundara
President, Australian Computer Society

WHAT’S THE PROBLEM?

In April 2016, Prime Minister Turnbull confirmed that Australia has an offensive cyber capability. A series of official disclosures have provided further detail, including that Australia will use this capability against offshore cybercriminals. This was the first time any state has announced such a policy. However, this commendably transparent approach to telegraphing our capability and intentions hasn’t been without challenges. In some cases, these communications have created confusion and misperceptions. There’s a disconnect between popular perceptions, typified by phrases like ‘cyber Pearl Harbor’, and the reality of offensive cyber operations, and reporting has at times misrepresented how these tools will be used. Public disclosures and the release of the report of the Independent Intelligence Review have also raised questions about how Australia will build and maintain this capability.

WHAT’S THE SOLUTION?

To reduce the risk of misunderstanding and misperception and to ensure a more informed debate, this policy brief seeks to further clarify the nature of Australia’s offensive cyber capability. It recommends improving communications, using innovative staff recruitment and retention options, deepening industry engagement and reviewing classification levels in some areas. Looking forward, the government could consider increasing its investment in our offensive capability to create an asymmetric capability; that is, a capability that won’t easily be countered by many militaries in our region.

INTRODUCTION

Governments routinely engage in a wide spectrum of cyber operations, and researchers have identified more than 100 states with military and intelligence cyber units.[1] The cyber units range considerably in both their capability and their compliance with international law. Leaks have highlighted the US unit's advanced capability, and public documents reveal its size. US Cyber Command's action arm, the Cyber Mission Force, is building to 6,200 military and civilian personnel, or about 10% of the ADF, and for the 2018 financial year requested a US$647 million budget allocation.[2] China has been widely accused of stealing enormous quantities of intellectual property. North Korea has used cyber tools to steal money, including in a US$81 million heist on the Bangladesh central bank. Russia is accused of using a range of online methods to influence the 2016 US presidential election and has engaged in a wide spectrum of actions against its neighbours, such as turning off power stations in Ukraine and bringing down government websites in Georgia and Estonia. Israel is suspected of using a cyber operation in conjunction with its bombing raid on a Syrian nuclear reactor in 2007 by temporarily 'tricking' a part of Syria's air defence system to allow its fighter jets to enter Syria undetected.[3]

In Australia, the government has been remarkably transparent in declaring the existence of its offensive cyber capability and its applications: to respond to serious cyberattacks, to support military operations, and to counter offshore cybercriminals. It has also established robust structures to ensure its compliance with international law. Three additional disclosures about Australia's offensive cyber capability have followed the Prime Minister's initial April 2016 announcement. In November 2016, he announced that the capability was being used to target Islamic State,[4] and on 30 June 2017 Australia became the first country to openly admit that its cyber offensive capabilities would be directed at 'organised offshore cyber criminals'.[5] The same day, the then Minister Assisting the Prime Minister for Cyber Security, Dan Tehan, announced the formation of an Information Warfare Division within the ADF.

While these disclosures have raised awareness of Australia's offensive cyber capability, the limited accompanying detail has meant that the ensuing public debate has often been inaccurate or misleading. One major news site, for example, led a report with the title 'Australia launches new military information unit to target criminal hackers'.[6] Using the ADF to target criminals would have been a radical departure from established protocols.

This policy brief seeks to clarify some of the misunderstandings arising from sensationalist reporting.

The report has the following parts:

1. What's an offensive cyber operation?
2. Organisation, command and approvals
3. Operations against declared targets
4. Risks
5. Checks, balances and compliance with international law
6. Strengths and weaknesses
7. Future challenges and recommendations.

