Jump TO Article

Jump TO Article

Military aspects of cyber warfare

An edited version of a presentation to the
2016 Seminar on Military Strategy on 31 May 2016 by

Brigadier Marcus Thompson, AM

Commander, 6th Combat Support Brigade, Australian Army[1]
Chief of Army's Special Adviser on Cyber Security and Cyber Warfare

The Australian Defence Force, well-practised in cyber warfare at the strategic level, is developing the capability to engage in cyber warfare at the operational and tactical levels. Here, Marcus Thompson outlines planning considerations; describes the operational and tactical employment of active and passive cyber defence measures; and explains what it takes to be a cyber warrior.

Key words: cyber warfare; operational planning; cyber operations; cyber tactics; cyber intrusions; cyber attacks; cyber personnel.

The Australian Defence Force has recently joined our 5-eyes coalition partners in recognizing cyberspace as another warfighting domain, along with sea, land, air and space. While cyberspace affords new means and methods for the conduct of warfare, war remains a fundamentally human endeavour, rather than a technical or engineering problem. Cyber effects, when used in isolation, are unlikely to achieve a decisive outcome; but they are highly likely to be key enablers of military operations, similar to indirect fire or air-delivered munitions.

There is little that is new in cyber warfare. Theft, espionage, deterrence, defence, and attack are not new concepts. What is new is the conduct of these activities in cyberspace. The Australian Defence Force (ADF) has increased its reliance on capabilities that operate in or through cyberspace. We have nascent cyber security and defensive capabilities, which will need to grow if we are to meet the threats of a range of actors, both at home and abroad. The Army's own modernisation path includes the digitisation of Army's command and control systems; and similar initiatives exist within the other Services. This will provide manoeuvre commanders with greater decision superiority, but it also increases our vulnerability to attack. Therefore, appropriate measures must be applied to protect the ADF's freedom to manoeuvre in the cyber domain.

In this paper, I will present the case for the ADF to generate cyber capabilities for use at the tactical and operational levels; I will then offer a broad description of the types of passive and active effects that we might seek to apply in a deployed joint task force setting; before concluding with a brief comment on the type of cyber workforce we need to develop within the ADF.

Operational and Tactical Cyber Planning Considerations

At the operational and tactical levels, we must apply cyber considerations to our existing doctrinal arrangements for the planning and conduct of operations. Essentially, we need to normalise cyber operations within our current approach to campaigns and operations, across the spectrum of armed conflict, as we have for each of the other warfighting domains.

At the operational level, this would involve planning and conducting operations to achieve a broad set of objectives for Commander Joint Operations, and/or a deployed Joint Task Force commander. Planning should involve a detailed understanding of the threats faced, as well as the information networks and systems that we intend to deploy. Targeting and intelligence functions also must be deployed in direct support of technical practitioners.

At the tactical level, the use of the cyber domain could involve the delivery of cyber effects against closed networks that are otherwise beyond reach. Commanders will also need to be mindful of actions that may inadvertently threaten the security of our own networks – such as the use of mobile devices, sending malware-embedded files to protected networks, or clicking on links in phishing emails. The actions taken to protect our networks and deliver cyber effects are analogous to our current doctrine for the conduct of information operations (IO). IO are planned at the operational level, and then conducted at the tactical level, by distributed force elements, to achieve stated information objectives. The planning and conduct of cyber operations to execute tactical actions to achieve operational objectives could be achieved in a similar way.

Cyber intrusions (or what some call cyber attacks) can occur, and are currently occurring, during what we would otherwise consider to be normal peacetime engagement. Imagine what would happen if soldiers from a foreign nation, without prior knowledge or authorization, commenced military activities, shaping operations or intelligence collection on Australian soil. Whilst some of this is considered normal for foreign intelligence services, it is not for foreign militaries. Yet, there are many reports in the open-source media of activity and intrusions performed by regional military units conducting malicious activities in cyberspace.

In combat operations, we expect that cyberspace will be more contested. It is easy to envisage a scenario where adversary cyber effects might move from espionage and disruption; to denial, sabotage, and the potential des-

[1]E-mail: marcus.thompson@defence.gov.au

truction of capabilities through cyber means.

The ADF must be vigilant to threats across the entire spectrum of conflict. In a non-combat overseas humanitarian assistance or peacekeeping mission, it may be difficult for a threat to gain physical access to our capabilities without detection. However, it may be far easier for them to access our networks and systems though cyberspace, including via the electromagnetic spectrum. In warfighting, active and passive measures (including cyber intelligence) can support command and situational understanding.

