RESEARCH NOTE

GOD DEFEND NEW ZEALAND

DEFENCE MODERNISATION FOR THE INFORMATION AGE

APRIL 2026

JOHN HOWARD

THE NEW ZEALAND INITIATIVE

www.nzinitiative.org.nz

About the Author

Major General (Retired) John G Howard, MNZM

Major General (Retired) John Howard, MNZM, is a Senior Fellow of The New Zealand Initiative and Managing Director of The Source Consultancy. He served over four decades in the New Zealand Defence Force, including as the inaugural Chief of Defence Intelligence, where he shaped NZDF's strategic intelligence enterprise and represented New Zealand across Five Eyes intelligence boards and Military Intelligence NATO.

His international appointments included Deputy Director for Commonwealth Integration at the U.S. Defense Intelligence Agency, the only non-American executive officer serving across all 18 U.S. intelligence agencies. He holds a Master of Management and International Defence Studies and a Master of Strategic Studies.

Published April 2026 by
The New Zealand Initiative
PO Box 10147
Wellington 6143
New Zealand
www.nzinitiative.org.nz

Research Note
ISSN 2816-0347

About the New Zealand Initiative

The New Zealand Initiative is an independent public policy think tank supported by chief executives of major New Zealand businesses. We believe in evidence-based policy and are committed to developing policies that work for all New Zealanders.

Our mission is to help build a better, stronger New Zealand. We are taking the initiative to promote a prosperous, free and fair society with a competitive, open and dynamic economy. We develop and contribute bold ideas that will have a profound, positive, long-term impact.

Contents

Executive Summary

New Zealand has begun to correct a long period of defence underinvestment. The Government's 2025 Defence Capability Plan commits $12 billion over four years, including $9 billion of new spending, and sets a path from just over 1% of GDP to more than 2% over the next eight years. That is a significant shift, and a necessary one. But increased spending alone will not produce a defence force that is modern, credible and useful at the speed the strategic environment now demands.

The harder problem is institutional. New Zealand's defence system still carries too much of the logic of an earlier era – long acquisition cycles, sequential approvals, platform-first thinking and insufficient emphasis on the information, digital and workforce settings that now shape military effectiveness. In a world of contested supply chains, rapid technological change, grey-zone competition and multi-domain operations, capability is no longer defined only by ships, aircraft and vehicles. It is increasingly defined by how well a force can collect, protect, process, share and act on information. The 2025 Defence Capability Plan itself reflects that shift through major emphasis on the information domain, improved intelligence functions, digital modernisation, information management and space capabilities.

That point extends beyond Defence in the narrow sense. New Zealand's first National Security Strategy makes clear that national security now requires a more integrated and open approach across government and society, with stronger cooperation between state agencies, the private sector, communities, iwi and hapū, academia and international partners. The issue is therefore not simply whether New Zealand buys more military equipment. It is whether the country can build a national security system that is sufficiently agile, connected and technically competent to convert investment into real effect.

This paper argues that New Zealand should treat the current uplift in defence spending as an opportunity not merely to recapitalise military platforms, but to modernise the policy and institutional settings that enable capability in the information age. New Zealand already has important foundations in place, including a National Security Strategy, a Defence Policy and Strategy Statement, a Government Data Strategy and Roadmap, a national space strategy and a Defence Industry Strategy. The problem is not the absence of frameworks. It is that these frameworks do not yet amount to a sufficiently coherent, accelerated model for defence and national-security modernisation.

The paper makes four claims. First, New Zealand's strategic history should caution against complacency. The country has repeatedly had to adapt to deteriorating security conditions later and at greater cost than it should have done. The lesson is not that history repeats mechanically. It is that delay in defence preparation carries real penalties, especially for a small and distant state.

Second, the main risk in the current moment is not simply underfunding. It is the possibility that new funding will be absorbed into a system that remains too slow, too fragmented and too focused on industrial-era processes to deliver modern capability at pace. Current official material already recognises the need for a force that is more combat capable, more interoperable, more technologically flexible and more effective in the information domain. The policy challenge is to align institutions and decision processes with those goals.

Third, New Zealand should place greater strategic weight on areas where a small state can generate outsized effect. These include intelligence, especially open-source and AI-enabled intelligence support; secure digital and data architectures; space-enabled services and ground infrastructure; and selected domestic defence and dual-use technologies. The Government's own defence and space

strategies already point toward several of these priorities, including sovereign space capabilities, domestic innovation and information-domain capability. The missing step is sharper prioritisation and faster implementation.

Fourth, New Zealand needs a more precise public debate about defence and national security. The National Security Strategy explicitly calls for greater transparency and a more informed conversation with the public. That debate should now move beyond the old binary of "guns versus butter" and focus instead on the kind of system New Zealand actually needs – one able to protect national interests, support partners, generate credible deterrent effects where appropriate and adapt quickly in a more contested region and world.

On that basis, this paper recommends six areas of action – an independent review of defence capability policy settings; accelerated investment in information, intelligence and digital integration; a defined sovereign space-security pathway; a targeted national intelligence uplift with strong open-source and AI support; a strategic pathway for selected domestic defence and dual-use innovation; and stronger public reporting with independent oversight of defence modernisation progress.

The central argument is straightforward. New Zealand now has more money on the table for defence. The country should use that moment not only to buy new capability, but to redesign the settings that determine whether capability can be generated, integrated and employed at the speed of relevance.

