Australia’s Defence White Paper 2015: Submission by Ian Dudgeon

Cyber Operations: The Requirement for Effective Defensive and Offensive Capabilities Across the Cyber Domain

Introduction

During war, or other circumstances involving hostilities between states, or states and non-state organisations, two key primary targets will be capability and will. 

Capability relates to the combat and logistic capability of both sides to mount and sustain hostilities, and will applies to the psychological and political commitment of the related combat forces, population generally, and government to pursue hostilities.

The cyber domain is a common and critical factor for both capability and will. Effective offensive cyber operations across the cyber domain are able to have a significant adverse impact on a targeted state or organisation’s capability and will. Effective defensive cyber measures are essential to mitigate the threat of offensive operations.

The ability to conduct effective offensive and defensive cyber operations is a capability that Australia must have for defence and broader national security reasons.

The Importance of the National, Global and Defence Information Infrastructures

The above information infrastructures make up the cyber domain. They are also the means for targeting capability and will.

We live in the Information Age where Australia’s society, the societies of all other developed and developing countries, and key areas of the government and the private sector in undeveloped countries, are dependent on the functionality of the cyber domain. Within the cyber domain – or cyberspace - the two key elements are information in digital or electronic form, and its supporting information technology (IT). These two elements are inter-dependent.

At the national level, the above elements, collectively, form the national information infrastructure (NII) which comprises the information itself and the hardware and software within and over which information is collected, processed, stored and transported. The NII’s seamless connectivity with similar infrastructures of other countries creates the global information infrastructure (GII), of which the internet is a major part.

The defence information infrastructure (DII) is also a part of the cyber domain. However, an estimated 10% only of the DII is exclusively owned and operated by Defence, and this mostly relates to combat communications systems. The remaining 90% is leased or shared services sourced within the NII, and GII, and provided by the private sector. In sum, the DII reaches across and is dependent on the full national and global spectrum of information infrastructures.

Dependency on the Cyber Domain

Understanding dependency on and inter-dependencies within the cyber domain is the key to understanding cyber operations. Dependency impacts on both capability and will.

Our dependence, and that of others, on the functionality of the cyber domain encompasses almost all the functions of government, business, and society generally. In government, dependencies include such key areas as treasury, social services, international relations, and emergency services
including defence; for business those dependencies underpin such fundamentals as industrial production, all forms of logistics, power supply, finance and marketing; and within society generally, they reach across such basics as transport systems, banking, shopping and the social media. The very high level of inter-dependence between these sectors of society is also a feature of the cyber domain.

For the ADF especially, dependency on the cyber domain spans both the tactical and strategic space, from its deployed front-line combat forces (sea, land, air, space) to its domestic or foreign sources of logistic supply and supporting delivery systems.

**Information Assurance**

Information assurance (IA) directly impacts on dependency. IA is about the timely availability of information, the integrity or reliability of that information, and confidentiality of information where this is a critical factor\(^1\). IA dictates the functionality, and thus value of the cyber domain, inclusive of the GII, NII and DII. In sum, IA impacts directly on capability.

IA is an essential factor in underpinning the effectiveness of the ADF’s planned networked information architecture that seeks to provide real-time connectivity and communications across its intelligence, surveillance, reconnaissance (ISR) and command and control (C2) systems. Redundancy and diversity, and high-grade physical, personnel and technical security protocols are essential ingredients of IA, and for assuring the functionality of all, especially networked systems.

**Cyber: Offensive Operations**

Offensive operations target IA through access to the exploitation of potential vulnerabilities of software and hardware (inclusive of power supply - without power, hardware and software cannot function). Types of operations include:

- intelligence collection: penetration or exploitation of software by hacking and/or ‘insider’ agent operations to breach confidentiality. Intelligence collection would seek access to or enable informed assessments about a hostile’s intent and tactics. Knowledge about these would diminish the effectiveness of their capability.

- diminishing a hostile’s capability by adversely affecting the availability and integrity/reliability of information/intelligence accessible to them:
  - penetration as above to insert malware to destroy, deliberately alter, or disrupt or corrupt key operational and/or logistics data/communications.
  - use of kinetic and non-kinetic weapons to destroy, deny, disrupt and corrupt targeted communications and/or supporting systems\(^2\). The effects may be short or longer term, and could include tactical combat, ISR and strategic/logistic systems.
  - strategic/logistic targeting above could include private sector-owned NII/DII elements engaged in homeland weapons production and logistics/supply to combat

---

\(^1\) Confidentiality is critical for many functions of government for both national security and other privacy reasons. National security reasons include protecting information about key aspects of defence capabilities, policy and plans, foreign policy, and the capabilities and effectiveness of our intelligence agencies.

\(^2\) Non-kinetic means may include use of a new suite of high energy radio frequency and other electronic weapons now being developed that can burn-out or otherwise disrupt and corrupt IT systems.
forces. In some circumstances, such targeting might also impact on the civilian population where these defence production industries, transport and power supply systems serve dual civilian-military customers³.

Offensive cyber operations also include separate psychological operations that specifically target will. The array of potential operations could include the penetration and specialist exploitation of all available direct and indirect messaging systems, including the modern and social media, with potential reach across the military, public and political spectrum. They would be mounted across the cyber domain in parallel with other cyber and non-cyber operations, and pick up on diminishing morale due to capability loss, to coordinate and maximise their effect.

