MANATŪ KAUPAPA WAONGA
NEW ZEALAND
MINISTRY OF DEFENCE

HOW TECHNOLOGY INNOVATIONS ARE LIKELY TO INFLUENCE NEW ZEALAND'S DEFENCE CAPABILITIES BEYOND 2035

FEBRUARY 2026

Te Kāwanatanga o Aotearoa
New Zealand Government

defence.govt.nz

Acknowledgements

The New Zealand Ministry of Defence acknowledges all those who provided their insight and expertise in response to our consultation on the proposed topic and draft briefing. We acknowledge the external experts, Ministry staff, and other government agencies in the development of this briefing.

Finally, we thank all those from the New Zealand Defence Force that supported this briefing with their insights and expertise. In particular, the Defence Science and Technology unit for their patience, guidance, and deep technical expertise throughout the development process.

Note on the use of Artificial Intelligence (AI)

Some of the content in this document was developed with the assistance of the Microsoft AI tool Copilot Chat. Copilot Chat was used for the development of icons, drafting and summarising text, and editing of some sections of this document.

The authors have reviewed and verified all factual content and references to ensure accuracy and uphold quality standards. For any queries about the use of Copilot Chat in this document, please contact engage@defence.govt.nz.

Photographs

Photographs have been provided by the New Zealand Defence Force.

ISBN: 978-0-473-77269-7 (Paperback)

ISBN: 978-0-473-77268-0 (PDF)

This Briefing is presented to the New Zealand House of Parliament pursuant to section 8, schedule 6 of the Public Service Act 2020.

Published by the New Zealand Ministry of Defence, February 2026.

Table of Contents

EXECUTIVE SUMMARY

The convergence of several technologies is transforming how societies and economies operate. The convergence of advances in automation, artificial intelligence/machine learning (AI/ML), robotics, data analytics, and the Internet of Things (IoT), among others, is revolutionising human productivity, connectivity, and decision-making.

This transformation is taking place in the military domain too. Accelerating technology advances are rapidly evolving the character of war in real-time, changing how defence forces organise and arm themselves. This technology driven change is also reshaping New Zealand's security threats.

The Government's Defence Capability Plan 2025 outlines major investments to deliver a combat-capable NZDF, with enhanced lethality and deterrent effect, and with the flexibility to both protect against and utilise new technologies.

Within this context, this Long-term Insights Briefing (LTIB) seeks to understand **how technology innovations are likely to influence New Zealand's defence capabilities beyond 2035.**

This briefing does not recommend what capabilities to purchase next. Rather, it seeks to contribute a grounded, technology-driven foresight that will support discussions about how defence forces can respond to Emerging Disruptive Technologies.

This briefing examines technology innovations most relevant to future defence forces, highlighting their potential impact on capabilities and illustrating possible application scenarios. It maps global trends relevant to New Zealand. Whether, or to what extent, New Zealand will adopt these innovations is not addressed.

What is a Long-term Insights Briefing?

The Ministry of Defence is required under the Public Service Act 2020 to produce a Long-term Insights Briefing (LTIB) every three years.

The briefings provide the public with information and impartial analysis about medium and long-term trends, risks, and opportunities that affect or may affect New Zealand and New Zealand society, including policy options for responding to these matters.

LTIBs are not government policy and are developed independently of Ministers. The subject matter of an LTIB is at the sole discretion of Chief Executives.

The briefing also begins to signpost some of the major challenges defence forces may face in responding to these technology changes.

This briefing extends beyond combat and warfighting functions, encompassing other critical defence tasks such as humanitarian assistance, search and rescue operations, and fisheries patrols — all of which stand to benefit from the technologies and capabilities discussed.

The findings of this LTIB have been organised around four central themes:

- The power of data.
- Human-machine teaming.
- Next-generation effectors.
- Expeditionary sustainment.

In this briefing

This briefing helps provide New Zealand's defence industry sector with an early indication of how technology may influence future investments and the areas of potential demand.

To conclude, the briefing identifies three major shifts which carry significant operational, policy, and system level implications for Defence[1] to consider:

- From human accountability by default, to human accountability by design.
- From software supporting hardware, to hardware supporting software.
- From public engagement, to public inclusion.

Through our analysis, engagements, and public consultation, several related topics emerged that are critically important when considering technology and New Zealand's defence capabilities, specifically:

- The future defence workforce.
- Supply chain resilience.
- New Zealand's defence industry.
- National resilience in a degrading strategic environment.

The LTIB could not comprehensively cover these issues, but they remain vital to New Zealand's security interests. Although some of the implications for these areas are highlighted throughout the LTIB, the need for further long-term research to deepen New Zealand's understanding of them will only grow in importance.

This briefing has been written for the public, while also providing some technical insight for the New Zealand defence system, including industry, to help shape future planning activity. This will help provide future New Zealand Governments with a technologically advanced, combat-capable force operating within a robust and ethical authorising framework.

[1] Collectively referred to as 'Defence', the Ministry of Defence and the New Zealand Defence Force are separate agencies that work together to ensure the New Zealand Government receives robust advice on defence and security matters, incorporating military and civilian perspectives.

1. Harnessing the power of data: C5ISRT technologies will elevate software as the core capability

Defence forces harness data through their Command, Control, Communications, Combat Systems, Cyber, Intelligence, Surveillance and Reconnaissance (ISR), and Targeting capabilities (C5ISRT). These systems form the 'brain' and 'nervous system' of defence forces and are critical for making informed decisions at pace and remaining combat-capable.

In the future, data will be collected and analysed at unprecedented speed, precision, and volume. Automated analysis and decision-making using complex data will become faster and more accurate.

Crucially, the quality of the software and algorithms underpinning C5ISRT capabilities will be a key determinant of military advantage.

Examples of how next-generation C5ISRT capabilities may be applied include:

In a nutshell

The future of C5ISRT is about turning more data into deeper knowledge, for maximum decision advantage, with the potential to revolutionise how defence forces operate.

- Multi-static radar networks illuminating stealth targets from one angle and observing them from another.
- Self-mending networks of drones that intuitively re-route and reform the network when compromised.
- Algorithms detecting unusual shipping behaviour to triage maritime patrol efforts across vast ocean areas.
- Hidden integrated sensor networks acting as persistent sentries, scanning the environment for real-time threat awareness around forward operating bases.
- Advanced algorithms fusing large, complex, and disparate information and transforming it into knowledge at machine speeds.

Modern C5ISRT technologies will be a non-negotiable for defence forces to remain combat-capable and interoperable with partners.

For future C5ISRT capabilities, this research indicates that innovations in Artificial Intelligence/Machine Learning (AI/ML), autonomous systems, advanced computing, communication, quantum, and sensor and network technologies, and the convergence of these, will strongly influence defence investments in:

IT Infrastructure

Computational power

Integrated communications

Intelligence & combat management systems

Next-generation sensing

People & training

2. Human-Machine Teaming: Defence forces will increasingly leverage operating models founded on Human-Machine Teaming

Human-Machine Teaming (HMT) is the collaborative interaction between humans and intelligent machines, to achieve military objectives. Technology advances will increasingly shift the role of humans from directly controlling defence systems, to managing and guiding them.

Machines will have the ability to act more autonomously, with the potential to take a greater role in the operation of defence systems and capabilities.

In a nutshell

HMT is a force multiplier for future defence forces. Machines will take on tasks they can do better than humans, freeing up personnel to focus on duties that only they can or should perform.

Examples of how next-generation HMT capabilities may be applied include:

- Autonomous navigation systems adjusting routes based on threats, environmental conditions, traffic, supplies, and mission objectives.
- Autonomous electronic warfare systems continuously scanning for electromagnetic threats.
- Robotic autonomous systems sharing data quickly and securely between themselves and crewed systems.
- Uncrewed systems operating faster and over larger distances.
- Algorithms detecting, classifying, and prioritising targets, shifting the human role to verification and authorisation.
- Robots conducting tasks that are difficult or impossible for humans (e.g. underwater hull searches in rough seas).

HMT is the most uncertain, encompassing, and ethically challenging technology theme considered in this LTIB. However, it also possesses significant potential. A focus on research and development will be essential to effectively and ethically leverage future HMT technology innovations within legal boundaries and New Zealand’s foreign and security policy.

For future HMT capabilities, this research indicates that the convergence of robotics, AI/ML, autonomous systems, and human factors integration technologies, will strongly influence defence investments in:

Research and Development

Attracting expertise

Robotic Autonomous Systems

3. Next-generation effectors: Technology innovations will widen the continuum of effectors available to defence forces

Effectors are the means of action that fulfil a military intent. Effectors can be kinetic (e.g. artillery) or non-kinetic (e.g. jamming of an adversary's digital systems). Technology innovations will expand the areas where conflict can occur, particularly in space, cyberspace, and the sub-threshold zone[2].