Introduction – New Zealand's warning from history

In the late 1930s, New Zealand entered a deteriorating strategic environment without having adequately modernised for the conflict that was coming. When war arrived, adaptation had to occur under pressure rather than in advance. That is a familiar pattern in the history of small states, where strategic warning appears early, but meaningful adjustment often comes late.

The lesson is not that New Zealand today faces a replay of 1938. The strategic context is different, the threats are different and the character of conflict has changed profoundly. Rather, it is that when governments delay difficult decisions about preparedness, institutional reform and capability, the eventual bill is usually paid under worse conditions and at higher cost.

That lesson is an essential reflection again now. New Zealand no longer operates in the unusually permissive strategic environment that shaped much of the post-Cold War period. The Government's own National Security Strategy states that the country faces a fundamentally more challenging outlook, shaped by strategic competition, disruptive technologies, climate pressures, foreign interference, cyber threats and growing stress on the international rules-based system. The Defence Policy and Strategy Statement similarly concludes that Defence must be fit for purpose in a more challenging and complex world.

The 2025 Defence Capability Plan reflects the same judgement. It is explicit that New Zealand must rebuild the New Zealand Defence Force for a more volatile world, with greater combat credibility, stronger interoperability with Australia and other partners, and improved ability to operate across maritime, land, aerospace and information domains. This is not the language of marginal adjustment. It is the language of overdue modernisation.

That makes the present moment unusually important. For the first time in many years, New Zealand has both an official acknowledgement that the world has become materially less secure and a significant fiscal commitment to begin responding to that change. The risk is that public debate treats the issue as largely settled once additional funding has been announced. It has not been settled.

Funding is only the enabling condition. The real test is whether New Zealand can translate strategic concern into a defence and national-security system that is faster, more integrated and better suited to the information age.

That is why historical analogy still has value. It is not useful as a dramatic device or a claim that governments today are repeating every error of the interwar period. It is useful because it reminds policymakers that preparedness is not measured by intention. It is measured by whether institutions, people, systems and equipment are ready before crisis forces adaptation upon them.

For New Zealand, that means the central question is no longer whether defence deserves more attention. Official policy has already answered that in the affirmative. The more important question is whether the country is modernising in the right way. A defence force can be recapitalised without becoming truly modern. A procurement pipeline can be active without becoming agile. A strategy can be published without becoming operational. The history that matters here is the history of recognising danger too slowly, and of confusing movement with readiness.

This paper therefore begins from a simple proposition – New Zealand's current defence uplift should be judged not by the volume of spending announced, but by whether it produces a force and a wider national-security system that are genuinely adapted to contemporary conditions. That requires more than new platforms. It requires institutional change.

More money is necessary, but not sufficient

The 2025 Defence Capability Plan marks a genuine break from the thin-investment settings that shaped much of New Zealand's recent defence posture. It sets out $12 billion of planned commitments over four years, including $9 billion of new spending, and a path to lifting defence expenditure from just over 1% of GDP to more than 2% over the next eight years. It also frames that investment over a 15-year horizon and commits to reviewing the plan every two years. By any recent New Zealand standard, that is a substantial change in ambition.

That shift is significant for three reasons. First, it brings funding closer to the scale of the strategic problem. The National Security Strategy states plainly that New Zealand faces a more challenging security outlook. The Defence Policy and Strategy Statement similarly argues that Defence must be fit for purpose in a changed environment. The Defence Capability Plan is therefore not simply a spending increase. It is an admission that the permissive assumptions of earlier years no longer hold.

Second, the plan recognises that military utility now depends on a broader conception of capability. It does not only fund traditional platforms. It also includes significant emphasis on the information domain, improved intelligence functions, classified digital services, digital modernisation, information management and space capabilities. That is important because it signals official acceptance that modern military advantage increasingly depends on the ability to connect sensors, systems, data, people and decision processes across domains.

Third, the plan makes a deliberate effort to link defence modernisation to industry and partnership. It describes industry as a critical partner in supplying, sustaining and operating capability, and states that implementing the plan will require a more resilient, agile and innovative relationship between Defence and industry. It also explicitly prioritises interoperability with Australia and partners. That is the right direction for a country that cannot generate all strategic effects alone.

But none of that means the problem is solved. The most common error in defence debate is to assume that announced spending equals delivered capability. It does not. Money can be committed years

before useful effects appear in the field. It can also be absorbed into a system that remains too slow, too fragmented or too poorly configured to convert funding into real readiness. That risk is especially acute when a force is trying to modernise across multiple domains at once while also dealing with workforce pressures, ageing infrastructure, integration demands and rapidly changing technology.

This is where the distinction between recapitalisation and modernisation becomes important. Recapitalisation means replacing or upgrading equipment so that the force can continue operating. Modernisation means changing how the force fights, senses, decides, connects and sustains itself in order to remain relevant in a different strategic and technological era. A country can do the first without really doing the second.

That distinction sits inside the current Defence Capability Plan itself. The document includes major traditional investments, but it also points toward a broader transformation – a combat-capable force with enhanced lethality and deterrent effect, closer integration with Australia, stronger information-domain capability and greater technological flexibility. Those ambitions are modernising ambitions, not merely replacement ambitions. The question is whether New Zealand's wider institutional settings are aligned to achieve them.

