Cyber Operations and the 2009 Defence White Paper: Positioning the Australian Defence Organisation to Be Effective, Transparent and Lawful

Chris Hanna

The Defence White Paper 2009 included important initiatives in Defence's approach to cyberspace. This article scrutinises Australian cyberspace operations as laid out in the White Paper, with a particular focus on policy towards cyber operations and the applicable legal regimes. It argues that Australia requires a cyber warfare capability, not just a cyber security capability. Furthermore, it suggests that Australia must genuinely enter the public debate on cyber warfare. Australia must review its domestic laws to ensure that any prospective cyber operations, particularly those going beyond passive defence, fit within the scope of the relevant agency's functions and that its personnel are provided with appropriate legal protection. The article proposes that Australia should allocate its cyber warfare capability to a distinctly Australian Defence Force element and recommends that Australia develop a philosophy on the application of the international laws of armed conflict to cyber warfare.

The Australian Government's Defence White Paper 2009, *Defending Australia in the Asia Pacific Century: Force 2030* ('the White Paper')[1] announced an ambitious program of developments for the Australian Defence Organisation (ADO)[2] for the next two decades. Much of the subsequent attention has focused on the large scale capital equipment acquisitions[3], as well as the future place of China in Australia's long-range strategic thinking.[4]

But the White Paper also included important initiatives in Defence's approach to cyberspace, the "communication network, conceived of as a separate world, access to which is gained through the use of computers".[5]

[1] Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, Defence White Paper 2009 (Canberra: Defence Publishing Service, 2009).
[2] In this context, the Australian Defence Organisation (ADO) is the collective label for aggregation of both the Australian Defence Force (ADF) and the civilian elements of the Department of Defence.
[3] For example, for Navy, Department of Defence, 'White Paper' p. 70, para. 9.3 (regarding submarines) and p. 71 paras. 9.11 and 9.13 (regarding Air Warfare Destroyers and Future Frigates). See also Cameron Stewart, 'Military Ambitions', *The Australian*, 2 May 2009.
[4] Department of Defence, 'White Paper', p. 34. See also, Stewart, 'Military Ambitions' and Michael Sainsbury and Cameron Stewart, 'China, a "Peaceful Force" in Beijing's Response to Defence Paper', *The Australian*, 6 May 2009.
[5] A. Delbridge and J. R. L. Bernard, *The Macquarie Concise Dictionary*, Third Edition (McMahons Point, New South Wales: The Macquarie Library, 1998), p. 277.

The national security interests in cyberspace are many and varied, ranging from basic defence of systems, through to the concept of deliberately targeting an adversary's cyber assets or non-cyber assets through cyber means.

This article scrutinises Australian cyberspace operations as laid out in the White Paper, with a particular focus on policy towards cyber operations and the applicable legal regimes, and makes a number of recommendations for the implementation of the White Paper proposals. It is, however, acknowledged at the outset that the White Paper is not, nor does it claim to be, an exhaustive or detailed treatise on all of Australia's national cyber capabilities. Nevertheless, the White Paper is an important statement of intent with respect to the ADO's role and capability in cyber operations.

Cybersecurity or Cyberwarfare?

The White Paper included significant policy statements relating to the national security aspects of cyberspace, declaring Australia would "hedge against future risk through modest capability developments"[6] to contend with the danger of "cyberattack on our defence, security, government and civilian information infrastructure".[7] In its discussion, the White Paper uses the terms "cyber security", "cyber attack" and "cyber warfare", but does not define or otherwise expressly distinguish any of these terms.[8] Moreover, they are not part of the Australian Defence Force's (ADF) doctrinal publications.

Taking into account the context in which the terms are used in the White Paper, the possibilities offered by United States military doctrine[9] and even relevant definitions in the Macquarie Dictionary,[10] it can be inferred that 'cyber security' involves protection of the nation's public and private computer systems and networks from unauthorised access and exploitation, or more broadly, protection from 'cyberattack'. 'Cyber security' is then purely defensive and does not involve a counter-attack (or 'active defence') capability.[11]

[6] Department of Defence, 'White Paper', p. 84, para. 9.97.
[7] Ibid., p. 85, para. 9.97.
[8] The White Paper also used is the term 'cyberattack' without any specific definition. US military doctrine defines 'cyber-attack' as "Actions taken through the use of computer networks to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves." US Department of Defense, Joint Publication 1-02, 'Dictionary of Military and Associated Terms', 12 April 2001 (as amended through 30 May 2008), <http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf> [Accessed 26 July 2009], p. 112.
[9] For example; 'computer network attack', 'computer network defense', 'computer network exploitation', 'computer network operations' and 'computer security'. Ibid.
[10] *Macquarie Concise Dictionary*, using the definitions of 'cyber', 'security' and 'warfare'.
[11] In this paper, 'counter-attack' or 'active' defence will be taken to mean either an automatic or manual response to a cyber-attack through some form of offensive measure. For instance, a