Next-generation effector capabilities will complement conventional capabilities, and in doing so will increasingly transcend the 'seams' that traditionally separate traditional military domains.

These developments will provide the future defence forces with an increased spectrum of proportionate military options, with greater range, speed, and precision than conventional methods. This is important for defence forces that may want to exert force or deter actions without using kinetic effects or escalating situations unnecessarily.

In a nutshell

A wider range of effectors will exist along the continuum between peace and war. These will complement, not replace, conventional capabilities.

Examples of how next-generation effectors may be applied include:

- Quantum-enabled computer network exploitation breaking military encryption.
- Cyber-electromagnetic capabilities disrupting communication networks and computer systems.
- Directed Energy Weapons disarming mine fields or disabling drone swarms from a distance.
- Electromagnetic railguns launching non-explosive projectiles at hypersonic speeds.
- Loitering munitions, manoeuvrable re-entry vehicles, and hypersonic missiles providing faster, long-range and more devastating strike regardless of geography.

Emerging weapon systems, such as directed energy and cyber-electromagnetic capabilities, will offer a graduated range of offensive and defensive options. When combined with sub-threshold effectors, these technological innovations will equip a future defence force with more flexible and graduated responses to threats.

For next-generation effector capabilities, advances in energetics, electromagnetics, autonomous systems, AI/ML, cyber, computing, quantum, and space technologies, will strongly influence defence investments in:

Offensive & defensive cyber

Information warfare

Space

Directed Energy

Sub-threshold effects

Test & development infrastructure

[2] Sub-threshold refers to activities or operations that fall below the level of armed conflict or conventional warfare yet still pose strategic challenges — such as cyber intrusions and disinformation campaigns.

4. Expeditionary Sustainment: Technology will assist, but not resolve, expeditionary sustainment challenges

In a nutshell

The wicked problem of supporting expeditionary defence forces will be assisted, but not solved, by technologies that enhance the agility, survivability, responsiveness, and efficiency of military sustainment functions.

Sustaining military operations is an extraordinarily complex logistical undertaking that is critical for successful operations. The task is especially testing for a relatively small defence force operating over large distances in austere and challenging environments.

Technology innovations will enable more dispersed and portable energy production, and increase the efficiency, speed, and protection of transport and distribution methods. In the future, force elements will become increasingly self-reliant and sustain their activities more independently of central supply provisions.

It will also deliver efficiencies and improve some logistics analysis and planning tasks, like resource optimisation and supply chain management.

Examples of next-generation sustainment capabilities may include:

- Portable energy production such as electrochemical fuel cells.
- High-density storage batteries enabling capabilities to persist longer and more independently.
- Additive manufacturing producing critical supplies and spare parts on site.
- Autonomous capabilities transporting cargo and supplies to and from contested areas.
- Predictive inventory management systems ordering and directing supplies ahead of time.
- Surgeons operating remotely on injured people in the field.

Despite many innovative use cases, technology will not change the fundamental physical challenges faced by expeditionary defence forces, namely, how to sustain complex, dangerous, time-critical, and resource intensive operations over extended distances, often in remote or austere environments.

For future expeditionary sustainment capabilities, innovations in energetics, propulsion, meta-materials, production methods, miniaturisation, quantum computing, AI/ML and autonomy, will strongly influence defence investments in:

Research & Development

Energetics

Advanced logistics management

Robotic Autonomous Systems

The way forward: Three shifts to consider

Adapting to these four technology themes will create significant change and is not without challenges, risks, and uncertainty for Defence. This research identified **three shifts** that carry operational, policy, and system level implications for defence systems.

All three shifts are positioned within a context where defence systems operate within legal boundaries, with appropriate human controls, and with political oversight:

***SHIFT ONE: From human accountability by default, to human accountability by design**:* When acquiring advanced military capabilities that leverage Emerging Disruptive Technologies (EDTs), human accountability, and adherence to domestic and international law, must be built into the system design.

SHIFT TWO: From software supporting hardware, to hardware supporting software: Military success will be increasingly defined, not by platforms and capabilities, but by the software that operates and connects them. The increasing importance of software carries implications for defence personnel, and for capability planning, acquisition, and management.

SHIFT THREE: From public engagement, to public inclusion: Public trust in defence forces is earned, not assumed. Ensuring Defence maintains public trust will remain essential, and possibly more challenging, in an environment defined by increased contestation and technological change. It will be important to ensure that long-standing democratic, legal, humanitarian and military conventions continue to apply.

INTRODUCTION

WHO WE ARE

The Ministry of Defence is the Government's lead civilian advisor on defence and is responsible for purchasing major capabilities used by the New Zealand Defence Force (NZDF) to enhance the security and national interests of New Zealand and its people.

Under the Defence Act 1990, the Ministry, headed by the Secretary of Defence, is a separate legal entity to the NZDF. To carry out our role, the Ministry:

- provides long-range assessments and advice (20-30 years) on New Zealand's defence interests and challenges,
- purchases major defence equipment for use by the NZDF as a defence capability,
- advises the Government on how the NZDF can meet current challenges (such as potential deployments) and possible future challenges,
- builds and maintains strong Defence relationships internationally, and
- advises on Defence's performance and effectiveness as a system.

What is a Long-term Insights Briefing?

The Ministry of Defence is required under the Public Service Act 2020 to produce a Long-term Insights Briefing (LTIB) every three years. The briefings provide the public with:

- Information about medium and long-term trends, and risks, and opportunities that affect or may affect New Zealand, and New Zealand society
- Information and impartial analysis, including policy options for responding to these matters.

LTIBs are not government policy and are developed independently of Ministers. The subject matter of an LTIB is the sole discretion of Chief Executives.

This LTIB answers the question **how technology innovations are likely to influence New Zealand's defence capabilities beyond 2035?**

STRATEGIC CONTEXT

Emerging technologies are reshaping New Zealand’s security context

The convergence of a number of technologies are actively transforming how societies and economies operate. Commonly referred to as Industry 4.0, the convergence of advances in automation, AI/ML, robotics, data analytics, and the Internet of Things, among others is revolutionising human productivity, connectivity, and decision-making.

This transformation is taking place in the military domain too. Developments in technology are rapidly evolving the character of war in real-time, changing how defence forces are organising and arming themselves, and altering New Zealand’s security threats.

The speed of decision making required on the battlefield is accelerating. The precision, range, and lethality of strike weapons is increasing too, while space capabilities present both a critical enabler and disabler for modern defence forces. Meanwhile, bio- technologies are set to enhance defence force personnel in entirely new ways, while simultaneously introducing novel risks from pathogens and other weapons.

Technology is enabling sub-threshold threats that sit beneath the threshold of armed conflict, such as information warfare, cyber, and electromagnetic attacks, and the spread of misinformation and disinformation is posing an increasing threat from both state and non-state actors.

The effect on New Zealand’s strategic context is profound. Our geographic isolation no longer shelters us from threats to the extent it once did as new forms and means of conflict diminish the protective value of physical distance and borders.

The deepening integration of civilian technologies is playing an increasingly decisive role in modern warfare and altering the balance of global power. As is the supply of certain materials critical for modern military capabilities and the global race to develop breakthroughs in revolutionary technologies such as quantum.

As a result, the international standards for defence capabilities are changing, putting the onus on defence forces to remain viable in future conflicts and interoperable with partners. New Zealand’s traditional partners are investing heavily in defence modernisation, while New Zealand’s recent Defence Capability Plan (DCP 25) included a focus on uncrewed technologies, exploring new technologies that will help with Intelligence Surveillance and Reconnaissance (ISR), and the adoption of new technologies earlier in their lifecycle.

New Zealand is facing its most challenging and dangerous strategic environment for decades

Recent geopolitical developments demonstrate the increasing and compounding nature of threats to our national security interests. These include Russia’s continuing illegal war against Ukraine and blatant disregard for international law, conflicts in the Middle East, and growing strategic competition in the wider Indo-Pacific.

The existing international rules-based order is increasingly being challenged by those who seek to undermine international rules or norms or reshape global orders in ways contrary to New Zealand’s values and interests.

Intensifying strategic competition is increasing global and regional tensions and is raising the prospect of military confrontation and conflict.

The Indo-Pacific is a primary geographical theatre for strategic competition, most visibly between China and the United States. China’s assertive pursuit of its strategic objectives is the principal driver for strategic competition in the Indo-Pacific, and it continues to use all of its tools of statecraft in ways that can challenge both international norms of behaviour and the security of other states. Of particular concern is the rapid and non-transparent growth of China’s military capability.