That is not a minor question. It is the central one. If the answer is no, then additional funding may still improve the state of the force, but it will do so more slowly and less effectively than the strategic environment now requires. Capability will arrive late. Systems will remain poorly integrated. Digital and intelligence functions will lag behind platform acquisitions. Workforce models will struggle to attract and retain the technical specialists needed to exploit new systems. Innovation will be treated as an adjunct rather than a design principle. Domestic firms will remain peripheral to delivery rather than being used deliberately where they can add resilience, responsiveness or niche advantage.

In that sense, the key policy issue is not whether New Zealand should spend more on defence. It already is. The issue is whether New Zealand is spending in a way that changes the operating logic of the defence system.

That is a harder question because it takes the debate beyond headline funding and into institutional design. It requires policymakers to ask whether current procurement, approval, workforce, digital and security settings are suited to the mix of platforms, software, data, information, talent and partnerships that contemporary defence capability now depends on. It also requires recognition that software-enabled and data-heavy capability often behaves differently from traditional military procurement. Hardware can sometimes be bought in bounded projects with long refresh cycles. Information-age capability more often requires continuous integration, iterative improvement, rapid upgrades, cross-agency interoperability and sustained technical support.

The current Defence Capability Plan offers several clues that this challenge is already understood inside the government. It states that the information domain includes intelligence activities, information operations, electronic warfare and cyberspace operations, and that investment in this area will improve the NZDF's ability to provide greater response options to government and make more informed and faster decisions. It also includes programmes for information management, digital modernisation and improved intelligence functions, explicitly linking them to real-time collaboration, interoperability and strategic decision-making.

That is the correct diagnosis. But a diagnosis embedded inside a capability plan is not enough by itself. It still needs to be matched by the institutional machinery required to deliver it. That is where the current debate remains underdeveloped. Public discussion still tends to focus heavily on headline assets, especially ships, aircraft and combat systems. Those are important, and in some cases overdue.

But they are only part of the capability equation. A modern force also needs the digital backbone, information-sharing architecture, intelligence support, trained personnel and decision systems that allow those assets to produce effect in real conditions. Otherwise New Zealand risks buying visible capability while underinvesting in the connective tissue that makes it operationally meaningful.

This point is especially important for a small state. Large militaries can sometimes absorb inefficiency because they possess scale, redundancy and depth. New Zealand cannot. A smaller force depends more heavily on coherence, prioritisation and the ability to combine modest resources intelligently. It therefore has less margin for slow processes, disconnected systems or capability that looks credible on paper but cannot be integrated effectively across the force and with allies and partners.

That is why more money, while necessary, is not sufficient. It creates an opportunity. It does not guarantee an outcome. The purpose of this paper is not to diminish the significance of the current uplift. On the contrary, the increase in ambition should be welcomed. The point is that New Zealand should now treat this fiscal moment as a chance to do something harder and more important than recapitalise a neglected force. It should use it to redesign the policy and institutional settings that determine whether defence investment becomes modern capability at pace.

The real bottleneck – policy and institutional design

The most important defence question facing New Zealand is no longer whether the country is prepared to spend more. The Government has answered that question. The more important question is whether the institutions responsible for turning funding into capability are configured for the kind of capability New Zealand now says it wants. That is a question of policy and institutional design.

New Zealand does not begin from scratch. Defence already has a Capability Management System shared between the Ministry of Defence and the New Zealand Defence Force. Official material describes it as a scalable and resilient system for delivering a portfolio of complex programmes and projects. It also reflects nearly a decade of earlier reform effort. A 2018 review of defence procurement found that Defence had already delivered 80 of 87 recommendations under the Defence Capability Change Action Programme and had developed an “International Exemplar 2020” vision for a more integrated end-to-end capability management system.

That is important, because the problem is not institutional emptiness. It is a harder problem than that. New Zealand has frameworks, processes and reform history, but the country is still not evidently producing capability fast enough, coherently enough or with sufficient bias toward the forms of capability that now matter most.

A modern capability system has to do at least five things well. First, it has to define capability properly. That means thinking beyond platforms and treating personnel, information, software, sustainment, data, infrastructure, doctrine, security settings and industrial support as part of the same system. Second, it has to make decisions at a speed consistent with technological change and strategic need. Third, it has to integrate across domains and agencies rather than reinforcing stovepipes. Fourth, it has to absorb innovation continuously, not episodically. Finally, it has to generate confidence that public money is being spent prudently, even when delivery models become more agile, iterative and software-intensive.

The current challenge is that those five requirements pull against some of the habits of traditional public-sector defence management. Defence acquisition in a small democracy is rightly designed to be careful. It should be lawful, contestable, documented and accountable. It should not behave like an unconstrained venture-capital fund. But the opposite error is now increasingly costly – designing

systems that are so linear, sequential and risk-averse that they struggle to deliver capability suited to contemporary conflict.

That risk is greater in information-age capability than in traditional procurement. Ships, aircraft and vehicles are often bought through long-cycle projects with defined acquisition milestones. Software, digital infrastructure, information systems, analytics tools, cyber capabilities and some intelligence systems are different. They often require modular procurement, continuous updates, rapid integration, regular refresh and closer interaction between users, technical specialists and suppliers. A system designed mainly for platform acquisition can still purchase these things, but often awkwardly and slowly.