In contrast, 'cyber warfare' involves both offensive and defensive measures taken in relation to any computer systems and/or networks as part of military operations during armed conflict or pursuant to national self defence during peacetime. Defensive measures, as a component of 'cyber warfare', will be presumed to include counter-attack (or 'active' defence).[12] 'Cyber warfare' is presumed to contain an inherent sub-element of cyber security in the context of military operations.[13]

These definitions may or may not match the reality within the ADO. Any such discrepancy, however, usefully highlights the problem that without properly framed terminology in cyber security and cyber warfare, discussion of related policy issues and legal frameworks becomes very difficult.

Despite statements in the White Paper indicating that the Australian Government proposes "to invest in a major enhancement of Defence's cyber warfare capability"[14] and suggesting that through "[a] comprehensive range of expanded and new capabilities will maximise Australia's strategic capacity and reach in this field",[15] this cyber warfare function is not described in any detail, and the White Paper contains no specific mention of offensive cyber capabilities.

The White Paper excuses itself from providing a great amount of detail on the basis that "[m]any of these capabilities remain highly classified",[16] before providing an 'outline' of the capabilities, which are described as,

> a much enhanced situational awareness and incident response capability, and the establishment of a Cyber Security Operations Centre to coordinate responses to incidents in cyberspace.[17]

This, however, sounds remarkably like cyber security rather than necessarily cyber warfare. Subsequent comments from ADO leadership indicate a reluctance to engage in discussion, particularly on the subject of offensive

---

measure which is designed to cause harm to the cyber system operated by the original perpetrator.

[12] Offensive measures will be taken to include such activities as "hacking, disabling information infrastructures, disrupting chains of command and decision-making processes, corrupting databases and conducting sophisticated IW". Ball in Gary Waters, Desmond Ball and Ian Dudgeon, 'Australia and Cyber-Warfare', Australian National University, E-Press, Canberra Papers on Strategy and Defence, No.168, 2008, <http://epress.anu.edu.au/cyber_warfare_citation.html> [Accessed 29 May 2009], p. 131.

[13] This paper will endeavour to limit discussion of cyber warfare away from broader notions of 'Information Warfare' and 'electronic warfare', although cyber warfare may be relevant to either.

[14] Department of Defence, 'White Paper', p. 83, para. 9.87.

[15] Ibid.

[16] Ibid.

[17] Ibid.

capabilities.[18] Consequently, it is difficult to scope the function of either the 'Cyber Security Operations Centre' (CSOC) or the wider ADF that flows from the White Paper's discussion of cyber warfare, and it is unclear whether an offensive or even counter-attacking/active defence capability is truly envisaged. This lack of clarity has very significant implications for the appropriateness of organisational and legal frameworks in place for the new CSOC and related activities.

Australia's National Security Architecture for Cyberspace

National leadership for cyber security of the national information infrastructure (NII)[19] lies with the Attorney-General (AG) and the Attorney-General's Department (AGD). It exercises its role through specialist branches, teams and programs, as well as by chairing the E-Security Policy and Coordination (ESPaC) committee.[20] The ESPaC committee comprises representation from a broad range of government department and agencies including law enforcement, defence and intelligence elements.[21]

Other elements with defined cyber security roles for the NII include: the Australian Computer Emergency Response Team (AusCERT);[22] the Australian Federal Police (AFP), including the 'Australian High Tech Crime Centre'; the State and Territory Police forces; the Australian Crime

[18] Following the release of the White Paper, when questioned on the potential offensive role of the Cyber Security Operations Centre (CSOC), the Chief of Defence Force (CDF) referred to the classified nature of the issue, and the Secretary of the Department reiterated the contents of the White Paper. See, Chief of Defence Force, Air Chief Marshal Angus Houston, Secretary of Defence, Nick Warner, 'Round Table Discussion for the Federal Government's Defence White Paper', 7 May 2009, MSPA 90507/09, <http://www.defence.gov.au/media/SpeechTpl.cfm?CurrentId=9069> [Accessed 26 July 2009].

[19] Dudgeon in Waters, Ball and Dudgeon, *Australia and Cyber-Warfare*, p. 61, quotes ADF doctrine, stating that "The NII is defined in Australian Defence Doctrine Publication (ADDP) 3-13—*Information Operations* (2006), as, compris[ing] the nation wide telecommunications networks, computers, databases and electronic systems; it includes the Internet, the public switched networks, public and private networks, cable and wireless, and satellite telecommunications. The NII includes the information resident in networks and systems, the applications and software that allows users to manipulate, organise and digest the information; the value added services; network standards and protocols; encryption processes; and importantly the people who create information, develop applications and services, conduct facilities, and train others to utilise its potential."