States within the Indo-Pacific and globally are responding to these pressures by increasingly investing in their own military and security capabilities with particular focus on the application of advanced technologies.

Climate change remains the primary security concern for Pacific Island countries - driving increasing and intensifying natural disasters.

Both climate change and growing strategic interest in the Pacific are layering on top of other regional security challenges, including vulnerability and exposure to natural hazards, transnational organised crime, illegal fishing, and maritime security threats.

While the future is always unknown, New Zealand's security outlook for the coming decades is likely to be fraught, challenging, and potentially dangerous.

BRIEFING SCOPE

The briefing presents research findings into **how technology innovations are likely to influence New Zealand's defence capabilities beyond 2035.**

Predicting the future is fraught

Forecasting how technologies will develop and their subsequent influence on defence capabilities is inherently speculative. Not least because some potentially revolutionary technologies are largely theoretical with uncertain timelines and outcomes for defence, such as the cutting-edge research in quantum science. There is also potential for a range of technology advances to converge with each other, for example biotechnology, robotics, and AI/ML may generate unforeseeable implications for future defence capabilities.

Even when expected technology advances are made, their influence on defence capabilities depend on a range of external factors including the wider geostrategic context, cost, acquisition, and adoption barriers, and the ever-evolving character of conflict.

"Prediction is very difficult, especially about the future." – Niels Bohr.

This briefing focusses on future defence capabilities, but does not make specific capability recommendations for New Zealand

Within this complexity, the analysis identifies technologies that are likely to influence the capabilities that may enter military service in New Zealand or elsewhere beyond 2035, and describes how these technologies are expected to influence those capabilities.

The report maps global trends that are relevant for New Zealand, but whether, and to what extent, New Zealand adopts any of these technology innovations is not addressed in this report.

Technology is a priority area in the Defence Capability Plan 2025 (DCP 25). DCP 25 has record levels of planned investment across a range of modern and emerging technologies over the next 10-15 years, including persistent surveillance, anti-drone systems, remotely piloted aerial systems, space capabilities, and information warfare, among others.

This briefing does not recommend what capabilities to purchase next. Rather, it seeks to contribute a grounded, technology-driven foresight to support discussions about how Defence can respond to the emerging disruptive technologies most likely to influence military capabilities. The insights gained through this research will help the Ministry develop more informed advice to Government regarding major defence capability procurements for New Zealand.

The briefing also begins to signpost some of the major challenges a future defence force may face in responding to these technology changes, and the big contextual shifts that carry policy, operational, or system-level implications for Defence.

The analysis includes both existing and new technologies

Many of the technologies contained within this briefing already exist or have existed for some time. The earliest computer was invented for defence application in the 1940s, but innovations in computing technology will continue to shape the world and national security in immeasurable ways. Innovation is about something new or improved (NZMBIE, 2019). As such, this briefing discusses innovations within technologies that will give rise to the next generation of defence capabilities.

While some technologies and capabilities already exist, New Zealand may not yet employ them, and as such, are considered technology innovations that are likely to influence New Zealand’s defence capabilities beyond 2035. Although 2035 may seem distant, the time it takes to procure and deliver capabilities means innovations that may exist now, or will likely exist soon, have also been assessed.

The briefing also includes technologies that are still to be proven or are not yet technically feasible to integrate into New Zealand’s military context, such as some quantum-enabled capabilities.

This briefing extends beyond combat and warfighting functions, encompassing other critical defence tasks such as humanitarian assistance, search and rescue operations, and fisheries patrols — all of which stand to benefit from the technologies and capabilities discussed.

A number of issues related to the core question were considered but deemed out of scope, including:

- Capabilities that other parts of the New Zealand Government may want or need to protect New Zealand’s interests.
- The NZDF’s current capabilities or detailed analysis of what the NZDF needs to do to adopt future technologies.
- How the New Zealand or international defence industry will deliver future capabilities, including the relationships and interface between Defence and industry.
- Defence supply chains.
- Geo-strategic considerations, except where necessary to understand or contextualise the capability innovations topic.
- Future Defence workforce, force design, or doctrine.

RESEARCH METHOD

With support from the NZDF’s Defence Science and Technology unit, this study employed a mixed-methods approach to identify and assess emerging technologies with the potential to influence the New Zealand’s future defence capabilities.

The analysis started with an assessment of technologies included in the European Defence Agency’s Emerging Disruptive Technology (EDT) Taxonomy. Each technology was assessed for its relevance to the future defence force and evaluated for maturity and potential impact using the Five-Eye-aligned Technology Readiness Level (TRL) maturity evaluation framework.

Further data was sourced from peer-reviewed journals, government and industry reports, expert interviews, and patent databases. Selection prioritised recent, credible, and militarily relevant sources. A range of expert interviews from across the defence system supplemented the assessments.

Public consultation helped shape the briefing

The Public Service Act 2020 required the Ministry to undertake public consultation on the LTIB topic.

The Ministry is grateful to all those that provided their feedback on the proposed topic and the draft briefing.

Public consultation helped inform the development of this briefing, the results of which are included in **Appendix One**.

Limitations include the rapid pace of technological change, restricted access to classified developments, and the inherent subjectivity of TRL evaluations. Despite these constraints, the study provides a robust foundation for identifying strategic technology opportunities for future capability development

This briefing summarises the technical findings discovered through this research, into a relevant and insightful format on an issue important to New Zealand's long-term future.

HOW TO READ THIS BRIEFING

This briefing is designed to signpost how technology innovations are likely to influence New Zealand's future defence capabilities. The LTIB has been written to be understood by the public, whilst also providing insights for the New Zealand defence system, including industry, to help shape future defence planning activity.

The findings have been organised around four technology themes:

- Harnessing the power of data.
- Human-Machine teaming.
- Next-generation effectors.
- Expeditionary sustainment.

Initially, the briefing was structured around each of New Zealand's core defence capabilities. However, it was quickly apparent that the increasingly integrated nature of future defence technologies meant the research needed to focus on connectivity and understand the macro-trends that transcend capability sets. This updated framing will allow Defence to think more cohesively across domains and helps to ensure the findings stay relevant, regardless of specific capability considerations.

Using the Glossary

This briefing includes a large number of technical and defence-specific phrases, words, and concepts.

A comprehensive glossary is included as **Appendix Three** to help guide the reader.

Each of the four chapters is introduced by a brief definition. Vignettes are provided throughout the discussion as examples of how a future defence force could plausibly operationalise some future technology innovations.

As you consider this briefing, it is important to keep in mind that what is signposted is ultimately about equipping a future defence force so that future New Zealand Governments have options to employ a combat-capable military within a robust, lawful and ethical authorising framework. Delivering an innovative combat-capable force, with strong adherence to domestic and international law, is what ultimately empowers the Government with options to use Defence capabilities to achieve national objective.

Icons to help navigate the reader

🔍 : Clarification

🗣 : Quote

🔭 : Possible future scenario

⚠ : Word of caution for a particular innovation

🌰 : Summarises an idea

HARNESSING THE POWER OF DATA: C5ISRT

WHAT IS C5ISRT

C5ISRT is a military acronym that stands for Command, Control, Communications, Combat Systems, Cyber, Intelligence, Surveillance and Reconnaissance (ISR), and Targeting. C5ISRT describes how defence forces use information and technology to see what's happening, make smart decisions, and act quickly and effectively in complex environments.

C5ISRT systems are the 'brain' and 'nervous system' of defence forces and are critical in providing the force with the ability to make informed decisions in a timely manner and to remain combat-capable in future conflicts.

In a nutshell

The future of C5ISRT is about turning more data into deeper knowledge, for maximum decision advantage, with the potential to revolutionise how defence forces operate.

DATA WILL BE COLLECTED AT UNPRECEDENTED SPEED, PRECISION, AND VOLUME

Advanced sensor technologies will revolutionise how surveillance and reconnaissance is undertaken

Advanced sensors are increasingly sensitive and are continually collecting more precise, comprehensive, and novel data. Multispectral/hyperspectral imaging, advanced radio frequency technologies, photonic technologies, bio-chemical sensors, and acoustic sensors will exponentially increase the amount of data available to future defence forces.

Sensors will likely be able to observe minute signals resulting from activity by platforms such as aircraft through to individual soldiers. Multi-static radar networks will illuminate targets from one angle and observe them from another, enhancing the ability to identify stealth platforms that are undetectable with today's technology.