This is where "policy settings" become more than a slogan. The term should be understood concretely. It includes Cabinet approval pathways and thresholds; rules for staged business cases and procurement assurance; how Defence distinguishes between capital acquisition, operating expenditure, software development and service contracts; workforce classification, recruitment rules and pay flexibility for technical specialists; information-sharing and security settings across agencies and with allies and partners; the extent to which experimentation, prototyping and incremental acquisition are treated as legitimate rather than second-best; and whether Defence and wider government can work with domestic firms early enough to shape useful solutions rather than only inviting industry in at the end of a highly specified process.

Unless these settings evolve, New Zealand risks pursuing information-age outcomes through industrial-age machinery.

There are already signs inside official policy that this tension is understood. The 2025 Defence Capability Plan emphasises not only platforms but the information domain, digital modernisation, information management, intelligence functions and space-enabled capability. It also states that industry partnership will be necessary to deliver capability faster and with resilience. The Defence Industry Strategy is even more explicit, describing actions over four years to deliver capability faster, with resilience, in support of the Defence Capability Plan. In other words, the official strategy is already moving toward speed, integration and partnership. The unresolved issue is whether the underlying delivery system is moving at the same pace.

This is not simply a defence bureaucracy problem. It is a whole-of-government problem that sits at the intersection of public finance, procurement, digital policy, workforce settings, security rules and ministerial risk tolerance.

New Zealand's broader national-security architecture already points in this direction. The National Security Strategy says the national security community must become more joined-up, with stronger leadership, clearer accountability and more open engagement where possible. The Government Data Strategy and Roadmap similarly treats capability, infrastructure, leadership and data as connected system issues rather than isolated technical ones. Those documents are not defence manuals, but they support the same conclusion – institutional fragmentation and weak integration are now strategic liabilities, if not strategic risks in and of themselves.

For Defence, that has three immediate implications. The first is that capability should be treated more consistently as a system-of-systems problem. Buying a platform without the intelligence support, data links, digital architecture, trained personnel and sustainment pathways to make it effective is not efficient acquisition. It is deferred capability and operational risk.

The second is that time itself must be treated as a strategic variable. In a more permissive era, slow delivery was often frustrating but manageable. In a faster-moving environment, late capability can be the same as no capability for the purposes that matter. Delay is not neutral.

The third is that agility should not be mistaken for carelessness. The choice is not between rigid control and reckless speed. The real task is to build approval, procurement and assurance models that preserve accountability while being more compatible with modular, iterative and software-heavy capability.

That will require a shift in mindset as much as process. For many years, New Zealand's defence system has operated in a way that encouraged caution, sequence and compartmentalisation. Some of that was rational. Budgets were tight. Strategic pressure was lower. Large acquisitions were infrequent. Public scrutiny of defence spending was often sceptical. But the operational environment has changed faster than many institutional reflexes are capable of matching.

A country that wants enhanced lethality, stronger deterrent effect, better interoperability, improved intelligence functions, digital integration and space-enabled resilience cannot treat those ambitions as just another set of projects moving through an unchanged machine. It needs a machine built for those ambitions.

Defence in the information age

Modern defence capability depends increasingly on the quality of a force's information environment. Platforms still matter. Mass still matters. Geography still matters. But the ability to sense, process, share, protect and act on information now shapes whether those more traditional forms of capability can generate timely and credible effects.

The 2025 Defence Capability Plan recognises that shift directly. It gives the information domain its own place alongside the maritime, land and aerospace domains. It defines the information domain as including intelligence activities, information operations, electronic warfare and cyberspace operations. It also states that investment in this domain will improve the NZDF's ability to respond to threats, provide greater response options to government and make more informed and faster decisions in an increasingly complex environment.

That is a significant conceptual development in the New Zealand context. It reflects a broader reality visible across contemporary conflict and competition. Information is no longer simply support to operations. It is woven through operations themselves. It determines what can be seen, how quickly events can be interpreted, how accurately effects can be directed, how securely forces can communicate and how effectively activity can be coordinated across agencies, domains and partners.

This has practical consequences for a force like the NZDF. A maritime patrol aircraft is more useful when it sits inside a system that can fuse information rapidly, distribute it securely and connect it to decision-makers and allies and partners in usable form. A strike capability is more useful when targeting, intelligence, communications and data-sharing are timely and robust. A deployed force is more survivable when its digital and classified services are resilient and current. A small force is more effective when it can share information quickly with Australia, Five Eyes partners and relevant domestic agencies.

That is why the Defence Capability Plan includes investment not only in major equipment but also in improved intelligence functions, updating classified digital services, digital modernisation and information management. Those programmes are designed to improve real-time information sharing,

interoperability, decision support and the ability to work across multiple domains, networks and countries.

For New Zealand, the implications are especially important because size magnifies the value of coherence. Larger militaries can sometimes compensate for weak information integration through greater scale or redundancy. New Zealand has less margin for that. A smaller force gains more from being connected, informed and interoperable. The quality of its information architecture therefore carries strategic weight out of proportion to its cost line.

This extends beyond Defence into national security more broadly. New Zealand's National Security Strategy describes a more integrated, open and preventive approach to security, with stronger cooperation across government and society. The Government Data Strategy and Roadmap likewise treats data, capability, infrastructure and leadership as linked parts of a wider system. Those frameworks are not military doctrine, but they reflect the same basic truth – decision advantage increasingly depends on whether institutions can turn data and information into coordinated action.