[20] For more on the Attorney General's role see Attorney General's Department (AGD), 'Security and Critical Infrastructure Division', <http://www.ag.gov.au/www/agd/agd.nsf/Page/Organisational_StructureNational_Security_and_Criminal_JusticeSecurity_and_Critical_Infrastructure> [Accessed 26 July 2009]. See also Attorney-General's Department, 'E-Security Review 2008 Discussion Paper for Public Consultation', <http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(3A6790B96C927794 AF1031D9395C5C20)~DRAFT+E-Security+Review+2008++Public+industry+Discussion+ Paper.DOC/$file/DRAFT+E-Security+Review+2008+-+Public+industry+Discussion +Paper.DOC> [Accessed 26 July 2009], p. 2.

[21] Ibid., p. 2.

[22] The Australian Computer Emergency Response Team (AusCERT) is a private, not-for-profit organisation which is part of the University of Queensland. Waters, Ball and Dudgeon, *Australia and Cyber-Warfare*, p. 103.

Commission; ASIO; the Australian Government Information Management Organisation (AGIMO); the Department of Broadband, Communication and the Digital Economy (DBCDE) and the Inspector General Intelligence and Security (IGIS).

There has been a general allocation of a cyber warfare role to the Department of Defence. Within the ADO, the Defence Signals Directorate (DSD) has a central cyber security role. However, the Defence Science and Technology Organisation (DSTO) and the Royal Australian Air Force (RAAF) No. 462 Squadron also have important functions. The White Paper indicates that DSTO would "increase its investigation and application of key enabling technologies which will provide significant returns for development of the future force, such as ... cyber warfare (including computer security)".[23] DSTO's is also tasked with developing Australia's cyber interoperability with its friends and allies.[24] The task of No. 462 Squadron is "to exploit, and protect against exploitation of the information domain and to support operational commanders in providing a secure information environment to support air operations".[25] This is a defensive cyber role, whether characterised as a cyber security role or, in keeping with its military status, as part of a cyber warfare capability. Other elements of the ADO can also have cyber security or cyber warfare functions as far as that function overlaps with 'network centric warfare' (NCW) or electronic warfare.[26]

DSD is the "national authority on communications and computer security (infosec)",[27] and has responsibility "for protecting Australian official communications and information systems".[28] DSD's role, however, goes further, providing assistance to industry for the development of new

[23] Department of Defence, 'White Paper', p. 134, para. 17.18.
[24] Department of Defence, 'White Paper', p. 136, para. 17.25. The Minister for Defence, the Hon Joel Fitzgibbon MP, and the Minister for Defence Science and Personnel, the Hon Warren Snowdon MP, 'A Smarter Defence For A More Complex World', 2 May 2009, <http://www.defence.gov.au/whitepaper/mr/07_A_SmarterDefence.pdf> [Accessed 26 July 2009], which states "Over the next four years the Government will fund a $53 million program to significantly enhance focused external engagement initiatives between DSTO and its national and international partners. This will generate more significant benefits for the Australian Defence Force and its allies."
[25] Royal Australian Air Force, 'RAAF Base Edinburgh', <http://www.airforce.gov.au/bases/edinburgh.aspx> [Accessed 26 July 2009].
[26] Network centric warfare (NCW) is subject to multiple definitions. The following definition is provided: "NCW is an approach to warfighting where the network supplies the right information at the right time in the right form to the right person. To these 'four rights' can be added 'and is put to the right use' (Fewell & Hazen 2003)." M. P. Fewell and M. G. Hazen, 'Network-Centric Warfare—Its Nature and Modelling', *DSTO Report RR-0262*, September 2003 cited in Tim McKenna, Terry Moon, Richard Davis and Leonie Warne, 'Science and Technology for Australian Network-Centric Warfare: Function Form and Fit', *Australian Defence Force Journal*, no. 170 (2006), p. 63.
[27] Defence Signals Directorate (DSD), 'Reveal their Secrets … Protect our own', <http://www.dsd.gov.au/> [Accessed 26 July 2009].
[28] Waters, Ball and Dudgeon, *Australia and Cyber-Warfare*, p. 123. Also DSD, 'Infosec', <http://www.dsd.gov.au/infosec/index.html> [Accessed 26 July 2009].

cryptographic products, network security, the development of guidelines and policies on information security and evaluating 'Infosec' products.[29] The role also includes,

> information and incident collection, analysis and warning services, setting awareness and certification standards, and defensive measures, including protective security measures, response arrangements, and contingency planning.[30]

DSD's cyber security role with respect to "information and incident collection" is reflected in its management of the Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS).[31]

Despite the presence in its workforce of ADF personnel,[32] DSD is a 'civilian' element of the Department of Defence, headed by a civilian and answering to a civilian Deputy Secretary, with the Secretary of the Department being primarily responsible to the Minister for Defence for DSD as a non-ADF element of the department. This is not to dismiss the role of the Chief of Defence Force (CDF), or to say that DSD works at cross-purposes to CDF. DSD, like the other intelligence agencies, supports CDF in relation to CDF's responsibilities and generally acknowledges and responds to the authority of the CDF. Nevertheless, DSD is not 'commanded' by the CDF. This aspect is not inconsequential and is discussed at relevant points in this article.

