The Need for a Contingency Plan if C4ISR, GPS and Other Technologies are Made Inoperable

This submission to the 2015 Defence White Paper (DWP), argues that a detailed contingency plan needs to be incorporated into the ADF’s force structure to be prepared for the loss of advanced networks, GPS, and other technologies. The ADF is growing increasingly more reliant on technologically advanced systems with the growing integration of C4ISR, GPS, and many others. These systems are therefore incredibly valuable targets for potential aggressors and are particularly vulnerable. The 2015 DWP needs to not only commit to defending these technologies as the Department of Defence did in the 2013 DWP, but also to commit to a contingency plan if these systems were attacked and made inoperable.

Western military superiority increasingly depends on GPS and advanced networks. Command, control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR), and the many military satellites in orbit are increasingly becoming the backbone of this military superiority. These networks not only coordinate or integrate forces effectively, but also are a necessity in the use of many advanced weapons systems.\(^1\) Therefore, the satellites and networks that make this possible are highly valuable targets to potential enemies. Destroying military satellites and using cyber-attacks against computer networks,

would seriously cripple western war fighting ability, and leave our forces vulnerable to powers that still have them intact.²

Indeed, the militarisation of space and cyberspace is already underway. China is developing anti-satellite missiles and offensive cyber capabilities in order to deter western forces by exploiting this reliance on advanced technology³. Its focus on these asymmetrical capabilities is testament to the weaknesses inherent in modern militaries that overly rely on advanced technology and networks for battlefield superiority. No reason exists to think that nations with inimical interests will not acquire similar capabilities in the future.

Therefore, the ADF’s force structure needs a contingency plan in place if the C4ISR networks, GPS systems and other technologies are made inoperable. These technologies are vulnerable and difficult to defend⁴. In a serious crisis these capabilities may be some of the first to be made inoperable by an opposing state.

Simply making a commitment to develop a stronger defence of ‘joint and enabling’ capabilities is not enough. A contingency plan would dampen the effectiveness of these asymmetrical capabilities and create a stronger force structure for the ADF. With a contingency plan in place Australia should be able to effectively use the ADF, wherever they may be, even in a worst case scenario.


Although an encouraging amount was written about defending Australia’s cyber networks and joint enabling forces from asymmetric attacks in the 2013 DWP\(^5\), no acknowledgement of the need for a contingency plan was noted. The force structure in the 2015 DWP needs to improve on its predecessor and also commit to a contingency plan if many of these technologies used by our joint enabling forces are made inoperable during a serious crisis.

The implications of this contingency plan could be extensive. However, this does not mean that it will be overly difficult or unrealistic to implement this contingency plan for the ADF. Indeed, knowledge in the operations of the ADF prior to these new technologies is readily available to guide future contingency plans.

Regardless of difficulties, if the ADF continues to develop a reliance on this vulnerable technology without being prepared to operate effectively without it, Australia’s force structure will be weak against those who can exploit this weakness. The 2015 DWP can improve on its predecessor by committing the ADF to countering this weakness in Australia’s force structure.


\textit{Jacob Mark Simpson}  
\textit{Student at the Strategic and Defence Studies Centre}  
\textit{Australian National University}

\hspace{1cm}