1. WHAT'S AN OFFENSIVE CYBER OPERATION?

For the purposes of this policy brief, we use a draft definition that's being developed as part of the Department of the Prime Minister and Cabinet's Cyber Lexicon project. It defines offensive cyber operations as 'activities in cyberspace that manipulate, deny, disrupt, degrade or destroy targeted computers, information systems, or networks'.[7] Given the range of countries with varying capabilities and using examples from open sources, offensive cyber operations could range from the subtle to the destructive: removing computer accounts or changing passwords; altering databases either subtly or destructively; defacing web pages; encrypting or deleting data; or even attacks that affect critical infrastructure, such as electricity networks.

Even though it may use the same tools and techniques, cyber espionage, by contrast, is explicitly designed to gather intelligence *without* having an effect—ideally without detection. The Global Commission on the Stability of Cyberspace has commissioned ASPI's International Cyber Policy Centre to do further work on defining offensive cyber capabilities.

2. ORGANISATION, COMMAND AND APPROVALS

Australia's offensive cyber capability resides within the Australian Signals Directorate (ASD).[8] It can be employed directly in military operations, in support of Australian law enforcement activities, or to deter and respond to serious cyber incidents against Australian networks. While physically housed within ASD, the military and law enforcement applications have different chains of command and approvals processes.

MILITARY

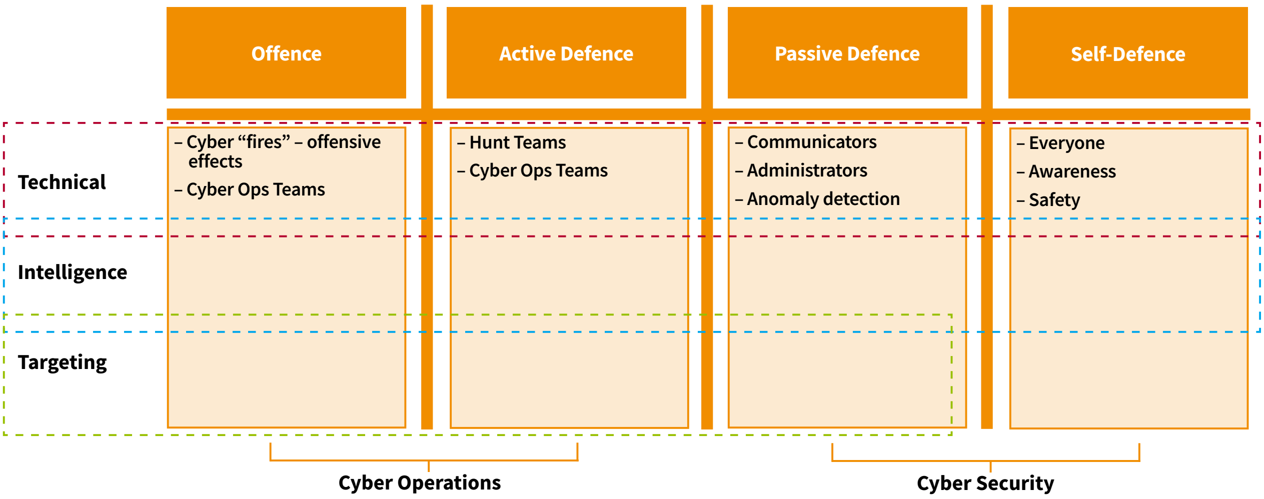
The Information Warfare Division within the Department of Defence was formed in July 2017 and is headed by the Deputy Chief Information Warfare, Major General Marcus Thompson.

Major General Thompson has presented the ADF approach to cyber capabilities as two distinct functions (Figure 1 on following page): cybersecurity (consisting of self-defence and passive defence[9]), and cyber operations (consisting of active defence and offence[10]).

The Australian Government's offensive cyber capability sits within ASD and works closely with each of the three services, which embed staff assigned to ASD from the ADF's Joint Cyber Unit. Offensive cyber in support of military operations is a civil–military partnership. The workforce to conduct offensive cyber operations resides within ASD and is largely civilian. Advice from Defence is that the laws of armed conflict are considered during the development and execution of operations, and that ASD personnel will act in accordance with legally approved instructions. There's no reason to doubt that, and the Inspector-General of Intelligence and Security has noted in the context of cyber operations in support of the ADF operations in Iraq and Syria that 'guidance in place at the time was appropriate and followed by staff, and no issues of legality or propriety were noted'.