Several strands sit inside this wider information-age challenge. The first is intelligence. The Defence Capability Plan includes improved intelligence functions as a specific investment area and links them to more effective use of existing capabilities, better targeting and improved sharing with other government agencies. That emphasis is well placed. Intelligence matters disproportionately to a small state because it allows scarce capability to be directed more accurately and efficiently. It also supports the broader national-security requirement to understand a more contested and less transparent environment.

Within that, open-source intelligence deserves greater emphasis than it has traditionally received in New Zealand public debate. The intelligence community itself now openly recognises the role of open-source intelligence in supporting intelligence activity. For a country of New Zealand's size, open-source methods offer a particularly important path to wider situational awareness, faster triage and more scalable analytic support. They also fit the reality that a growing share of strategically useful information now exists outside traditional classified collection channels.

The second strand is digital architecture. The Defence Capability Plan includes digital modernisation and information management programmes intended to consolidate and integrate data and digital technologies across services and platforms, improve storage and retrieval of information, and enable growth in analytics and information management capability. That is foundational work. Without it, information remains fragmented, difficult to access and hard to share in secure and timely ways. With it, the force gains the stable base needed for modern combat systems, multi-domain coordination and coalition interoperability.

The third strand is secure communications and classified services. The plan includes continued investment in classified digital services so that NZDF personnel can communicate securely internally and with allies and partners while deployed, receive critical intelligence and maintain interoperability. This is important because contemporary defence activity depends on reliable participation in trusted networks. Secure connectivity is no longer a back-office function. It is part of operational and coalition credibility.

The fourth strand is space. The Defence Capability Plan states that space is critical for modern operations and has become a domain of competition. It points to investment in systems that connect New Zealand into allied and partner networks to understand what is happening in space and improve access and resilience across space-based services such as communications, surveillance and navigation. This sits alongside New Zealand's wider Space and Advanced Aviation Strategy, which

includes sovereign space capability development, use of space-based data for national security outcomes and government roles spanning regulation, policy and strategic interests.

That combination is key because space-enabled services increasingly underpin activity across national security, maritime awareness, civil resilience and defence operations. For New Zealand, assured access, domestic ground infrastructure, data exploitation and selected sovereign capabilities may all carry more strategic value than public debate has yet fully absorbed.

The fifth strand is people. Information-age capability depends on technical specialists as much as on military hardware. Data engineers, software specialists, intelligence analysts, cyber operators, information warfare personnel and digital architects are now part of the core capability equation. The Defence Capability Plan itself recognises this in describing investment in new hardware, software and skilled personnel across the information domain, and in proposing an Information Warfare Academy to strengthen training. That is a useful start. The harder question is whether wider public-sector workforce settings, recruitment models and career pathways are adequate to build and retain these people at the depth required.

This has a direct bearing on New Zealand's strategic choices. A small state cannot match larger allies and partners in scale. It can, however, become more valuable by being sharper in selected areas that improve collective effectiveness. Information-age capability offers several such opportunities – better intelligence support, stronger data integration, resilient digital services, niche space contribution, effective open-source analysis, trusted interoperability and domestic innovation in dual-use technologies.

Public debate in New Zealand still tends to give greater attention to visible hardware than to these less visible enablers. That is understandable. Ships, aircraft and combat systems are easier to see, easier to debate and easier to count. Information architecture, analytic workflow, digital resilience and data integration are less tangible. Their operational value is no less real. In some cases it is more decisive, because they shape how everything else performs.

That should influence priorities. Defence modernisation in New Zealand should place sustained weight on the information domain, not as a secondary adjunct to traditional force structure but as a central determinant of effectiveness, interoperability and speed. The country's existing strategic documents already provide room for that move. The next step is to treat information-age capability as a primary organising principle for investment, workforce design and institutional reform.

Building sovereign advantage – space, intelligence and domestic innovation

New Zealand cannot pursue sovereign capability across every domain at a meaningful scale. The country's size, geography, fiscal base and labour market rule that out. Serious defence policy therefore requires selectivity. The strategic task is to identify areas where New Zealand can generate disproportionate value for itself and for close partners, and where investment strengthens resilience rather than producing small, expensive replicas of what larger allies already do better.

Three areas stand out: space, intelligence and selected domestic innovation.

Space

Space has moved from the margins of New Zealand policy to a position of growing strategic importance. The Government's Space and Advanced Aviation Strategy sets an explicit objective of developing sovereign space capabilities through a national space mission, supporting local space technologies and enabling the use of space-based data for environmental and economic outcomes. It

also places security, regulation and strategic interests inside the same policy frame, with MBIE, MFAT and the Ministry of Defence all holding defined roles.

The 2025 Defence Capability Plan takes the next step by treating space as critical for modern operations and a domain of competition. It points to investment in systems that connect to allied and partner networks in order to understand activity in space and improve access and resilience across communications, surveillance and navigation services. It also recognises that space-based systems are now relied on for intelligence, surveillance and reconnaissance, communication, navigation and targeting.

That combination gives New Zealand a stronger foundation than public debate often assumes. The country already has an active launch environment, an established regulatory framework under the Outer Space and High-altitude Activities Act, and further policy development underway around ground-based space infrastructure. It also has a policy architecture that links sovereign capability, economic opportunity and national-security interests more directly than was the case only a few years ago. The strategic opportunity now lies in moving from general support for the sector to a more defined national-security pathway.