For New Zealand, the most significant application of advanced sensors will likely be in maintaining awareness across an extensive maritime domain and area of interest. However, advanced sensors will impact all operating environments of the future defence force. Defence intelligence capabilities will be influenced by innovations in radio frequency sensors, including software defined radio systems, which will enable better collection of adversary communication. Next-generation sensor technology will enable greater miniaturisation of sensors, allowing them to be transported and deployed in a variety of ways such as micro-drones, for example. Such technologies will be useful across a range of functions, for example search and rescue teams will benefit from advanced sensor technologies during Humanitarian Assistance and Disaster Response (HADR) operations, such as detecting buried survivors after an earthquake or landslide.

The speed, precision, and volume of data collected by future sensors cannot be overstated and will likely have a transformational influence across all future C5ISRT capabilities.

Networks of sensors will monitor large areas for long periods of time

Many defence forces are tasked with significant surveillance and reconnaissance responsibilities and are often required to understand what is happening across expansive geographical areas. For example, New Zealand has interests in its maritime surrounds covering 1/12th of the Earth's surface [3], providing trade, travel, and undersea communication links to the rest of the world. Because efficient monitoring of threats and illegal maritime activity are fundamental for underpinning national and economic security, leveraging technology innovations is essential for future defence forces to reach new levels of domain awareness.

[3] New Zealand Ministry of Transport, 2024

> *“The Pacific Ocean is so vast you could sink the entire European continent into it 20 times over. We are big ocean states with big airspace, and in the future, it will be about who dominates these spaces – in technology, commerce and security”*
> – James Marape, Prime Minister of Papua New Guinea, 2025.

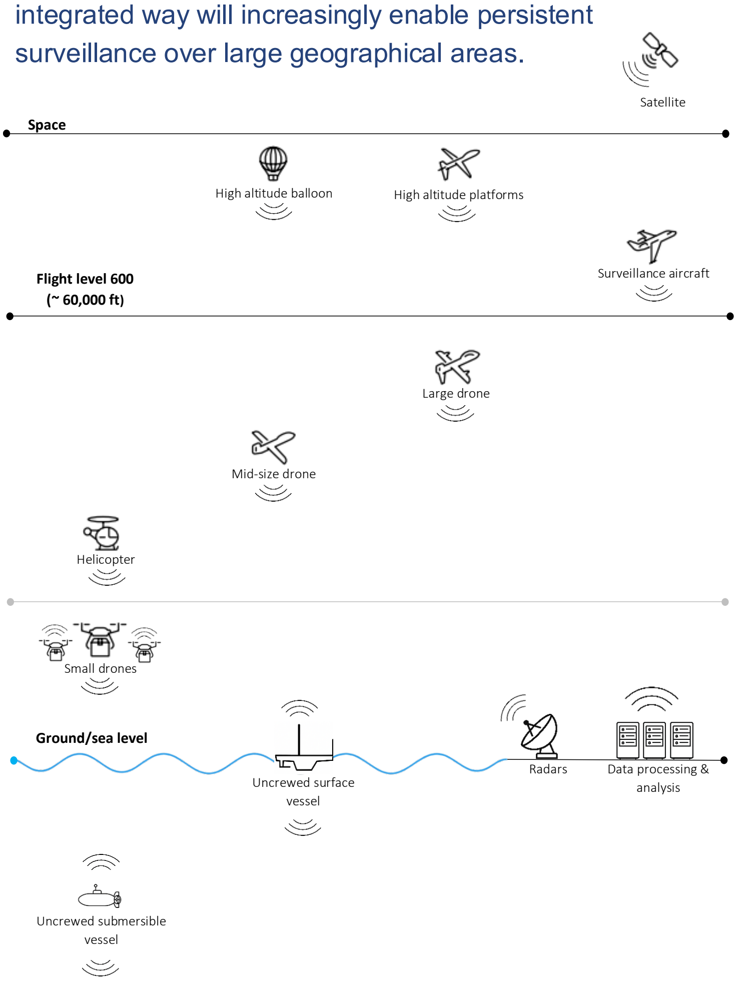
More advanced sensor platforms developed in integrated networks will provide the potential for comprehensive, coordinated, and persistent understanding of such areas - drastically enhancing the effectiveness and efficiency of currently resource intensive tasks.

Currently, sensor technologies are being paired with developments in uncrewed, optionally crewed, and autonomous technology enabling sensor carrying platforms to operate and persist in austere environments for longer periods. Innovations in high-density energy storage and propulsion technology will allow these sensor platforms to travel further, faster, and endure longer. Systems will operate under sea, on the surface, or in the air, complementing stationary land-based and aerostat radars to create comprehensive networked systems.

Increasingly affordable rapid-launch small-satellites will also provide the future defence forces with new opportunities to complement sea, air, and land-based sensors with space-based alternatives. Leveraging New Zealand’s significant space launch experience and expertise could greatly support future ISR networks of this nature.

Persistent Surveillance

Many ISR-enabled capabilities operating together in an integrated way will increasingly enable persistent surveillance over large geographical areas.



Systems will be more adaptive, automated, and networked

Effectively organising disparate sensor systems into integrated networks will be critical for ensuring their efficiency, resilience, and impact. Next-generation network and communications technologies will deliver advances in these areas. Developments in network technology, among others, will allow integrated networks of sensor-carrying drones to intuitively adapt and self-mend by re-routing and reforming the network when required. This will be possible without human intervention and with the ability to occur at machine speeds.

Advances in system integration will enable data collection from a variety of means to be fully integrated with other collection points and systems, including other government agencies and partners, to create a more comprehensive understanding of the environment and battlespace.

Possible scenario: Expeditionary patrol

Networks of Robotic Autonomous Systems (RAS) create an expeditionary patrol capability across a maritime area.

The network is supported by recoverable floating or submersible ‘docking stations’ that recharge and transmit information throughout the integrated network. These RAS systems and docking stations support an enhanced persistent ISR mission. This knowledge can then be used for tailored and proportionate maritime interdiction responses.

C5ISRT systems will become increasingly autonomous and adaptive, responding quickly to changes in real-time. Already, integrated and persistent sensor networks are being utilised by the Ukrainian military for air defence. By linking thousands of low-cost acoustic sensors across 80% of Ukrainian territory and utilising AI/ML to sort the data to cue air defence radar, Ukraine has increased its detection rate of incoming Russian drones and missiles to 98%. This is up 22% compared to its previous systems (CSIS, 2025).

Predictions will be progressively used to inform decisions

AI tools are increasingly able to recognise and learn from patterns in data and detect anomalies to predict and create extrapolations of future scenarios for subsequent analysis by human analysts. Although this capability has existed for many years, rapid innovations in AI/ML and computational power will transform the reliability and accuracy of data-driven forecasting. Innovations in predictive analytics will provide future defence forces with the ability to increasingly detect and monitor more threats, changes in environment, or shifts in behaviour, to exploit more opportunities in near real-time, even in ‘noisy’ data environments.

Maritime patrol capabilities could use greater analysis of shipping data to detect unusual behaviour, such as unscheduled vessel stops, or identifying suspicious behaviour, activities, and associated locations. Future targeting decisions could be informed through machine learning of real-time battlefield dynamics, or predictions about adversaries’ response to certain scenarios.

Possible scenario: Supply and sustainment

A logistics function can harness data on consumption rates of materials and fuel in real-time. When combined with soldier fatigue and capability loss, logistics officers can better predict what will be required to sustain an expeditionary force and adapt accordingly.

Communications will be rapid

Fully realising the transformational potential of C5ISRT systems will require defence forces to be fully networked internally, with all parts of the organisation communicating as a cohesive whole. Technology innovations in communications systems and integrated systems technology will help provide defence forces with new opportunities to be fully integrated vertically through the chain of command as well as horizontally across domains.

Enhanced computing and communications infrastructures will quickly process and transport the information needed for fast decision making. Photonic computing technology, for example, uses light instead of electrons (via traditional copper wiring and printed circuit boards) to transmit information, providing faster and more secure defence communications systems. Such technologies will allow large amounts of data to be transmitted throughout a network at speeds a fraction of the time previously needed.

Systems will need to be secure

The secure transfer of information will be critical to enabling future C5ISRT functions and staying connected with partner defence forces. Cybersecurity innovations in areas such as photonics, secure computing methods, encryption, and quantum sciences will be needed to strengthen network resilience and to protect sensitive information. These will offer digital communication tools that are high-speed, secure, and more challenging to detect, intercept, jam, or exploit.

Adversaries will almost certainly make use of cutting-edge offensive and defensive quantum computing techniques. To counter this threat, defence forces need to be researching and adapting technologies such as photonic systems that enable quantum key distribution providing extremely secure encryption. Using technologies like these, future defence forces will be better prepared and protected from many methods to exploit computer networks or intercept military communications. The technical capability and capacity of future Communications Information Systems will be a critical enabler for future defence force effectiveness. These systems will be designed to process and manage vast volumes of diverse data types, while ensuring robust protection of classified information and adherence to custodianship responsibilities. This includes supporting the operational and tactical needs of deployed force elements.