Within DSD, cyber-related tasks are performed by its Information Security Group and, prospectively at least, by a CSOC, which the White Paper announced would be created within DSD.[33] The CSOC, as disclosed in the White Paper, is not modelled upon the specialist 'cyber warfare centre' proposed by Ball, which involved lodging an operational element within the ADF itself.[34] Moreover, the CSOC as with the remainder of DSD, is not commanded by the CDF. The CSOC's staff will, however, include ADF members, as well as DSTO personnel and representatives from other government agencies.[35]

---

[29] Waters, Ball and Dudgeon, *Australia and Cyber-Warfare*, p. 123. See also the Crisis and Risk Network, 'Publications', for CRN Team review 'Country Survey Australia', <http://www.crn.ethz.ch/publications/crn_team/ciip_by_chapter/partI/australia.pdf> [Accessed 25 July 2009], pp. 56-7.

[30] Ibid., pp. 56-7.

[31] See 'Incident Ready Reckoner', at DSD, library webpage, <http://www.dsd.gov.au/_lib/pdf_doc/incident_ready_reckoner.pdf> [Accessed 26 July 2009].

[32] ADF personnel will be part of the CSOC. See Department of Defence, 'White Paper', p. 83, para. 9.88.

[33] Ibid., p. 83, para. 9.88.

[34] Thereby overcoming current difficulties with the "full exploitation of cyber-space for either military operations or IW [Information Warfare] more generally as well as the planning and execution of both offensive and defensive IO [Information Operations]".

[35] Including from AGD, AFP and the intelligence agencies. Department of Defence, 'White Paper', p. 83, para. 9.88.

The CSOC will "coordinate responses to incidents in cyberspace"[36] and includes a "continuously staffed watch office and analysis team to respond to cyberthreats in a timely fashion".[37] The CSOC will also be "available to provide cyber warfare support to ADF operations", while being "purpose-designed to serve broader national security goals".[38] These broader aspects, falling within the cyber security rubric, include "assisting responses to cyber incidents across government and critical private sector systems and infrastructure".[39] The White Paper states that "whole of government coordination will be achieved through the appropriate representation within the Centre from relevant Government agencies".[40]

Overall, the CSOC proposed by the White Paper appears to be, as its name suggests, primarily a cyber security element, with some undefined level of residual or complementary cyber warfare function in support of ADF activities. More generally, it is unclear whether the functions of DSD (CSOC included) will radically change from its pre-existing allocated and authorised cyber security role. The operational security coordination role, however, does appear to be a new function not previously allocated across the whole-of-government,[41] although it would be wrong to see this as necessarily revolutionary given existing interagency arrangements for handling cyber security incidents.[42]

An issue for the future is the question of 'leadership' of the Australian Government's overall activities in cyber space. To date, the Attorney General (AG) and AGD have provided leadership from a cyber security perspective. If and when a cyber warfare capability develops within the ADO then it may or may not be appropriate for the AG and AGD to assume or extend leadership to this new area. One consideration may be the role of the National Security Adviser (NSA) and the National Security Chief Information Officer (NS CIO) operating from the Department of Prime Minister and Cabinet. Philosophically, these positions may be more concerned with coordination rather than day-to-day operations. The NSA and NS CIO may, however, be positioned to take on an overall leadership

[36] Ibid., p. 83, para. 9.87.
[37] Ibid., p. 83, para. 9.88.
[38] Ibid., p. 83, para. 9.89.
[39] Ibid., p. 83, para. 9.89.
[40] Including from AGD, AFP and the intelligence agencies. Ibid., p. 83, para. 9.89.
[41] That is, AUScert.au have the at-the-scene responsibility for incident response and ESPaC has responsibility for policy coordination, the overall coordination of a response major incident had been left unallocated.
[42] DSD, ASIO and the AFP already operate with each under "formal, classified, Joint Operating Arrangements supporting threat and vulnerability assessment and the analysis of, and the response to, critical incidents affecting the integrity of Australia's information infrastructure." Australian Security Intelligence Organisation*, ASIO Report to Parliament 2005-06*, Commonwealth of Australia, September 2006, <http://www.asio.gov.au/publications/Content/AnnualReport05_06/pdf/ASIO%20annual%20Report%20to%20Parliament%2005-06.pdf> [Accessed 26 July 2009], p. 28.

role, but leave the frontline leadership and management of the cyber security and cyber warfare capabilities split between AG/AGD and the ADO respectively.