The ability to conduct an operational planning process that takes into account the desired outcome, situational awareness and the possible range of effects is a military discipline that resides in the ADF.

FIGURE 1: FRAMEWORK FOR ADF CYBERSPACE OPERATIONS



This arrangement is expected to continue under proposals from the 2017 Intelligence Review to make ASD a statutory authority within the Defence portfolio.

As clarified in Australia’s International Cyber Engagement Strategy, ‘Offensive cyber operations in support of [ADF] operations are planned and executed by ASD and Joint Operations Command under direction of the Chief of Joint Operations.’[11] Targeting for offensive cyber operations occurs in the same manner as for kinetic ADF operations. Any offensive cyber operation in support of the ADF is planned and executed under the direction of the Chief of Joint Operations and, as with any other military capability, is governed by ADF rules of engagement.

The full integration of Australia’s military offensive cyber capability with ADF operations sets Australia’s capability apart from that of many other countries. Only a very limited number of states have this organisational arrangement, which provides a distinct battlefield edge that with modest additional investment would give Australia an asymmetric advantage in a range of contexts.

Australia, and two key partners, the UK and US, each have slightly different organisational structures for integrating their offensive cyber military capability with military operations. In contrast to Australia’s model, the UK’s National Offensive Cyber Programme is a partnership between the Ministry of Defence and the Government Communications Headquarters[12] (the latter organisation’s minister is the Secretary of State for Foreign and Commonwealth Affairs). In the US, the offensive cyber military capability is housed within Cyber Command, which will be raised to the status of a unified combatant command for cyberspace operations.[13]

LAW ENFORCEMENT

The announcement that Australia would be using its offensive cyber capability against offshore cybercriminals created considerable confusion. Public messaging was one contributing factor: the announcement about the ADF’s Information Warfare Division bled into the same-day announcement that the government would also be using its offensive cyber capability to deter offshore cybercriminals, making them appear one and the same thing.[14]

While some media outlets characterised the announcement as Australia potentially attacking the whole suite of ‘organised offshore criminals’, the announcement focused only on offshore actors who commit cybercrimes affecting Australia.

Decisions on which cybercriminal networks to target follow a similar process to those for military operations, including that particularly sensitive operations could require additional approvals, although the exact processes haven’t been disclosed. Again, these operations would have to comply with domestic law and be consistent with Australia’s obligations under international law.

3. OPERATIONS AGAINST DECLARED TARGETS

Australia has declared that it will use its offensive cyber capabilities to deter and respond to serious cyber incidents against Australian networks; to support military operations, including coalition operations against Daesh in Iraq and Syria; and to counter offshore cybercriminals. Given ASD’s role in intelligence gathering, operations can integrate intelligence with cyber operations—a mission critical element.

4. RISKS

Offensive cyber operations carry several risks that need to be carefully considered. For cyber operations in support of the ADF, as with conventional capabilities, the commander must weigh up the potential for achieving operational goals against the risk of collateral effects and damage.

When offensive cyber capabilities are used, there’s a high chance that future effectiveness might be compromised. Unlike defending against kinetic weapons, an information system might be protected from cyberattack through relatively simple measures, such as upgrades, patches or configuration changes.

Another risk is that, despite extensive efforts to disguise the origin of the attack, the Australian Government could lose plausible deniability or be identified (including contextually) as the source and face embarrassment or retaliation.

5. CHECKS, BALANCES AND COMPLIANCE WITH INTERNATIONAL LAW

When the first public disclosure of Australia’s offensive cyber capability was made, the Prime Minister emphasised Australia’s compliance with international law: ‘The use of such a capability is subject to stringent legal oversight and is consistent with our support for the international rules-based order and our obligations under international law.’[15]

Interviews for this policy brief suggest that the users of the capability take compliance with domestic and international law extremely seriously. The core principles are as follows:

1. Necessity: ensuring the operation is necessary to accomplish a legitimate military / law enforcement purpose.
2. Specificity: ensuring the operation is not indiscriminate in who and what it targets.

