The fog of smokeless war:
A cyber security capability for NZDF

The recently published Defence Capability Plan earmarks an investment on new cyber warfare capabilities for the NZDF. Military cyber threats are increasing, which means a 'defensive' capability makes sense, but with laws of cyber conflict remaining unclear, all is quiet on the 'offensive' capability front.

A big change in the 2016 Defence White Paper from the previous 2010 paper is its focus on cybersecurity in terms of both national resilience and the protection of defence systems. Noting the threat posed by increasing reliance on networked technology, it stated that New Zealand has an interest in "contributing to international cyberspace and space efforts to protect this infrastructure from being exploited or disrupted."

Massey University's Dr Andrew Colarik

While not providing specifics in relation to what a cyber warfare capability may look like, Defence Minister Gerry Brownlee stated at the time that "it will be a significant number of people who are deployed into the armed forces or from the armed forces who will specialise, to a greater extent, in this sort of deterrent."

In a television interview subsequent to the White Paper release, Minister Brownlee indicated that this would include a capability to defend and to offensively retaliate against cyber attacks. Just what this means – like much of the White Paper – has been the topic of much speculation

The recent Defence Capability Plan provides some answers. Firstly, in relation to the amount to be spent, the Plan states that capital investment into this capability, including infrastructure and software, will be within the range of "less than $25 million" out to 2030.

This will buy a learning curve into hardened cyber defence," says Dr Andrew Colarik, an expert in cybersecurity at Massey University's Centre for Defence and Security Studies. "I suspect more will be required if current technologies and events are any indication."

The Plan also clarifies what the cyber security and support capability will be focused on: providing services for deployed operations and specialist military equipment. "As the Defence Force's platforms and networks are frequently deployed abroad," it states, "a similarly deployable, and dedicated, cyber security and support capability is required to enable operations."

In order to meet the intelligence support and cyber protection capabilities enhanced and established by the White Paper, states the Capability Plan, "recruitment will be undertaken across the Defence Force in the area of intelligence data analysis and dissemination."

The capability, however, will not overlap with the Government Communications Security Bureau's national cyber defence role or its foreign intelligence role.

Given that the NZDF tends to deploy in joint operations with other military partners, the capability will need to protect our forces in coalition contexts. "NZDF systems will require an interoperability with the allies they integrate and deploy with," says Dr Colarik. "As such, the risk of cyber-attacks to both information and

infrastructure will be comparable."

On the question of a capability to offensively retaliate against cyber attacks, clarity remains elusive.

"I think their plan to further harden their infrastructure and operational environment is important," Dr Colarik observes. "However, while the fluidity and innovative nature of the battlespace involving network centric warfare greatly enhances military operations, it also requires the means to eliminate those attacks that specifically seek to disrupt and/or eliminate the use of this capability. What form this takes is open to discussion."

The international context

"New technology is helping streamline the transfer of data - a big advantage for defence organisations looking to connect troops and servicemen with the latest intelligence information," says Graham Grose, Industry Director, Aerospace & Defence at global enterprise applications company IFS.

But while advancements in surveillance and IT systems have helped organisations react to emerging insurgent-type threats, says Grose, "as the volume of sensitive and classified data being stored has increased, so has the number of digital vulnerabilities."

"Cyber threats are one of the biggest threats to military organisations right now and are becoming more sophisticated, more damaging and much more frequent. Because of this, the cyber security market is set to be worth over USD 200 billion by 2021.

"Military organisations need an end-to-end solution with a view of entire security operations in order to efficiently monitor and react to attacks. It is imperative that military organisations and troops know that a vehicle, aircraft or naval vessel is not going to be interfered with while out on an operation."

It comes as little surprise, therefore, that while defence budgets have been declining in North America and Europe, "both the US and UK plan on increasing military cyber security spending."

Russia, well known as a source of cyber attacks globally, is widely forecast to continue to enhance its hybrid warfare capabilities – blending conventional, irregular and cyber elements.

In the context of its concerns over an expanding NATO, one of the ways Russia can counter NATO expansion "without physical destruction and without a cost in human lives is to use cyber," Leo Taddeo, Chief Security Officer for Cryptzone, told online publication Cipher Brief. "Therefore, it's natural that the Russians are going to escalate the use of cyber in their efforts to convince us that we should not continue the expansion toward their borders."

Taddeo sees a similar scenario in the contest over the South China Sea. "Cyber is another tool that we will see China use against adversaries like Vietnam, Japan, and the Philippines," he suggests.

The Russian and Chinese use of proxies, such as patriotic hackers, hactivists and media and IT specialists, complicates things, limiting the ability of states to properly attribute cyber-attacks to their sponsors.

"Attribution is extremely difficult," says Dr Colarik. "One network machine can hack another machine which in turn hacks a third. Who is to say which actor belonging to what group launched a given attack when these attacks can occur from anywhere at any time? How do you attribute a machine's actions on to a person, group or state?"

"The smart ones will never get caught. The dumb ones are expendable and likely will have no idea who pulled the strings. In my opinion, decisions regarding attribution are political, and these rarely end well."

Proxies also target the weak. According to Taddeo, "we'll see Chinese proxies – patriotic or directly sponsored – acting against countries that don't have the kind of cyber defences that the United States does."

It all presents a strong argument for boosting cyber security capabilities, but with states scrambling to improve their military cyber security, it also portends the very real spectre of a cyber arms race, which – perversely – favours cyber aggressors due to the fundamental asymmetry of the cyber battlespace.

"The relative cost to develop a weaponised cyber-attack is time and a small learning curve," explains Dr Colarik. "The cost to re-engineer and deploy someone else's weapon is far less. I see an arithmetic progression occurring. The more energy we put into attacks that are deployed, the greater proliferation of the next generation, and its offspring."

A new battlespace

The cyber battlespace is a 'smokeless' one in which state and non-state actors have been inflicting damage on each other for years, but with – arguably – no human casualties. But with increasing reliance on networked real-world capabilities, militaries are increasingly acknowledging cyber as a new battlefield.

"It's like an operational domain: Sea, land, air, space, and cyber," Charlie Stadtlander, chief spokesperson for the US Army's Cyber Command, told Tech Insider. "It's a place where our presence exists. Cyber is a normal part of military operations and needs to be considered as such."

The normalisation of cyber into definitions of conflict, however, is a vexed process, and is likely to remain so for some time.

The NATO Cooperative Cyber Defence Centre of Excellence, established in Estonia in the wake of crippling Russian cyber attacks on that country in 2007, sponsored the preparation of guidelines to address Law of Armed Conflict (LOAC) as applicable to cyberspace.

The resulting 2013 Tallinn Manual on the International Law Applicable to Cyber Warfare, is considered by NATO to be the most comprehensive analysis of how existing international law applies to cyberspace. It is, however, non-binding.

Of course, Russia and China have their own ideas about how cyber should be written into international law, having entered into their own Information Security Pact in 2015. Termed by some as a 'nonaggression pact', the agreement also demonstrates glaring differences between Sino-Russian and Western ideas about what constitutes cyberspace.

And, again, there is the attribution problem. It's no wonder then that many governments and militaries – like New Zealand's – are coy on the question of whether they have – or intend to develop – 'offensive' cyber warfare capabilities. Although the cyber battlespace has been characterised as 'smokeless', its rules of engagement remain obscured in the fog of international cyber politics.