Legal Framework

The applicable legal regime spans both domestic and international law. The law actually applicable to and during an event will depend on a range of factors. This article confines itself to raising the principal issues of domestic Commonwealth law applicable to cyber security and the application of the international laws of armed conflict to cyber warfare.

DOMESTIC LAW

Of primary importance is DSD's enabling legislation, the *Intelligence Services Act 2001* (Cth) (ISA), which details its lawful functions. In accordance with section 7 of the ISA, DSD is to provide:

> (c) … material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; and
>
> (d) … assistance to the Defence Force in support of military operations and to cooperate with the Defence Force on intelligence matters; and
>
> (e) … assistance to Commonwealth and State authorities in relation to: (i) cryptography, and communication and computer technologies; …[43]

Under the ISA, DSD is specifically prohibited from undertaking,

> any activity unless the activity is (a) necessary for the proper performance of its functions; or (b) authorised or required by or under another Act.[44]

It is against this prohibition that DSD's prospective role as the home of the CSOC, as well as its performance of other cyber functions outlined in the White Paper, must be measured. A reasonable contention is that offensive cyber warfare does not necessarily, or at least easily, fall within DSD's statutorily authorised functions, and this may also be the case for 'active' or counterattacking defensive measures.

For offensive cyber warfare to sit within DSD's prescribed functions, a broad interpretation of the existing provisions would be required. For instance, for offensive cyber warfare to sit within sub-section 4(c), the reference to "matters relating to the security and integrity of information" would need to be

[43] *Intelligence Services Act 2001* (Cth) (ISA) section 7. None of these functions are limited by DSD general prohibition from performing its functions "only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia" (ISA section 11).

[44] ISA section 12. In addition, DSD's functions are expressly stated to not include "carrying out police functions; or … any other responsibility for the enforcement of the law". ISA section 11(2)—some relevant 'incidental' exceptions are provided.

interpreted to go beyond assurance or defensive measures in relation to 'friendly' systems. Similarly, or at least alternatively, broad interpretations would be required in relation to either sub-section 7(d), with respect to "assistance to the Defence Force in support of military operations"[45] and/or subsection 7(e), with respect to "assistance to Commonwealth or State authorities in relation to … computer technologies", would be required.[46] With the former, references to the 'Defence Force' and 'military operations' as the object and purpose of the support, of themselves immediately constrain the circumstances in which the function can be exercised. With the latter, the term 'computer technologies' could encapsulate any activity connected with computers, or, it could be as constrained as providing advice on future cyber technology purchases.

While in each case a broad interpretation of the provisions is possible, this is not an area of activity and law where relying on an arguable case is sufficient basis for operations, particularly given the potential for offensive cyber operations to directly or indirectly cause property damage or even casualties. Noting that that under the ISA, the immunities, limited as they are for actions taken by DSD personnel depend upon a correlation between the action and DSD's prescribed functions,[47] a greater level of assurance of lawfulness is required. Such assurance is required, first, from the perspective of the individual who wishes to avoid criminal liability and, second, from the perspective of the ADO. That is, the ADO will not only want to protect its reputation for lawful conduct, but also ensure that operations are not unnecessarily impeded by refusals by its personnel to perform tasks because of uncertainty whether their actions are covered by the ISA-based immunity. In this latter context, unequivocal lawfulness may be viewed as a basic enabler of operations in cyberspace.

The second aspect of domestic law is the criminal law, which is of relevance both from the perspective of addressing the conduct of persons from whom the NII requires protection, but also as a potential fetter upon DSD and other ADO elements in the performance of their assigned cyber roles, save perhaps in a genuine armed conflict. Most relevant in this context is *The Criminal Code Act 1995* (Cth),[48] which contains a range of 'computer offences' that are "directed at conduct which impairs the security, integrity and reliability of computer data and electronic communications".[49] It also contains telecommunications offences which are potentially applicable to

[45] ISA section 7(d).
[46] ISA section 7(e)(i).
[47] ISA section 14.
[48] As amended by the *Cybercrime Act 2001* (Cth).
[49] Cybercrime Bill 2001, Revised Explanatory Memorandum, Item 4. See Part 10.7 Computer Offences—for example, "unauthorised modification of data to cause impairment using a 'Commonwealth computer' or using a 'carriage service' to access 'restricted data'" (section 478.1).