3. Proportionality: ensuring the operation is proportionate to the advantage gained.
4. Harm: considering whether an act causes greater harm than is required to achieve the legitimate military objective.

These capabilities are subject to ASD's existing legislative and oversight framework, including independent oversight by the Inspector-General of Intelligence and Security. However, there seems to be room for updating these provisions to account for technological developments. Section 7(e) of the *Intelligence Services Act 2001, for example, authorises ASD 'to provide assistance to Commonwealth and State authorities in relation to … (ii) other specialised technologies'*—a foundation that could be strengthened for 21st-century technological applications.

When seeking approval for operations from the Minister for Defence, ASD seeks legal, foreign policy and national security advice from sources external to Defence.

Every offensive cyber operation is planned and conducted in accordance with domestic law and is consistent with Australia's obligations under international law.

6. STRENGTHS AND WEAKNESSES

Offensive cyber capabilities have both strengths and weaknesses.

STRENGTHS

- For military tasks, they can be integrated with ADF operations, adding a new capability and creating a force multiplier.
- They can engage targets that can't be reached with conventional capabilities without causing unacceptable collateral damage or overt acknowledgement.
- They provide global reach.
- They provide an asymmetric advantage against an adversary for a relatively modest cost.
- They can be overt or clandestine, depending on the intended effect.

WEAKNESSES

- Capabilities need to be highly tailored to be effective (such as the Stuxnet worm that targeted Iran's nuclear centrifuges), meaning that they can be expensive to develop and lack flexibility.
- When used in isolation, they are unlikely to be decisive.
- Major, blunt attacks (such as Wannacry or NotPetya) are relatively cheap and easy, but are unusable by responsible state actors such as Australia. Achieving the appropriate specificity and proportionality requires investment of time and effort.
- The capability requires constant, costly investment as cybersecurity evolves.
- Government must compete for top-tier talent with private industry.
- For operations short of 'cyber attacks',[16] the effects can be relatively short-lasting and limited.

- Capability can't be showcased as a deterrent in the same way that conventional capability can, because revealing specific capability renders it redundant as defences are repaired.
- Target development can require intensive intelligence support and can take a very long time.

7. FUTURE CHALLENGES AND RECOMMENDATIONS

Offensive cyber operations are relatively new and developing in a fast-moving environment. Below are issues and recommendations stemming from research for this report.

RECOMMENDATION 1: CAREFULLY STRUCTURE COMMUNICATIONS TO REASSURE NATION-STATES AND ENFORCE NORMS

As Australia's offensive cyber capability has only recently been publicly acknowledged and is subject to sensationalist reporting, careful communication is required. When he first acknowledged the capability, the Prime Minister said doing so 'adds to our credibility as we promote norms of good behaviour on the international stage'.[17] Poor communications, however, can have the opposite effect. The limited detail and mixed reporting of the announcement that Australia would use offensive cyber capability against offshore cybercriminals inadvertently sent the message that it was acceptable for states to launch cyberattacks against people overseas whom they considered to be criminals. This might encourage some states to use crime as a pretext to launch cyber operations against individuals in Australia.

To address this, the Australian Government should be careful when publicly discussing the offensive capability, particularly to distinguish the military and law enforcement roles. One option to do this would be to have the Attorney-General, the Minister for Justice or the new Home Affairs Minister discuss operations related to law enforcement aspects of the capability and to have the Minister for Defence discuss those related to military capabilities.

RECOMMENDATION 2: USE INNOVATIVE STAFF RECRUITMENT AND RETENTION OPTIONS

Recruiting and retaining Australia's top technical talent is a major hurdle. In the medium term, ASD will have to continue to invest heavily in training, raise salaries (ASD becoming a statutory authority will help it address this) and develop an alumni network and culture that allow former staff to return in new roles after a stint in private industry. A pool of alumni working as cleared reservists could also be used as an additional workforce without the significant investment required in conducting entirely new clearances.