TECHNOLOGY-DRIVEN INTEROPERABILITY

C5ISRT technologies can bind and connect people, organisations, and countries both in peacetime and in conflict. The growing pace and scale of defence innovation will mean that maintaining technological interoperability will become increasingly expected by allies, partners, other government agencies, and industry.

C5ISRT technology innovations will continue to open new opportunities to integrate defence systems with international partners. This will require defence forces to continue developing the required technical, operational, and policy infrastructure required. For New Zealand, this may include new policy infrastructure such as data sharing arrangements that are consistent with domestic policy and law.

Keeping pace with technology innovations will be critical to remaining interoperable and meeting future minimum standards for theatre entry. However, future defence forces will need to balance the benefits of interoperability with considerations around cost, sovereignty, legality, and social licence. For many defence forces, these trade-offs could be challenging to manage, particularly if partner positions begin to deviate from international norms, or where the cost of capabilities enabled by advanced technology becomes prohibitive.

In some cases, it may be beneficial to expand the concept of a networked defence force to include other government agencies. For instance, technology-driven data sharing has the potential to deliver significant national benefit by unlocking the power of integrating national security relevant data held across various government agencies.

For New Zealand, opportunities exist to harness the significant technology innovations occurring within industry, particularly in New Zealand’s technology sector. Options could include deepening existing relationships that provide greater workforce exchanges, developing commercial relationships that facilitate collaborative problem solving, or contractual partnerships that are open to greater innovation and the associated risks.

While many defence technologies promote and sometimes require a degree of civil-military integration, it will be important for future defence forces to hedge against the risks of over-relying on non-sovereign commercially-operated systems. The risk of losing access to space connections and services during conflict or losing appropriate sovereignty over data, or AI services, are two such examples.

Timing technology, in particular, is a critical capability that defence forces rely on to enable communications, computing, and navigation. The critical need for assured timing services in degraded environments may necessitate defence forces investing more into assured timing infrastructure, such as sovereign satellite or atomic clock systems.

Similarly, future defence forces will require assurance that commercial arrangements do not adversely affect the accountability and transparency of defence systems, especially for any autonomous and AI/ML-enabled effector systems. There is a risk that adopting technology creates an overdependency on foreign and/or commercial organisations, which could create vulnerabilities during times of conflict or decrease the transparency of how complex systems operate.

ANALYSES, ASSESSMENTS, AND DECISIONS DERIVED FROM COMPLEX DATA WILL BE INCREASINGLY AUTOMATED, FASTER, AND OF HIGHER QUALITY

Machines will do most data analysis automatically

Continuing developments in AI/ML, machine learning, and advanced computing will significantly improve the integration and analysis of data. AI/ML-enabled tools are increasingly interpreting data independently, alerting human analysts only when action or key decisions are needed, allowing humans to focus more on interpreting strategic meaning rather than cleaning, fusing, and analysing raw data.

These innovations in particular present transformative opportunities for smaller defence forces that lack the advantage of scale, enabling them to multiply their analytical capabilities.

> *"One French observation satellite produces over 1,000 high-resolution pictures every day, of which human analysts can only process 5% at most." -* International Institute of Strategic Studies, 2023.

The growing convergence of 'AI at the edge' and Internet of Things technologies are enabling real-time sensing, learning, understanding, decision-making, and acting at the point of collection. Over time, this convergence will improve speed, network resilience, data security, and bandwidth efficiency, while negating risks associated with centralised analysis (EPoSS, 2021). Hidden sensor networks placed around forward operating bases, for example, could act as persistent sentries, scanning the environment and providing real-time threat assessments to command elements.

Future C5ISRT systems will be powered by advanced software and algorithms

Maximising the value of data will depend in large part on the quality of the software. Software is the unifying capability that integrates sensors, command and control, weapon systems, and platforms through effective use of data.

> *"Western reliance on conventional military hardware (i.e., military platforms) which aggregates sensors and effectors to generate mass and military advantage alone is untenable in the medium and long term without a reorientation towards software-defined defence."* - International Institute of Strategic Studies, 2023.

Within software, algorithms direct what will happen, and when. Algorithms are often what dictates the effectiveness of the system. With autonomous capabilities set to play larger roles in future warfare, attaining algorithmic superiority may become the most decisive factor in complex large-scale conflicts.

Machines will help provide a more detailed intelligence picture

The potential for AI/ML to help process bulk data, such as analysing continuous streams of visual data and intercepted radio frequency signals, will enable intelligence analysts to deliver a wider, more detailed intelligence picture to decision makers.

AI/ML is increasingly able to quickly extract pertinent insights from large amounts of open-source data. For intelligence, applications could include, for example autonomous monitoring of open-source media to monitor shifts in population sentiment and enhance situational awareness. Future Humanitarian Aid, Disaster Relief and Stability and Support Operations will likely use such capabilities more often to target and develop their activities.

AI may also play a critical role in mitigating potential cognitive biases throughout the intelligence and operational planning cycles by helping analysts understand large amounts of complex information in ways previously inaccessible to them (David Stebbins et al, 2024). As they become increasingly powerful, emotionally intelligent AI capabilities will better interpret, understand and respond to the emotional behaviours of humans in real-time. This could fundamentally alter how influence and informational operations are undertaken and defended against.

Advances in AI-enabled human language technologies will enrich the ability of intelligence analysts to overcome language and cultural barriers to access greater insights. AI-enabled natural language processing for example is increasingly capable to translate spoken or written material, making it possible for analysts to access instant translations, irrespective of the language or medium. This is enabling live interpretation of intercepted communications, broadcasts, or online content. Future natural language processing tools will also analyse tone, urgency, stress, and emotional cues despite language or cultural barriers. Such capabilities will add value across the spectrum of defence tasks including disaster relief.

Developments in information and signal processing technologies will refine and expand intelligence collection, analysis, and production capabilities. Combined with advances in data fusion, speech, and natural language processing and cognitive systems, future defence forces will have access to information containing unprecedented insight, precision, and depth.

The war in Ukraine provides an illustrative example of how AI/ML can quickly integrate intelligence satellite and drone imagery with open-sourced social media content used for identifying and tracking Russian troop and equipment movements in near real-time (Bendett, 2023).

Possible scenario: Defence intelligence providing the full picture

An expeditionary peace and stability operation is being planned. A future army is trying to understand the context they will be operating in.

AI/ML-enabled systems intercept radio frequency, signals, and geospatial communications, some in a foreign language. Functioning at machine speed, the system identifies relevant insights for translation and inclusion in an intelligence report.

The report also combines a range of unique data points, the latest analysis of local social media sentiment, and satellite imagery of the area. All collected, analysed, and approved in real-time to provide analysts with unique insights on which to base decisions and tactics for the upcoming operation.

Possible scenario: Networked force undertaking HADR response

A future Navy vessel acts as a forward operating base in response to a cyclone in the Pacific coordinating air, land, and maritime capabilities.

Drones and satellites collect data on survivors and the areas most damaged. This is viewed and updated in real-time on visual maps for Commanders.

Air assets are kept abreast of the best locations for landing and for air dropping supplies, while littoral craft are directed to remote island beaches where survivors are gathering.

CHAPTER CONCLUSION

Innovations in AI/ML, autonomous systems, advanced computing, communication, quantum, sensor, and network technologies will revolutionise how the future defence forces use data, with opportunities to accelerate analysis, augment understanding, improve decision-making, and optimise operational effectiveness.

C5ISRT capabilities underwrite the ability for all other military capabilities to function properly. How defence forces integrate, maintain, and capitalise on these technologies will determine success in the future battlespace.

Modern C5ISRT technologies will be a non-negotiable for a defence force to remain combat-capable. Such capabilities are increasingly important to remain interoperable as partners acquire more developed C5ISRT capabilities, particularly for secure communications and intelligence sharing.