operations involving the linkages between computers.[50] The principal difficulty with respect to the criminal offences is that there are either no immunities, as in the case of 462 Squadron, or the immunities that are available, in the case of DSD, are heavily caveated, if not circumstance dependant.[51] Consequently, should the cyber activities of either element involve offensive measures, counter-attacking or 'active' defensive measures, or even just intrusive (such as during an investigation), the risk of liability for criminal offences cannot be discounted.[52]

Finally, while under the ISA, the IGIS supervises DSD,[53] the IGIS has no specific mandate to supervise DSTO or RAAF No. 462 Squadron and could only exercise indirect supervision, via DSD, in relation to any foreign signals intelligence collected by the unit (which may, of course, be none). This very limited level of supervision arises from CDF directive, by which DSD now has oversight of the those units of the ADF involved in the collection and dissemination of foreign signals intelligence.[54] This means that IGIS can now indirectly supervise these units through its oversight of DSD's role in monitoring these units.[55]

INTERNATIONAL LAW

There is presently no specific international convention encapsulating Australia's specific international cyber warfare rights and obligations during armed conflict. In the context of armed conflict, however, a prevalent opinion is that the correct international legal paradigm for regulating cyber warfare is the laws of armed conflict (LOAC).[56] That is, without any general agreement on the detail, various commentators, including those connected with the

[50] See Part 10.6 Telecommunication Services. This includes "interference with telecommunications", "wrongful delivery of communications", "interference with facilities".
[51] Under ISA section 14(2), the immunities applicable for domestic activity still require a specific overseas aspect to the activity.
[52] The *Telecommunications Act 1997* (Cth) also contains significant provisions requiring telecommunication carriers to protect, amongst other things, the contents of communications (which will include computer data),[52] which may be of direct relevance to Defence given its use of the general NII infrastructure for much of its communications.
[53] ISA section 8(2).
[54] Inspector-General of Intelligence and Security (IGIS), 'Annual Report 2007-2008', p. 55. CDF directive issued 4 September 2007.
[55] Inspector-General of Intelligence and Security, 'Annual Report 2007-2008', p. 55. IGIS comments that in this context he has visited these "specialist units with a senior member of DSD, and was satisfied with the compliance regimes and reporting processes put in place by DSD."
[56] For example, Michael N. Schmidt, 'Wired warfare: Computer network attack and *jus in bello*', *International Review of the Red Cross*, vol. 84, no. 846 (June 2002), p. 365; Captain Robert Hanseman, 'The realities and legalities of information warfare', *The Air Force Law Review*, vol. 42 (1997), p. 173; Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, Second Edition (Washington, DC: United States Department of Defense, November 1999), (copy held by author); Major General Charles J. Dunlap, Jr., 'Towards A Cyberspace Legal Regime In The Twenty-First Century: Considerations For American Cyber-Warriors', *Nebraska Law Review*, vol. 87 (2008), p. 712.

United States Military,[57] have accepted the application of the principles of military necessity, distinction, proportionality and humanity to cyber warfare, and most particularly, that cyber means and effects could be viewed as analogous to kinetic means and effects in conventional warfare. This has profound implications for offensive cyber warfare in particular.

The positioning of a 'warfighting' function within a civilian element raises questions regarding the legal propriety of such action under the LOAC. If civilians take a "direct part in hostilities",[58] then they lose their immunity from attack and possibly expose themselves to criminal prosecution. This situation could be moderated by internal arrangements whereby only uniformed ADF members actually engage in the cyber-warfighting activities, but such a dichotomy may be difficult to maintain. On a wider policy level, the Australian Government may consider that in era where the physical and legal distinctions between 'warfighters' and the general civilian population have been challenged (particularly by non-state actors), it is in interests of nation states to demonstrably confine the conduct of combat operations to uniformed military personnel, if only to avoid allegations of hypocrisy.

Notably, little of the publicly available work on the subject of the LOAC or other elements of international law relating to cyber security and cyber warfare issues, has emanated from Australia, whether from academic, military or other government sources. Moreover, there is little guidance on how the Australian Government might perceive its international legal rights or obligations either inside or outside of armed conflict. In particular, there is no coverage of cyber legal issues (international or domestic) in either the ADF legal doctrine available on the internet,[59] or in other joint doctrine. Moreover, the last significant quasi-official Australian attempt to discuss the applicable international legal framework was published in 1997.[60]

Conclusions: A Need for Greater Clarity in a Sensitive Area

Presently, it is unclear in the Australian context, whether the term 'cyber warfare' is confined to military activity or has application outside of a genuine armed conflict. Moreover, the use of the term 'cyber security' does not inherently indicate that offensive or even 'active defence' operations, are or are not excluded. Overall, what is inside and outside of the scope of