The ADF is increasing its reliance on systems that use cyberspace to support force generation and sustainment. Our protection of these systems is vital if we are to protect our forces from being compromised at the outset. Planners will also need to consider how the use of the cyber domain and cyber effects will support other functions such as force projection, force application, and force protection.

Moving beyond the more theoretical aspects of operations, cyber considerations must be incorporated into our joint planning, targeting, and intelligence functions. Cyber should already be considered during all stages of the joint planning process.

The targeting process, synchronisation of effects, and battle damage assessment will be as necessary for cyber operations as they are for other effects. Planners, operators, and targeteers will need to understand the abilities and limitations of cyber effects, how they synchronise these effects with other non-cyber effects, and what branch plans they need to consider if a planned cyber effect is rendered unusable, due for example, to a change in target behaviour prior to delivery. Following the delivery of a cyber effect, how can an accurate battle damage assessment occur? We understand that the delivery of a bomb or missile has a scientifically-calculated blast radius, which can be used to determine the level of the effect and, of course, the potential for collateral damage. Cyber effects will not necessarily be as easy to predict or assess post-delivery.

Intelligence will be required for cyber operations at all levels. It includes technical intelligence as well as the addition of cyber considerations to existing military intelligence processes and capabilities. Vital information will include knowledge of threat actors and their tactics, techniques and procedures; knowledge of previous threat intrusions and the vectors used; and a detailed understanding of the cyber battlespace, including the types of physical infrastructure, operating systems, and software used in information networks and specific platforms. Without accurate and timely intelligence, it will be extremely difficult to prosecute operations in cyberspace with any degree of confidence.

The Stuxnet Worm

The Stuxnet worm is now widely regarded to be the first cyber weapon. Stuxnet's aim was to find and then sabotage centrifuges at Iran's nuclear facility at Natanz. This worm is believed to have entered the standalone or 'air-gapped' system through a physical means such as a USB thumb drive. Stuxnet's script was targeted towards a specific type of Siemens Programmable Logic Controller (PLC) that was used to control and monitor centrifuges. Ultimately the worm was successful in damaging and destroying a number of centrifuges and reportedly setting the Iranian nuclear enrichment programme back by several years.

The effort taken to plan and conduct this operation must have been immense. Accurate intelligence would have been required about Iran's nuclear programme, including hardware, and the network required to operate the centrifuges. This allowed the planners to target the PLCs and predict the type of effect that Stuxnet would provide.

What is less widely known is that the Stuxnet worm has infected thousands of machines across the world. It does not affect them because they do not contain the specific Siemens PLC needed to execute the script. I wonder whether the people who created the worm considered the containment of their effect. Would it be possible for the target, or an entirely different threat altogether, to re-engineer the script in a worm and use it back against its attacker? I suggest that it is.

I am not advocating that the ADF should be capable of designing and delivering sophisticated cyber weapons such as Stuxnet, but it highlights the importance of the intelligence function to cyber operations, and the challenges associated with containment and battle damage assessment.

Active and Passive Defence

The 2016 Defence White Paper requires the ADF to defend our deployed networks. In order to do so effectively at the operational and tactical levels, the ADF requires both active and passive defensive capabilities. Consider the example of the physical defence of a Forward Operating Base (FOB). In this case, we do not sit inside the FOB waiting for rockets to come over the protective barriers! We dominate the surrounding ground; we assess and determine possible launch sites; and we patrol those areas with rules of engagement that allow us to prosecute any threat to ourselves or those it is our duty to protect. So it is with the defence of our networks – we cannot be exclusively passive.

Active defence is required to deter and respond to threats. Passive defence capabilities are needed to secure and protect networks and systems from intrusion, collection, disruption, denial, or destruction. The ADF also requires all Defence members to have a basic awareness of cyber security and the risks they face, similar to every member being required to know how to use a weapon and render basic first aid.

These capabilities will be required to operate on and protect enterprise networks as well as service-specific systems. The three services each have a role to play in the defence of their own personnel and platforms. An example is Army's Battle Management System (BMS). The Army relies on the BMS for tactical command and control and, therefore, must protect it!

We must also consider the strategic to tactical integration of our capabilities. While the White Paper nominates the Australian Signals Directorate (ASD) and the Chief Information Officer's Group as the leading entities for cyber operations, it is important to recognise that their capabilities, like all highly valuable capabilities,

may at times be in short supply. There will inevitably be a limit to the reach and capacity of ASD, and it may not be able to meet the full expectations of a deployed Joint Task Force commander. The services, therefore, must be able to generate and deploy both passive and active capabilities well forward in support of the immediate priorities of a manoeuvre commander. In some cases, these capabilities may be able to directly support efforts where standalone or closed networks may otherwise be unreachable, especially with regard to military targets.