**Cyber: Defensive Operations**

Defensive operations must be able to mitigate the threat from offensive operations undertaken by a hostile state, or non-state organisation. Qualitative measures must apply not only across the DII, but key elements of the NII and GII which could be targeted. Effective IA demands a binding partnership between government and the private sector. To meet this demand, strong government leadership is essential.

However, because of our national dependency on the cyber domain, *its defence is also a national necessity in its broadest sense*; organised crime, other issue motivated groups and accidents also threaten infrastructure, and do so more consistently. There is a very high level of overlap between defence and broader national interests, and planning should be coordinated accordingly.

**Conclusion**

Cyber operations are not a replacement for the traditional political and military tools of war or other hostilities, but are a critical supplement. Used offensively, they offer significant potential and often asymmetric advantages, and offensively and defensively they could truncate any period of hostilities and save military and civilian lives. Australia must develop advanced capabilities in both for defence and broader national security reasons.

Ian Dudgeon
Ian Dudgeon & Associates P/L
27 October 2014

³ Any targeting by Australia of a hostile state’s NII/DII that could impact on civilians would be subject to strict review to assess the acceptability of the scope of impact, and ensure activities were lawful, and met Australian moral and ethical standards.
Australia's Defence White Paper 2015 Submission by Ian Dudgeon

The Importance of a Comprehensive Intelligence Collection and Assessment Capability

Introduction

*Knowledge is Power* is a common expression which is directly relevant to Australia’s defence capability requirements. In this context *knowledge* is both the quality of

- the *collection* of all-source information about strategic, operational and tactical matters of defence interest, and
- the *assessment* of that information to produce intelligence that contributes to *power*.  

*Power* in this context is the quality of the resultant decision making, inclusive of policy formulation and planning, and the implementation of action relevant to those interests.

This submission promotes the importance of Defence’s investment in *knowledge*.

Collection

Collection requires a clear understanding of requirements, both short and long term, and their priorities. While any area of actual or probable ADF deployment, including out-of-region deployments, must be afforded appropriate priority, the area of Australia’s priority strategic interests - the archipelago to our immediate north inclusive of Timor Leste and PNG, and the SW Pacific - must be the focus of comprehensive enduring collection.

That collection must include all data relevant to the conduct locally of combat operations, peacemaking, peacekeeping or significant humanitarian operations, consistent with the government’s political objectives. Collection must encompass not only information of tactical significance (e.g. capability and tactics of local security forces, roads, railways, harbours, airports, communications systems etc.) but also key sociological information about such fundamentals as national and regional politics, tribalism culture and religion that is essential to enable or shape, ultimately, a political outcome consistent with Australian interests.

Collection must be all-source, including open-source information available through the local media, other local government literature, academia, and drawing on the resources of DFAT, Defence Attaches, the defence intelligence collection agencies e.g. the Australian Signals Directorate (ASD) and Australian Geospatial Intelligence Organisation (AGO), other Australian foreign intelligence collection agencies e.g. the Australian Secret Intelligence Service (ASIS), and any relevant foreign liaison sources.

The ideal should be no gaps in essential information, and data should be regularly reviewed to ensure it is current. Updating contingency planning and regular gaming will facilitate both.

Collection is a demanding and resource intensive investment. It must be relevant, of high quality, comprehensive and timely.

Assessment

Quality assessment depends on and demands quality collection. This applies also where the collection, assessment, decision and action cycle is all technical e.g. sensor to trigger systems. For these systems, high quality programming, inclusive of input, is critical to ensure that threats are accurately identified and responded to. Inaccurate or incomplete collection data can have a
significant negative impact on the accuracy and value of an assessment, and thus resultant decisions and actions. Deficiencies in the quality of assessments can cost time, resources and lives. They can also result in mistaken targeting with tragic consequences.

Investment in the quality of assessment resources is as important as for collection resources. Team leaders of assessors at all levels must be qualified and experienced, not only in the assessment function, but also in the subject matter itself and context relevant to the subsequent decision and action process. Assembling such assessors, particularly where targeted situations are unique in nature, may require accessing specialists from elsewhere within or outside government e.g. DFAT or academia, to meet particular requirements. In some cases the collectors and assessors may be one and the same person, or institution. Whatever the formula, the goal and key outcome must be quality.

The Fusion Process

This process is where the collectors, assessors, and decision-makers work as an integrated team to maximise the timeliness and effectiveness of action and outcomes. It is particularly relevant in live combat situations where all the resources feed in to and out to each other in real or near-real time to enable combat forces to maintain situational awareness and exploit operational opportunities and momentum to advantage. This was particularly effective in the latter stages of the deployment of ADF forces in Afghanistan; the co-location of most combat and intelligence elements, and real-time networked linkages to other elements, including those based in Australia, fostered a strong sense of teamwork and achievement. It is important that this process be further developed, and the teamwork exercised through gaming.

Conclusion

Comprehensive high-quality knowledge is a key element of defence capability. Investing in knowledge, to maintain and further develop both its collection and assessment elements, is an essential Defence priority requirement.

Ian Dudgeon
Ian Dudgeon & Associates P/L
27 October 2014