That does not require New Zealand to aspire immediately to a large sovereign satellite fleet. It does require clarity about which space-linked functions the country should be able to assure, influence or exploit more directly. Those functions could include maritime domain awareness, secure access to allied and partner-enabled services, domestic ground infrastructure, space domain awareness contribution, data processing and exploitation, hosted payload opportunities and dual-use support for disaster response and Pacific resilience.

For a small state, the real prize is not symbolic presence in space. It is assured utility. The question should therefore be framed functionally: what space-enabled services are so important to New Zealand's national security, civil resilience and regional role that the government should seek more direct assurance over access, exploitation and sustainment?

This is worth considering, because dependence without leverage creates fragility. The more that communications, navigation, surveillance and decision-support rely on space-enabled systems, the greater the value of domestic capacity in the ground segment, data layer and associated specialist workforce. New Zealand's comparative advantage may lie more in those enabling layers than in trying to mimic the full sovereign space architectures of larger states.

This is also one of the few areas where New Zealand can plausibly align national security needs with economic and innovation policy. The space strategy already links sovereign capability, sector development, talent growth and application of aerospace technologies to national challenges. A sharper defence and national-security demand signal could strengthen that ecosystem further.

Intelligence

Intelligence is another area where a small state can gain disproportionate return from well-directed investment. The Defence Capability Plan explicitly includes improved intelligence functions and links them to more effective use of platforms, better targeting, faster response and easier sharing with other agencies. That is a practical recognition that intelligence is one of the main ways scarce capability is focused rather than dispersed.

For New Zealand, the case for stronger intelligence capability rests on several factors. The first is efficiency. Better intelligence raises the value of existing assets by helping direct them more precisely. The second is strategic warning. A more contested region and more complex global environment

increase the need for timely understanding, not just reaction. The third is national integration. Intelligence contributes across diplomatic, military, economic and informational dimensions of statecraft, and increasingly needs to support wider government and not just traditional defence consumers. The fourth is coalition relevance. A smaller partner strengthens its value when it contributes trusted insight, niche analytic depth and usable situational awareness.

Within this, open-source intelligence has particular significance. Official material from the intelligence community now acknowledges the role of open-source intelligence across intelligence activity. For New Zealand, that is important not only because open sources have become richer and faster-moving, but because they offer scale that a smaller system can use intelligently if it has the right tools and workforce.

That is where artificial intelligence becomes operationally relevant. The strongest case for AI in intelligence is not rhetorical futurism. It is productivity. AI-enabled tools can help with discovery, translation, triage, entity extraction, pattern identification, summarisation and prioritisation across volumes of public and mixed-source information that would otherwise overwhelm human analysts. Human judgement remains central to interpretation, contextualisation and decision support. The gain comes from using machines to expand reach and speed while reserving analytic responsibility to people.

For New Zealand, this is essential because the country is unlikely to win through scale in intelligence. It can still improve dramatically through smarter use of open sources, better tooling, better analyst support and tighter integration between intelligence, operations and decision-makers. That would also align with the wider emphasis in the Defence Capability Plan on information-domain capability and more effective decision-making.

The policy challenge is therefore whether current workforce, procurement, digital and classification settings allow intelligence functions to adapt at the pace they now need to.

Domestic innovation and defence industry

The third area is selected domestic innovation. New Zealand's defence discussion has often treated local industry as a secondary issue – useful where available, but peripheral to the main business of buying proven overseas capability. That mindset is becoming less adequate in a world where resilience, sustainment, supply assurance, software adaptation and niche technical advantage are growing in importance.

The Defence Capability Plan states that industry is a critical partner in the supply, sustainment and operation of military capability. It says implementation of the plan requires partnership with industry to deliver capability faster and with resilience, and it points explicitly to harnessing and enabling industry innovation and technologies. The Defence Industry Strategy reinforces that direction, presenting industry engagement as part of faster, more resilient capability delivery.

That opens the door to a more mature defence-industrial approach. The question is not whether New Zealand should try to produce everything domestically. It should not. The question is where domestic firms can make the system stronger.

There are several plausible categories. One is dual-use digital technology, where smaller local firms may be able to move faster than large incumbents and provide tailored solutions in data, analytics, software integration, autonomy support or information management. Another is sustainment and specialist support, where domestic capability can reduce dependence, improve responsiveness and strengthen operational resilience. A third is niche hardware and sensing technologies in areas where

New Zealand firms already possess export potential or close fit with national operating conditions. A fourth is space-linked services and ground infrastructure, where economic growth and national-security value may overlap more directly than in many other sectors.

A sensible national approach would therefore be selective and criteria-based. The government should back domestic innovation where it contributes at least one of the following – greater resilience, faster adaptation, sovereign sustainment, niche export advantage, improved interoperability or stronger bargaining position with larger suppliers and partners. That would place industry policy on firmer ground than generic patriotism. Domestic support should follow strategic logic.

The same applies to the workforce. Backing home-grown capability is not only about companies. It is also about retaining engineers, analysts, software specialists and technical founders whose work may otherwise be absorbed offshore. In fields such as space, digital, autonomy and information systems, the loss of talent is often as strategically significant as the loss of firms. A clearer defence and national-security demand signal can therefore help anchor a wider innovation base inside New Zealand.