[57] Each of the authors cited at footnote 56 is either a past or present member of the US military.
[58] Article 51.3 of The 1977 Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflict [Protocol I] Australian Treaty Series 1991 No. 29.
[59] Royal Australian Air Force, *AAP 1003 – Operations Law for RAAF Commanders*, Second Edition, Air Power Development Centre, May 2004.
[60] Chris Westwood, *The Future is not what it used to be: Conflict in the Information Age*, Air Power Studies Centre, RAAF Base Fairbairn, 1997. This is a RAAF Fellowship Paper which includes a chapter on domestic and international legal aspects.

terminology is unclear, and while setting rigid boundaries may be unhelpful,[61] some effort should be expended to develop and then maintain a set of definitions that are reasonably current. The absence of a clear distinction between cyber security and cyber warfare reduces public scrutiny of, first, the functions that have been assigned to the ADO (and DSD in particular), second, whether the organisational structure is therefore suitable for those intended functions and, finally, whether the existing legal constraints are challenged.

The scope of the CSOC's function is thus unclear and the description of its functions in the White Paper, set in the context of the wider discussion of cyber security and cyber warfare, could even be viewed as evasive. Considering the ambiguity in the function, Ball's observation regarding the "organisations operating in the Defence intelligence or cyber-security areas" that "none of them has any mandate for the planning and preparation of offensive cyber-warfare activities" may still be correct.[62] Moreover, if the role of the CSOC is to conduct all facets of cyber warfare, then this raises the structural issue, with policy, organisational and legal aspects, that the Australian Government has positioned a war-fighting function within an element that is not commanded by the CDF.

As matters stand, if DSD became the focus of cyber warfare activities, then unlike the elements of ADF combat power that fall under a military chain of command descending from CDF, any prospective cyber warfare capabilities may be being deployed by civilian personnel who are not subject to the control of a military discipline system. This raises the question whether personnel engaged in cyber warfare operations, at least to the extent that the operations may lead to property damage or casualties, must, or should be, subject to military discipline. That is, a disciplinary system that may severely sanction individuals for disobedience of the commands of their superior, for instance, to execute or not execute a particular cyber mission, or to execute it in a particular way. While this issue has an international law dimension, the policy aspect is highlighted here. Essentially, it is important that a conscious decision is made regarding the nature of the control that is placed on the deployment of cyber warfare capabilities, and this includes consideration of the status of the personnel involved in the delivery of that capability.

Whether or not Australia possesses an offensive cyber warfare capability may be considered a sensitive issue. A reflex reference to 'security classification' to deflect discussion is, however, unhelpful and out of step with what is occurring in the United States, where senior military leaders

[61] As Ball, points out "Cyber-techniques will be increasingly used to penetrate the electronic components in weapons systems." Waters, Ball and Dudgeon, *Australia and Cyber-Warfare*, p. 124.
[62] Waters, Ball and Dudgeon, *Australia and Cyber-Warfare*, p. 130.

have been reasonably frank.[63] If Australia actually has an offensive cyber warfare capability then the contrast with the United States' approach may suggest that the ADO lacks confidence in its own position despite the bold statements in the White Paper. If, alternatively, Australia lacks a capability, then perhaps it should not be using the term 'cyber warfare' at all. More importantly, this raises questions of 'why not', given comments from senior United States military leadership which indicate that offensive and defensive cyber capabilities must come as a package, as well as the views of Australian commentators that an offensive cyber warfare is required.[64]

The wider issue is that if Australia's cyber capabilities are currently or remain under-developed, the potential consequential problem for Australia is that this could compromise a core tenet of wider defence policy, that is, the conduct of NCW.[65] In essence, if Australia is not positioned to protect its NCW assets from cyber attack, nor able to access the networks of its adversaries through cyber techniques, then a fundamental premise upon which the ADO is resting into the future, is undermined.[66] This risk is magnified by the ADO's reliance on non-ADO/non-Government infrastructure and linkages for much of its communication. Short-term this could be a valid basis for prioritising defensive over offensive measures, but then again, as suggested by the US military, offence (or at least counter-attack) may be the best form of defence.

The legal dimension is worth re-emphasising. The ADO is set on an ambitious program with no evident position on the application of international law and no recent or readily available local debate on the international legal perspective. There is also a possibility that civilian DSD staff may be exposed to both physical and/or legal risk through the application of international law. With respect to domestic law, the ADO's legal position has not been altered to take on new or, arguably, its existing roles. This raises questions regarding DSD's functional allocation under the ISA and the potential risk to ADO members of falling foul of the criminal law. Most particularly, while benign computer security measures fall inside DSD's

[63] For example, Marine Corps General James E. Cartwright, Vice Chairman of the Joint Chiefs of Staff, See Jim Garamone, 'Questions Abound in Cyber Theater of Operations, Vice Chairman Says', American Forces Press Service, 8 April 2009, US Department of Defense, 'News', <http://www.defenselink.mil/news/newsarticle.aspx?id=54709> [Accessed 26 July 2009]. Further example, Air Force General Kevin P. Chilton, Commander, US Strategic Command, See Jim Garamone, 'Cyber Defense Cost Pentagon $100 Million in Six Months, Officials Say', American Forces Press Service, 9 June 2009, US Department of Defense, 'News', <http://www.defenselink.mil/news/newsarticle.aspx?id=53852> [Accessed 26 July 2009].