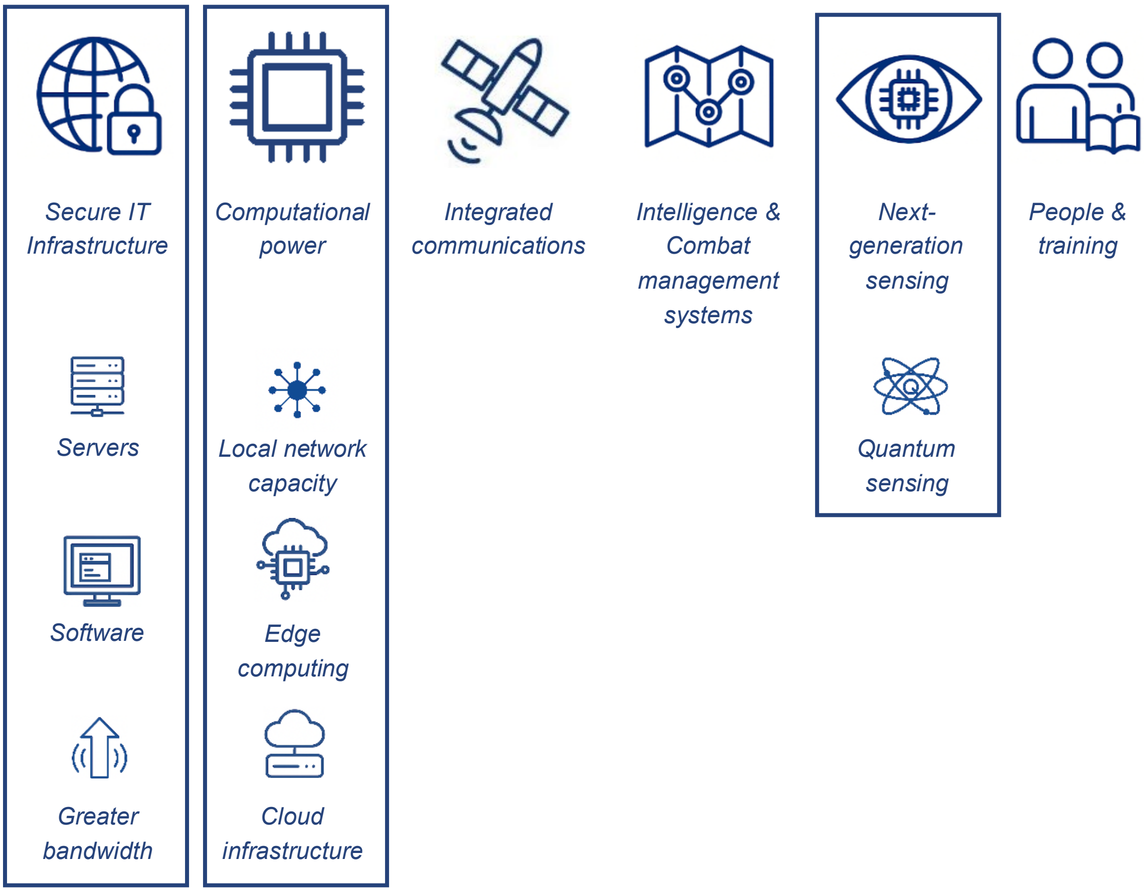
Fully harnessing the power of data through C5ISRT will require future defence forces to position software as its core capability– flipping the perception of software as an enabler of hardware, to one where software defines the capability. It will require a greater focus on leveraging data-power to achieve battlefield advantage.

A word of caution

Defence forces will likely face significant challenges developing next-generation C5ISRT capabilities. Most notably, incorporating new technology while maintaining legacy systems. Fiscal constraints, personnel, and doctrine may also pose challenges.

Additionally, careful consideration and management of legal and ethical issues around accountability and oversight will need to be considered, such as the need to ensure autonomous surveillance systems collect and process data legally.

This research indicates that innovations in AI/ML, autonomous systems, advanced computing, communication, quantum, sensor, and network technologies, and the convergence of these, will have a particular influence on defence investments in:



Secure IT Infrastructure

Servers

Software

Greater bandwidth

Computational power

Local network capacity

Edge computing

Cloud infrastructure

Integrated communications

Intelligence & Combat management systems

Next-generation sensing

Quantum sensing

People & training

HUMAN-MACHINE TEAMING

WHAT IS HUMAN-MACHINE TEAMING?

Human-Machine Teaming (HMT) refers to the collaborative interaction between human personnel and intelligent machines such as AI/ML systems, robots, drones, and decision aids, to achieve military objectives.

HMT is the most uncertain, encompassing, and ethically challenging technology theme considered in this LTIB. It also possesses significant potential. In complex operating environments where speed is a decisive factor, defence forces will need to leverage emerging HMT operating models to project force.

In a nutshell

HMT is a force multiplier for future defence forces. Machines will take on tasks they can do better than humans, freeing up personnel to focus on duties that only they can or should perform.

THE ROLE OF HUMANS WILL SHIFT FROM DIRECTLY CONTROLLING DEFENCE SYSTEMS, TO GUIDING AND MANAGING DEFENCE SYSTEMS

Although humans have interacted with machines for centuries, the extent of this interaction is always limited and defined by available technology. From using early computers to predict astronomical positions or mechanical clocks to measure time, to operating complex submarines and fighter jets to win wars, the human-machine relationship is constantly evolving.

Many defence functions have been automated for some time, such as auto-pilot capabilities in aircraft or close-in weapon systems on frigates which still require human authorisation. However, innovations in AI and ML, autonomous systems, and robotics are actively shaping the human-machine relationship in novel ways, where the role of humans will increasingly shift from directly controlling defence systems, to guiding them.

With machines poised to take on more tasks, human focus is increasingly likely to shift from manual tasks and tactical decision making to strategic oversight and guidance of systems. As a result, the future role of human oversight is likely to include functions such as:

- Ensuring that autonomous systems act within the law and ethical boundaries.
- Training and tuning automated systems.
- Adjusting system settings to ensure alignment with mission directives.
- Interpreting system outputs and validating ambiguous cases.
- Making decisive decisions that autonomous systems are not authorised to make.

The future role of human-machine teaming will rely critically on highly trained human operators to extract the ‘bigger-picture’ meaning from the machine-driven insights to make coherent strategic responses.

Possible Scenario:

Autonomous systems conduct persistent underwater surveillance

Future navies deploy fleets of small submersible drones that scan for acoustic signatures of adversarial military vessels, drug smugglers, and other illegal activity within defined areas. Acting autonomously, the fleets provide advanced warning of possible threats allowing humans to verify the information and act accordingly.

Harnessing the complex topography of the ocean floor, hidden docking stations and repair pens provide the fleet with sustainable energy and maintenance capabilities, ensuring they never resurface

Equipped only with the power to navigate and sense, these autonomous systems persist continually without round-the-clock human control and can be remotely piloted if required.

"Over time, defence functions have been shifting from human-centric to machine-assisted systems. For example, the US military force that went into Afghanistan after the 2001 attacks used zero robotic systems; now the force has over 22,000 in its inventory" - (Langford, 2025).

Machines will increasingly operate systems, processes and capabilities independently of humans

The defence application of autonomous systems will be ubiquitous worldwide, and used across a range of functions, such as:

- Platform navigation: Fully autonomous navigation systems dynamically adjusting routes based on threats, environmental conditions, traffic, supplies, and mission objectives.
- Electronic warfare (EW): Autonomous EW systems will continuously scan the electromagnetic spectrum to detect and respond to electromagnetic threats (e.g. radar tracking, jamming, cyber electronic attacks)

These advances will also lead to decisions increasingly being made independent of human analysis and inference, where it is lawful, and ethically and operationally sensible to do so. For example, a decision to lock down low-risk areas of a compromised IT network or an engine control system due to malicious cyber activity could be made by autonomous systems, with humans alerted accordingly. Additionally, a decision to monitor maritime vessels could be made by an autonomous system based on data collected, such as vessel type, flag, and Automatic Identification System signal. Decisions made by such systems will be fast and highly adaptive to changes in context, but will need to be weighted in accordance with approved ethical, legal, and operational frameworks.

A word of caution

As defence forces adapt to the demands of industry 4.0, eventually, the force will be unable to revert to analogue and mechanical methods of operating should core critical digital infrastructure fail.

It is important for Defence to understand and manage the risks associated with dependence on fully digitised systems.

HMT capabilities will be increasingly used to project force

A range of technology advances are expected to converge that will exponentially increase the role of uncrewed, or optionally crewed, military vehicles and vessels. In particular, the convergence of:

- AI/ML (especially AI at the edge) will allow for uncrewed systems to navigate, make decisions, and coordinate among platforms without human input.
- Advanced sensors and data fusion will improve the information available to uncrewed systems thereby enhancing operational effectiveness and 'technical autonomy', i.e., technologies that support resilient autonomous systems.

A word of caution

There is an emerging risk that future military systems using AI/ML-enabled autonomous technologies could escalate conflict situations faster, and with less human control, than current systems. This could result from the speed at which systems can react and how decisions are made, combined with exponentially more complex contexts where actions, and counteractions, occur simultaneously across many domains.

Capability development must therefore design systems that retain the ability for humans to stay in control and de-escalate conflict.