A sharper model of sovereignty

Across all three areas, the central issue is sovereignty understood properly. Sovereignty does not require self-sufficiency. New Zealand will remain deeply reliant on alliances, partnerships and international technology ecosystems. Nor does sovereignty mean performing strategic autonomy theatrically. For a country like New Zealand, sovereignty is better understood as the ability to make meaningful choices, retain assured access in critical functions, sustain key capabilities and contribute enough value that dependence remains reciprocal rather than passive. That is the kind of sovereignty space, intelligence and selected domestic innovation can strengthen.

Each offers a way for New Zealand to contribute more than symbolic effort. Each can improve national resilience while also increasing value to partners. Each fits the broader shift in contemporary defence away from pure mass and toward connected, information-enabled, technologically adaptive capability.

The practical implication is that New Zealand should use the current defence uplift to define a smaller number of areas where the country will aim to be genuinely strong rather than broadly present. Space, intelligence and selected domestic innovation meet that test better than many alternatives.

Recommendations

New Zealand now has the strategic rationale, the high-level policy framework and the beginnings of a fiscal commitment to rebuild defence capability. The next step is to convert that intent into a more disciplined programme of institutional reform and focused investment. Six actions would materially improve the chances of that happening.

1. Conduct an independent review of defence capability policy settings

New Zealand should commission a short, independent, hard-edged review of the policy settings that shape how defence capability is currently defined, approved, acquired, integrated and sustained. The purpose of the review would not be to revisit the case for greater investment. That case has already been accepted in the 2025 Defence Capability Plan. The purpose would be to identify which current policy settings most directly slow the delivery of information-age capability.

That review should examine at least five areas – approval pathways, procurement rules, treatment of software and digital systems, workforce flexibility for technical specialists and information-sharing settings across agencies and with trusted partners. It should also distinguish clearly between capability

categories. A system designed primarily around long-cycle platform acquisition should not automatically govern software-heavy, data-driven and rapidly evolving capabilities in exactly the same way.

This review should be practical rather than academic. It should have very clear terms of reference which identify specific rules, thresholds and institutional habits that are slowing delivery, and recommend changes that preserve accountability while allowing for more modular, iterative and technically current acquisition models.

In addition to being mandated to deliver clear deliverables, the independent review must be bound by very focused timelines, i.e., a total of 90 days to execute – 30 days to review, 30 days to report and 30 days to implement appropriate strategic changes to current policy settings.

The most critical factor for the success of such a review will be the selection of the review board and leadership. If New Zealand is to be serious about its security interests through a defence lens, then finding the best individuals will be key. The requirement is to recruit and employ the very best, not the status quo.

In order to ensure that the findings and recommendations of such a review land in a timely and effective manner with the right policy and decision-maker, there will need to be very clear reporting lines. Given the strategic nature of the review and the potential strategic opportunities that might be on offer, this review should report to the cabinet table and not be bound by one ministerial portfolio or one chief executive.

2. Create an accelerated information-capability pathway inside the Defence Capability Plan

The Defence Capability Plan already includes substantial lines of effort in the information domain – improved intelligence functions, updating classified digital services, digital modernisation, information management and space capabilities. Those areas should now be treated as a coherent acceleration pathway rather than as loosely related projects sitting beside one another.

The immediate objective should be to connect these efforts more deliberately around operational effect. That means designing them as parts of one information-capability agenda with common governance, clearer sequencing and explicit emphasis on interoperability, secure sharing, decision support and workforce development.

This is not an argument for reducing attention to ships, aircraft or combat systems. It is an argument for treating the information layer that enables those systems as a first-order priority in its own right. New Zealand should therefore publish, within the framework of the next Defence Capability Plan refresh, a more explicit account of how information-domain investments combine to improve military utility and wider national-security responsiveness.

3. Define a sovereign space-security pathway

New Zealand's wider space strategy already commits the government to developing sovereign space capabilities, supporting local technologies and applying space-based data to national outcomes. The Defence Capability Plan also recognises space as a critical operational domain and a domain of competition. What is still missing is a clearly defined pathway that links those strands together for national-security purposes.

The government should therefore produce a dedicated sovereign space-security pathway within the next 12 months. That pathway should set out which space-related functions New Zealand should seek to assure more directly over the next decade. Those functions may include domestic ground

infrastructure, greater resilience in access to partner-enabled services, space domain awareness contribution, hosted payload options, data exploitation capability and selected dual-use support for maritime awareness, disaster response and Pacific resilience. This would sharpen priorities, reduce drift and help connect defence demand, wider national-security needs and domestic industry development.

4. Build a targeted national intelligence uplift with strong open-source and AI support

New Zealand should strengthen intelligence capability in a way that reflects the realities of a smaller state and the scale of contemporary information flows. The most useful near-term gains are likely to come from better open-source exploitation, better tooling, stronger workforce development and improved integration between intelligence functions and operational or policy consumers. Official material already acknowledges the role of open-source intelligence, and the Defence Capability Plan has already identified improved intelligence functions as a specific investment area. That should now be pursued more deliberately.