[64] Specifically comments by Air Force General Kevin P. Chilton, in 'Cyber Defense Cost Pentagon $100 Million in Six Months, Officials Say'. Note also, Waters, Ball and Dudgeon, *Australia and Cyber-Warfare*, which in multiple places stresses the need for an offensive cyber warfare capability. See, for example, pp. ix, 34, 130.

[65] It has been given prominence in the White Paper. See Department of Defence, 'White Paper', p. 82, para. 9.82, concerning situational awareness.

[66] See Waters in Waters, Ball and Dudgeon, *Australia and Cyber-Warfare*, p. 112.

express functions, everything else is a matter of interpretation. The current domestic laws were not drafted with 'active' cyber defensive measures and certainly not cyber offensive measures, in mind.

If it is the intention of the Australian Government to deploy an offensive cyber capability in peacetime (that is, outside of a genuine 'armed conflict'), this would require amendment of domestic law. This will make it difficult to avoid public discussion, particularly with respect to proactive moves to enable agents of the ADO to interfere with private individuals and elements within Australia. The open nature of the Australian parliamentary and legislative system means that the Australian Government would need to enter the process assuming there will be a great deal of public interest and attention, if not a requirement for explanation.

The Australian Government has also embarked the ADO upon a cyberspace agenda with little elaboration on how Australia's capabilities will fit within a global framework, and relate to its friend and allies (notwithstanding DSTO's prospective role). Noting the geographically unbounded nature of cyberspace, this appears to be a deficiency at least in the current public debate.

There are, however, three important positive aspects. First, the lodgement of the CSOC within the ADO, rather than as a standalone organisation or as an adjunct to one of the other members of the AIC, does mean that the CSOC can leverage off existing expertise and capability already resident in DSD. Provided that the lead agent on cyber security, the Attorney-General, is satisfied that they still have sufficient cross-departmental control, influence and/or supervision of an ADO element, then the location of the function is practicable. Second, undeniably the CSOC's lodgement within DSD, facilitates the creation of a 'one-stop', consolidated cyber capability covering both security and warfare within the one department (even if not within the ADF). Finally, the White Paper indicates that the Australian Government has preserved a flexible approach, stating that if the "risk of cyberattack is even greater than we had first thought, … we might decide to build on a foundation in this area by further enhancing our cyber security capabilities".[67]

The White Paper discloses the intent to defend Australia from cyber-threats, but the ways and means have not yet been presented for serious public discussion, albeit that the Australian Government will remain open-minded regarding responding to an increased threat of cyber attack. Moreover, the current lack of transparency is set against a history of relatively little public discussion in relation to the ADO's involvement in cyber security and cyber

[67] Department of Defence, 'White Paper', p. 29, para. 3.22.

warfare.[68] Consequently, it will be necessary for the cyber warfare component to rapidly mature in a number of contexts. Five recommendations flow from this analysis:

First, if not already in place, based on the United States model and philosophy, Australia should consider acquiring a genuine cyber warfare capability, including offensive and/or counter-attacking capabilities. This may require a reorientation of the CSOC's role.

Second, whether or not the first suggestion is adopted, the Australian Government needs to develop a public affairs strategy concerning cyber warfare that allows it to enter the public debate, like the United States military, without immediately resorting to claims of security sensitivity. In essence, the Australian Government needs to be able to talk about cyber warfare to the greatest extent practicable as just another weapons system.

Third, to comply with domestic legal obligations, a thorough review should be conducted of the ADO's legal position before any deployment of offensive, counter-attacking or intrusive methods is contemplated (at least during peacetime). If amendment to legislation is required, then these should be considered.

Fourth, noting the international legal operations under the LOAC and other policy considerations, allocating the genuine warfighting aspects of the cyber warfare capability to a distinct element of the ADF, whether located within DSD or otherwise, should be considered.

Fifth, and finally, an Australian-based philosophy on the application of the laws of armed conflict to cyber warfare needs to be developed.

Chris Hanna is studying for his Master of Arts at the Centre for Defence and Strategic Studies, Australian Defence College. A lawyer by training, he holds the rank of Group Captain in the Royal Australian Air Force. The views expressed in this article are those of the author alone. chrishanna@hotmail.com.

[68] For instance, prior to the publication of *Australia and Cyber-Warfare* in 2008, the last major work was produced by Chris Westwood in 1997. See Westwood, 'The Future is not what it used to be'.