- Robotic Autonomous Systems (RAS) will share data quickly and securely between themselves and crewed systems. Furthermore, organic networks that self-heal and can build ad hoc networks, will also support ‘technical autonomy’.
- Continued breakthroughs in miniaturisation and high-density energy storage will support RAS capabilities to travel further for longer, such as lightweight solar cells powering high-altitude drones.

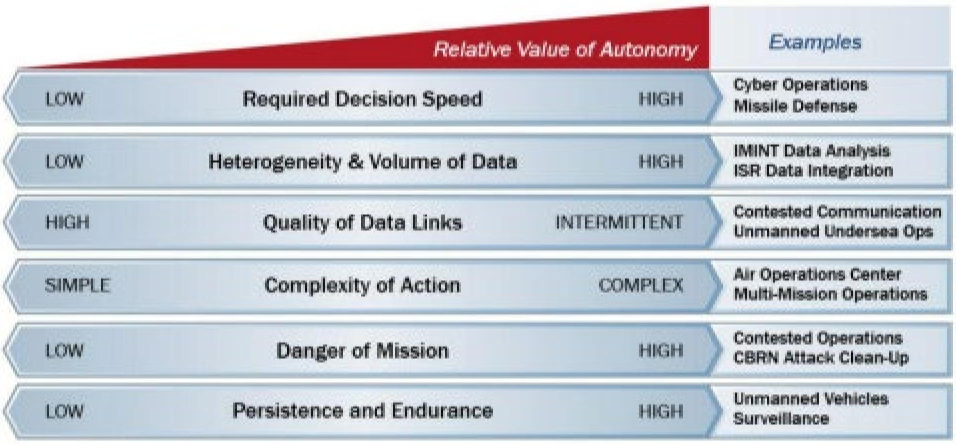
The integrated application of these technologies will produce the next-generation of uncrewed systems that will be fully networked, more resilient, and operate as independent or collaborative actors in complex environments.

> *“Depending on the task, autonomous systems are capable of augmenting or replacing humans, freeing them up for more complex and cognitively demanding work.”* – US Congressional Research Service, 2020.

Autonomous systems will enhance force projection

The rapid advancement of machine capabilities is transforming the nature of force projection, increasingly enabling aspects of operations to occur with greater autonomy. These capabilities span a spectrum from fully autonomous systems capable of identifying, selecting, and engaging targets independently, to those remotely operated by humans. The effectiveness and appropriateness of such systems depends on mission objectives, strategic and political considerations, legal frameworks, and rules of engagement. Crucially, compliance with domestic policy, international humanitarian law, and ethical standards is fundamental to ensuring the responsible and effective use of force, particularly when employing autonomous military technologies.

It is not expected that autonomous systems will herald a wholesale replacement of human presence on the ‘front-line’, however, these systems are likely to be used as complementary tools within an HMT paradigm. While the exact level of human involvement will adapt to the task, environment, and capability in question, the value of autonomous systems is proportionate to the speed, complexity, and danger of the operating context (Krause, 2021).



Relative Value of Autonomy			Examples
LOW	Required Decision Speed	HIGH	Cyber Operations Missile Defense
LOW	Heterogeneity & Volume of Data	HIGH	IMINT Data Analysis ISR Data Integration
HIGH	Quality of Data Links	INTERMITTENT	Contested Communication Unmanned Undersea Ops
SIMPLE	Complexity of Action	COMPLEX	Air Operations Center Multi-Mission Operations
LOW	Danger of Mission	HIGH	Contested Operations CBRN Attack Clean-Up
LOW	Persistence and Endurance	HIGH	Unmanned Vehicles Surveillance

Figure 1: Value of Autonomy to the Department of Defence Science Board

Source: Defence Science Board, “Summer Study on Autonomy”, 2016. As referenced in Sayler, 2020, p.28.

Some autonomous capabilities are well suited for use by New Zealand, for example, to project influence across New Zealand’s vast maritime domain. The ability to detect potential adversaries from a distance will significantly strengthen New Zealand’s deterrence posture

Advances in technologies, such as electric propulsion, aerodynamics, gas turbine, and novel engine designs, are also increasing the speed of uncrewed capabilities, in some cases to reach super-sonic speeds. This is especially the case for future drones and would allow a future defence force to respond to threats in its region faster, and with more stealth.

These use cases are already being considered by key international defence partners. For example, the United Kingdom’s latest strategic review fore-shadows a land force where “a 20-40-40 mix is likely to be necessary: 20% crewed platforms to control 40% ‘reusable’ platforms, and 40% ‘consumables’ such as rockets, shells, missiles and ‘one-way effector’ drones” (UK Strategic Review, 2025).

Possible scenario: Uncrewed systems respond to assertive maritime activity

It is suspected hostile actors may be asserting a maritime military presence and conducting activities that are against a nation’s interests.

Long-endurance Uncrewed Surface Vehicles (USVs) and drones are dispatched to exert presence, deter hostile actions, and collect real-time intelligence to confirm the nature of the activity.

The USVs and drones identify and confirm a hostile presence. A large USV dispatches a swarm of smaller aerial drones that surround the vessels to collect more detailed intelligence. The drones are clearly unarmed but assert a deterring presence.

Submersible drones are deployed to search for sea mines and other illegal installations in the ocean.

Meanwhile, a medium-size USV patrols and transmits warnings to the vessel in multiple languages.

A frigate remains some distance away maintaining command and control functions, and may project greater force if assessed as appropriate and proportionate.

This approach does not escalate the situation unnecessarily. It helps reduce the risk to human life, and high value capabilities, whilst still demonstrating resolve and proactively deterring hostile actions.

Machines will play an increasing role in targeting processes

Traditionally, human analysts manually identified and prioritised targets. Increasingly, algorithms will detect, classify, and prioritise targets at machine speeds, shifting the human role to verification and authorisation. Incorporating such evolutions into the decision-cycle could lead to decisive battlefield advantages, noting the ethical and legal complications of targeting decisions discussed later in this briefing.

> “*Robotics advances combined with AI/ML will create autonomous machines that can perform far more complex tasks, perhaps reasoning their way through a battlefield or a set of collection targets.”* - Centre for Strategic and International Studies, 2023.

Similar AI/ML tools are already being implemented by other militaries around the world, such as Project Maven in the US. This project is producing AI/ML tools which can collate data from various sources (e.g., satellite imagery, radar, CCTV, etc.) and identity enemy personnel, vehicles, and locations of interest, presenting them as targets for approval to a human operator. Although still under development, in 2024, the project was shown to increase the speed of target acquisition and approval by two to three times that of a human analyst alone (Manson, 2024).

A word of caution

Autonomous systems used for targeting will need to have accountability and transparency built into their design to ensure compliance with domestic and international humanitarian law.

TECHNOLOGY INNOVATIONS WILL IMPROVE HOW MACHINES SUPPORT HUMAN CAPABILITIES

Human Factors Integration is a field of research that ensures human needs, capabilities, and limitations are factored into the design of machines. This could include software interfaces which match how humans think to minimise overload and improve decision making, or physical ergonomics that design machines that integrate with human anatomy. This complements a related field, Human Information Processing, that is concerned with how machines can complement human sensory, perceptual, and cognitive processes.

Such fields will influence the future of how most defence capabilities are designed and used, like cockpits that integrate with the pilot physically and cognitively, for example. It will likely lead to new applications of augmented reality, physical, and cognitive monitors and enhancers, brain-machine interfaces, and AI/ML assistants.

Augmented reality will deliver tools that overlay real-time data onto the vision of defence personnel. Background data will be collected by AI/ML powered sensors that translate the data into information of relevance for specific personnel, such as interactive maps, or augmented vision that plots hostile and friendly positions. Tools like these will fulfil a range of functions for future defence forces, such as translating signage for personnel operating in a foreign country, providing warnings of chemical threats, or recognising and describing unknown objects in real-time.

Machines will also learn from their users and present information that considers their environment, stress levels, and preferences. This will be particularly evident in AI/ML assistants that will partner with humans in the long-term, providing them with advice, guidance, and information. For example, future AI/ML assistants will monitor a person’s heart rate, temperature, hydration, and fatigue levels.

This would be of particular use where defence personnel operate in demanding physical environments such as the Southern Ocean or tropical jungles.

Possible scenario:
Human-machine boarding team

A future Navy maritime patrol drone identifies a vessel suspected of illegal fishing. A crewed patrol vessel is dispatched with instructions to board the vessel.

A boarding team is supported by drones that travel ahead of boarding to map the deck and interior spaces of the vessel being boarded as well as crew positions and numbers.