A targeted national intelligence uplift should include AI-enabled support tools for discovery, triage, translation and analytic prioritisation, alongside clearer pathways for recruiting and retaining analysts, engineers and technical specialists. It should also include stronger links between intelligence, information management and digital modernisation, so that intelligence is not treated as a separate specialist function disconnected from wider information-age capability.

For New Zealand, the gain here comes from improved productivity, faster warning, stronger focus and more useful contribution across the national-security system. That is a high-return area for investment.

5. Establish a strategic pathway for selected domestic defence and dual-use innovation

The Defence Capability Plan and Defence Industry Strategy both point toward stronger partnership with industry and faster delivery of capability with resilience. New Zealand should build on that by defining a more explicit strategic pathway for domestic firms in selected categories where local capability offers clear national benefit.

That pathway should be selective. It should not try to create a comprehensive domestic defence-industrial base. It should identify a narrower set of areas where New Zealand firms can add genuine value through resilience, sustainment, niche technical advantage, dual-use innovation or improved responsiveness. Software integration, information systems, selected sensing technologies, space-linked services and specialised sustainment functions are all plausible candidates.

The government should also use this pathway to help retain technical talent within New Zealand. A clearer demand signal from Defence and wider national-security agencies would strengthen the domestic innovation ecosystem and reduce the risk that promising firms and specialists are pulled offshore before they can contribute materially at home.

6. Improve public reporting on defence modernisation

New Zealand's National Security Strategy calls for more open engagement with the public on national security and argues that a more informed society is a more resilient society. That principle should be applied more concretely to defence modernisation.

The government, through the NZDF and MoD, should therefore publish a short annual public report on defence modernisation progress. The report should not disclose sensitive operational details. It should explain, in accessible terms, what has been committed, what has been delivered, how efficient

and effective the acquisition process has been, what lessons have been identified and what changes have been directed as a result of that learning, where major delays or trade-offs sit and how investment is improving readiness, resilience, interoperability and information-age capability, and most of all what strategic risks are being carried (and by whom) as the modernisation programme moves forward.

The annual report on defence modernisation progress should then be provided with an appropriate level of independent oversight with the aim of not only validating the report but also offering a level of transparent reporting which will serve to strengthen democratic legitimacy, sharpen delivery discipline and help move public debate beyond occasional bursts of interest around major platform announcements.

Pulling the recommendations together

Taken together, these recommendations are designed to do three things. First, they would improve the speed and coherence with which New Zealand turns funding into capability. Second, they would place greater strategic weight on areas where a small state can generate disproportionate return. Third, they would connect defence modernisation more clearly to the wider national-security, innovation and resilience agenda already visible in current government strategy.

That combination is the central policy requirement of the current moment. New Zealand does not lack official recognition that the world has become more dangerous. It does not lack a defence capability plan. It does not lack a national-security strategy, a data strategy or a space strategy. The challenge now is execution – stronger prioritisation, faster institutional adaptation and a more deliberate focus on the forms of capability that will matter most over the next decade.

Conclusion

New Zealand has reached a more serious moment in defence and national-security policy. The strategic environment has deteriorated. Official policy now says so clearly. The Government has also begun to respond with a materially larger funding commitment through the 2025 Defence Capability Plan and with a broader policy architecture that includes the National Security Strategy, the Defence Policy and Strategy Statement, the Government Data Strategy and Roadmap, the Space and Advanced Aviation Strategy and the Defence Industry Strategy. The country therefore enters the next phase with stronger policy foundations than it had even a few years ago. That should change the focus of the public debate.

The central question is no longer whether New Zealand should take defence and national security more seriously. It already is. The harder question is whether New Zealand will modernise in a way that matches the character of the challenge it now faces.

That challenge is shaped by speed, complexity and interdependence. It sits across military, technological, economic and informational domains. It places greater value on intelligence, digital resilience, secure communications, space-enabled systems, data integration and trusted interoperability. It also rewards institutions that can adapt quickly and punishes those that remain slow, fragmented or too tied to the habits of an earlier era. The Defence Capability Plan itself reflects this shift in its emphasis on the information domain, improved intelligence functions, digital modernisation, information management and space capabilities.

For New Zealand, that has a clear policy implication. Modernisation should not be understood simply as the replacement of ageing platforms. It should be understood as the redesign of the wider system

that turns investment into useful capability. That system includes policy settings, approval models, workforce design, digital architecture, industrial relationships and public accountability. Unless those conditions improve, new money will still produce gains, but more slowly and less coherently than the strategic environment now demands.

New Zealand's size makes this more urgent, not less. Larger states can often carry more inefficiency, duplication and delay. New Zealand cannot. A smaller state depends more heavily on clarity of purpose, sharper prioritisation and the intelligent combination of modest resources. Its defence and national-security system has less margin for institutional drag. That is one reason the country should place greater weight on areas where it can create disproportionate value – intelligence, information-age capability, selected domestic innovation and a more deliberate space-security pathway.

The historical warning that frames this paper therefore remains relevant. The danger is not simply underinvestment. The danger is late adaptation. A country that recognises the need for change but modernises too slowly still pays the cost of strategic delay.

New Zealand now has an opportunity to avoid that pattern. It has more money on the table. It has official recognition of a harder world. It has emerging policy frameworks in the right broad areas. The task now is to turn those foundations into a defence and national-security system that is faster, more integrated and more credible in the information age. That should be the standard by which this moment is judged.

Research Note
ISSN 2816-0347