RECOMMENDATION 3: DEEPEN INDUSTRY ENGAGEMENT

ASD capability being deployed against cybercriminals is likely to generate increased interest from corporate Australia. There's a policy question about whether or not Australia's offensive cyber capability should be used in support of Australian corporate interests. Given the finite resources and the tricky situations that could arise, government should consider useful ways industry could engage, clarify the limits of industry engagement and assess how to handle industry requests to use the offensive cyber capability against actors targeting its operations.

RECOMMENDATION 4: CLASSIFY INFORMATION AT LOWER LEVELS

It has long been argued that overclassification of material, such as threat intelligence, by governments prevents easy information exchange with the outside world, including key partners such as industry. The government has recognised this and is positioning 'Australian Cyber Security Centre (ACSC) 2.0' to facilitate a more cooperative and informed relationship with the private sector. Similarly, the government should continue to scope the potential benefits from lowering the classification of information associated with offensive cyber operations. In particular, there are benefits in operating at the SECRET level for workforce generation and training, and providing a 'halfway house' to usefully employ incoming staff as they wait during vetting procedures. More broadly, excessive classification slows potentially valuable two-way information exchange with the information security community.

RECOMMENDATION 5: INVEST TO CREATE AN ASYMMETRIC CAPABILITY

The *2016 Defence White Paper noted that 'enhancements in intelligence, space and cyber security will require around 900 ADF positions'.*[18] Those positions were part of the $400 million[19] in spending announced in the White Paper and will be spread across the ADF. While this is significant, given the limits of what can be achieved with current spending on conventional kit, the Australian Government should consider conducting a cost–benefit analysis on the relative value of substantial further spending on cyber to provide it with an asymmetric capability against future adversaries. This would need to include a considerable investment in training.

RECOMMENDATION 6: CONSIDER UPDATING THE POLICY AND LEGISLATIVE FRAMEWORK

There appears to be sufficient legislation, policy and oversight to ensure that ASD and the ADF work together in a lawful, collaborative and cooperative manner to support military operations. The 2017 Independent Intelligence Review noted that ASD's support to military operations is indispensable, and will remain so.

While those oversight arrangements may be sufficient for now, the ADF will inevitably need to incorporate offensive cyber on the battlefield as a way to create local effects, including force protection measures and to deliver effects currently generated by electronic warfare (such as jamming communications technology). It should not always be necessary to reach back to the national authorities for clear-cut and time critical battlefield decisions. There appears to be scope to update the existing policy and legislative framework that governs the employment of offensive cyber in deployed operations to support those kinds of activities.

ACRONYMS AND ABBREVIATIONS

ADF	Australian Defence Force
ASD	Australian Signals Directorate

NOTES

[1] Noah Shachtman, Peter W Singer, *The wrong war: the insistence on applying Cold War metaphors to cybersecurity is misplaced and counterproductive*, Brookings Institution, Washington DC, 15 August 2011, online.

[2] Michael S Rogers, *Statement of Admiral Michael S Rogers, Commander, United States Cyber Command, before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities,* 23 May 2017, p. 1, online*;* Laura Criste, 'Where's the cyber money for fiscal 2018?', *Bloomberg Government,* 19 July 2017, online*.*

[3] Thomas Rid, *Cyber war will not take place,* Oxford University Press, 2013, p. 42.

[4] Malcolm Turnbull, 'Address to parliament: national security update on counter terrorism', 23 November 2016, transcript, online.

[5] Malcolm Turnbull, 'Offensive cyber capability to fight cyber criminals', media release, 30 June 2017, online.