So let me use another physical security analogy. Most soldiers are familiar with the effects of indirect fire and have been trained in how to call for those effects when required. We understand that to deter and protect ourselves from the threat of indirect fire, we need to aggressively patrol areas where those attacks may be launched. We may also be able to respond with say, counter battery fire or other effects. These examples are analogous to cyber defence.

We need active defence capabilities to deter and shape our adversaries. For example, this could be through the use of honey pots, or malware embedded in files that we *want* the adversary to 'pull' from our network. Deception has been used in warfare throughout history, and the cyber domain affords us many opportunities to deceive an adversary. For example, we might consider creating and operating separate environments and provide false information to mislead an adversary about the ADF's capabilities, plans and objectives.

Continuing the indirect fire example, let me now turn to passive defence. Every member of the ADF knows what types of indirect effects could be employed against them, included range and blast radius. In the presence of an indirect fire threat, everyone knows to wear protective body armour, spread out, and if necessary, seek cover to minimise the impact of indirect fire. In order to protect our networks, and hence our warfighting ability, we must be aware of the threat's capabilities as well as our own network posture. Our capabilities must be able to inform the design and implementation of defensive security measures in operational theatres, including a range of physical, personnel and electronic security measures.

We need the ability to detect intrusions or attacks against our information networks; and to take appropriate measures to respond by rerouting, reconnecting, or even by isolating and sanitising them. It can take an average of 180 to 200 days for many businesses to detect an intrusion on their network. On operations, we could not accept those kinds of delays in recognising and responding to breaches of our own networks.

Importantly, active and passive defence of our networks should occur under the technical control of appropriate strategic agencies. The ADF cannot afford, and nor should it seek, to replicate capabilities resident elsewhere within the Defence portfolio.

Finally, we must not consider passive defence to be an exclusively reactive capability. It must also include proactive steps to search or hunt for advanced threats that may exist on our networks, operating below normal threshold detection levels. Importantly, the ability to understand advanced threats and search for them must also be supported by accurate and timely intelligence.

Personnel Challenges

The cyber effects I have described will ideally be delivered by appropriately trained and empowered military personnel. I see the future workforce comprising of a range of roles, not just technical operators. Many people associate cyber operations with hackers, but it is so much more than that. Sure, we need network specialists, software developers and system administrators. However, the future workforce must also include targeting and intelligence specialists, with an intimate understanding of the cyber domain and the effects that can be employed through it. And leaders, planners and capability developers also form part of a cyber workforce.

Selecting the right personnel to conduct cyber operations should be based on attributes rather than skills. The cyber domain is constantly changing and the required technical skills will require continuous refreshment. Fortunately, these skills can be taught. Any member of the Defence Force with the attributes required to successfully execute cyber operations can be trained to be a cyber warrior, regardless of rank, trade, service, specialisation, full-time/part-time, or gender. To find the right people in a competitive market, the ADF may need to reconsider its recruiting model, physical entry standards, and pay structures in order to open up cyber roles to both new and existing personnel with the appropriate skills and attributes.

Conclusion

Up until now, the ADF's cyber capabilities have largely been within the remit of strategic agencies. There are nascent capabilities in the services, particularly within the Army and Air Force, and we now have the strategic guidance and funding to further develop these capabilities for use at the operational and tactical levels. Despite the best of intentions, military forces cannot always choose the time and place in which they fight. Therefore, if an adversary is in cyberspace, then we need to be prepared to fight there as part of a joint, inter-agency effort just like we do in the other warfighting domains. Established warfighting concepts – new warfighting domain!

There is much work to be done by each Service as we collectively develop our capabilities to operate in this relatively new domain. With the right people, in the right place, and with the right training and equipment, I am confident that the ADF will be able to conduct effective operations in, and through, cyberspace.

The Author: Marcus Thompson is commander of the Australian Army's 6th Combat Support Brigade, which includes the Army's command support and intelligence, surveillance, target acquisition and reconnaissance (CS & ISTAR) units. He is also the Chief of Army's Special Adviser on Cyber Security and Cyber Warfare. He is a former commanding officer of the 3rd Combat Signals Regiment and has recently served in Special Operations Command, and in Afghanistan. He has a PhD in cyber security from the University of New South Wales; has published on the cyber threat to Australia; and was made a Member in the Military Division of the Order of Australia in 2014.