[6] 'Cyber warfare: Australia launches new military information unit to target criminal hackers', *The Australian,* 30 June 2017, online*.*

[7] This is consistent with public statement by the Minister Assisting the Prime Minister for Cyber Security, who has described using 'offensive cyber capabilities to disrupt, degrade, deny and deter' adversaries.

[8] Department of Foreign Affairs and Trade (DFAT), *Australia's International Cyber Engagement Strategy*, Australian Government, 2017, p. 55, online*.*

[9] 'Self defence' includes raising basic cyber hygiene and awareness across the defence forces, while 'passive defence' includes standard network administration procedures, such as complying with security standards.

[10] 'Active defence' includes actively working to identify intrusions and threats, while 'offence' includes Australia's national offensive cyber capability.

[11] DFAT, *Australia's International Cyber Engagement Strategy*, p. 55.

[12] UK Government, *National Cyber Security Strategy, 2016–2021,* London, 2016, p. 51, online*.*

[13] 'Statement by President Donald L Trump on the elevation of Cyber Command', The White House, Washington DC, 18 August 2017, online.

[14] 'Tehan announces "information warfare" unit', *ABC News,* 30 June 2017, online*.*

[15] Department of the Prime Minister and Cabinet (PM&C), 'Prime Minister launches Cyber Security Strategy', media release, 22 April 2016, online.

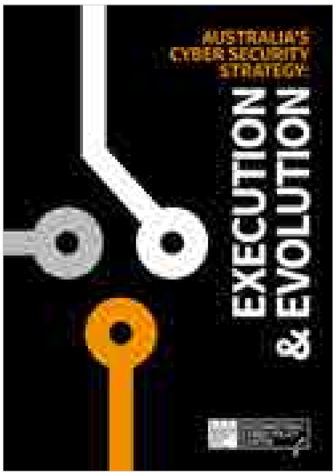
[16] The Australian Government defines cyber attack as 'a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or prosperity'; Australian Cyber Security Centre, *2017 threat report*, p. 52, online.

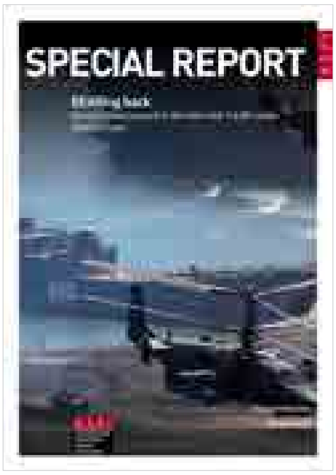
[17] PM&C, 'Prime Minister launches Cyber Security Strategy'.

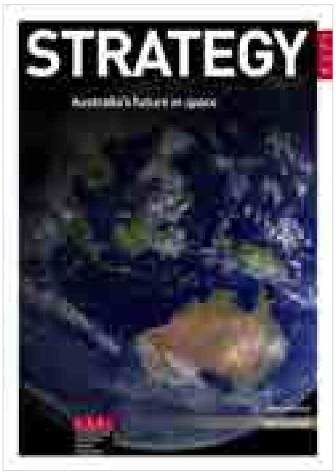
[18] Department of Defence, *2016 Defence White Paper*, Australian Government, 2016, p. 147, online.

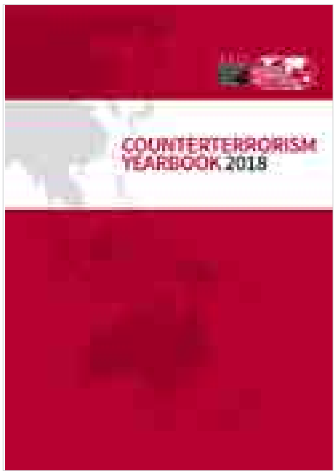
[19] Tobias Feakin, 'Matching rhetoric with action: cyber and the 2016 Defence White Paper', *The Strategist,* 25 February 2016, online.

Some previous ASPI publications









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
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC
www.aspi.org.au/icpc/home

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

INTERNATIONAL
CYBER POLICY
CENTRE