With a real-time scan of the ship shown in their visors, the team can board with greater confidence and safety. At the same time, micro-drones deploy to enter hatches and monitor for dangerous chemicals, firearms, or concealed persons, providing real-time updates to each personnel.

The boarding crew are physically supported by machines that lift them to allow quick and safe boarding in rough open ocean.

Once on board, sensors worn on body armour supply the team with real-time information about the identities of crew members and AI tools translate audio to enable effective human-human communication.

Machines will increasingly complement and interact with humans in ways that suit human capabilities, such as being directed by voice command, gestures, or eye movement. Breakthroughs in biotechnology are gradually delivering brain-machine interfaces that detect brain activity to direct machines with thoughts. Innovations in such sensors could monitor for cognitive fatigue and initiate the automatic administering of nutrients to boost alertness, memory, or decision making.

Future defence forces will also have the option of enhancing its personnel’s sensory capacities, such as night vision contact lenses, adaptive camouflage, or integrated biosensors that can sense threats from distance.

> *"AI-enabled technology and autonomy certainly aren't going to replace [humans], but the [service] that augments them and the one that masters human-machine teaming is going to have a critical advantage going forward in warfare."* – Gen. David Allvin, US Air Force Chief of Staff, 2024. (Park, 2024).

Future robots will help do things humans find difficult

Robots will conduct tasks that are difficult or impossible for a human. Ranging in sizes, capabilities, and functions, these machines could conduct more tasks that are challenging or impossible for humans to perform such a navigating through pipes, squeezing into tight machinery to check for contraband, or performing underwater hull searches in rough seas, for example.

The physical capabilities of humans will also be enhanced through developments in capabilities such as exoskeletons. Exoskeletons are rigid external frames that people can 'wear' to greatly enhance strength, endurance, and durability, for example. The use cases for them are broad and could include supporting future special forces teams traveling long distances on foot with heavy equipment, or supporting loadmasters to hoist heavy machinery onto transport vehicles. Innovations in human augmentation capabilities are driven by advancements in a range of fields, including:

- High-density energy storage will deliver better and safer options for powering exoskeletons, wearable devices, or other human-machine interface technologies.
- Advanced materials that optimise weight bearing and movement.
- ML and biometric monitors to learn and predict operator activity.
- Neural integration that uses electrical signals from muscles or brainwaves to drive movement directly.

Machines will change training and mission preparation

Training will increasingly incorporate virtual and augmented reality, synthetic environments, and ML-driven simulation. Such training facilities will present fully immersive scenario-based training options currently not replicable. Through simulation, defence personnel will gain virtual experience of an operation and prepare for complex operating environments, such providing disaster relief following a devastating earthquake in a populated city.

Such training platforms will be able to adapt to each user's strengths and weaknesses, track performance, monitor physical and emotional stress levels, and provide AI/ML generated coaching (such as replaying footage and analysis). As the technology develops, the training environments will become increasingly flexible and tailored to the latest battlefield intelligence and capability developments.

Platforms and defence systems will be more robust and resilient

Machines will monitor and assess other machines to ensure they are able to perform optimally. For example, software will test whether the navigation and communication systems within an aircraft are operating as they should. This will be done continuously and in real-time reducing the burden on people and improving the reliability and availability of capabilities.

Such systems will help predict potential failures and schedule maintenance activity, reducing repair times and improving readiness.

CHAPTER CONCLUSION

The convergence of AI/ML, robotics, and autonomous technologies seems increasingly likely to shift the role of humans from directly controlling defence systems, to guiding them. Machines, on the other hand, will act more autonomously as they take greater responsibility for operating defence systems and capabilities. Ultimately, humans and machines will be physically present where they are best suited, reducing the risk to personnel whilst maximising impact in the field.

HMT is the most uncertain, encompassing, and ethically challenging technology theme considered in this LTIB. It also possesses significant potential. In complex operating environments where speed is a decisive factor, defence forces will need to investigate how to best leverage emerging HMT operating models to project force.

HMT systems will accelerate the speed at which decisions are made and communicated throughout the force and enable greater specialisation between humans and machines. As a significant force multiplier, machines will take a larger share of low-risk decisions, freeing up defence personnel to specialise in more human-specific tasks.

The HMT transition could therefore transform force projection, allowing human operators to be increasingly situated further from front-line engagement. For the future workforce, this shift will demand skills in machine learning literacy, strategic reasoning, and (rapid) ethical and legal decision-making.

Defence forces will therefore need a deep understanding of the legal, ethical, technical, and operational implications of integrating and leveraging HMT innovations. This will require expertise, research, and development.

This research indicates that the convergence of AI/ML, robotics, autonomous systems, and human integration technologies will have a particular influence on defence HMT investments in:

Research and Development

Attracting expertise

Robotic Autonomous Systems

NEXT-GENERATION EFFECTORS

WHAT ARE EFFECTORS?

Effectors are the means of action that fulfil an operational intent. Effectors can be kinetic (e.g. artillery), or non-kinetic (e.g. electromagnetic jamming of adversary's digital systems). Effectors can be used for offensive or defensive purposes.

Emerging effectors will expand the places where conflict occurs and are being increasingly applied to new conflict areas like space, cyberspace, and the information environment. Advanced effector capabilities will be utilised by both state and non-state actors and will increasingly transcend the 'seams' that traditionally separate traditional military domains.

In a nutshell

A wider range of effectors will exist along the continuum between peace and war. These will complement, not replace, conventional capabilities.

NEW EFFECTORS WILL EXPAND THE PLACES WHERE CONFLICT OCCURS AND TRANSCEND THE BOUNDARIES THAT TRADITIONALLY SEPARATE DOMAINS

Traditional domains are being transcended

For much of the last century, militaries were primarily structured around the maritime, land, and air domains and the corresponding services of the Navy, Army and Airforce. While domains are still very relevant to modern defence forces, emerging technology and the associated changes in warfare are increasingly integrating the domains.

Earlier chapters discussed technology advances that elevate the importance of real-time data across domains and the role of technology in integrating command-and-control structures. One effect of these developments will be to further break down the delineation between domains, and elevate the use of cross-domain effects and integrated operations.

Technology is raising the importance of 'new' battlespaces

Technology has also given rise to three 'newer' areas of space domain, cyber domain, and information environment. The pervasiveness of these domains and environments means that they cannot be fully distinct from each other, or from traditional maritime, land, and air domains. For example, space capabilities provide critical communication infrastructure across all other domains, as does cyber. Similarly, information and electronic warfare is domain agnostic but may require 'all of domain' responses.

These newer areas should not be viewed as enablers, as space, cyber, and information can be decisive battlefields in their own right – as well as being integrated into all other domains.

Possible scenario: Achieving an effect using capabilities from multiple domains

An adversary platform is operating illegally within the territorial waters of another country. In response, that country has a range of effectors to deter the adversary, including:

- Space-based surveillance and information campaign to expose nefarious actions.
- Autonomous UAVs and USVs and underwater drones harass the approach of the vessel.
- Cyber intrusion to disable or delay adversary operations.
- Precision strike from air or sea capabilities.

Depending on the context, a mix of several capabilities could be engaged based on multi-domain intelligence and coordinated through integrated command and control.

Space domain awareness is essential to protect critical services like navigation that depend on space connections. This will require continued investment in a network of ground-based space infrastructure, radar, and observational satellites, among others. Reusable launch systems, portable, or more dispersed launch sites, and more rapid smaller launch options could provide resilience to a space ecosystem critical to future defence forces.

Emerging technologies will also push military activity further into subsea and high-altitude areas. Developments in Unmanned Underwater Vehicle technology, automation, and energetics will expand the technological limits of the maritime domain to encompass more of the subsea environment. Because these environments are difficult to monitor, both state and non-state actors will increasingly target this area for military activity.

Greater reliance on deep sea infrastructure such as deep-sea mining, pipelines, and undersea cables have increased the need for greater surveillance of the subsea domain, and the ability to conduct and combat sub-threshold effects.

A word of caution

There is a risk that expensive capabilities and assets become 'stranded' or obsolete due to the pace of technology change. Additionally, the competitive acceleration of the 'development-counter-development' cycle encourages military innovation to accelerate, with the aim of retaining a competitive advantage.

Major capability investments should be assessed for their ability to withstand the pressures associated with an increasingly technologically advanced environment.

Developments in high-altitude technologies are increasingly expanding the aerospace domain. High-Altitude Platform Stations or High-Altitude Pseudo-Satellites (HAPS) come in the form of 'heavier than air' fixed wing autonomous aircraft and 'lighter than air' balloons and airships. These capabilities are quickly filling the physical gap between satellites and conventional aircraft and have the advantage of providing surveillance capabilities beneath the cloud layer. Innovation in HAPS capabilities will increasingly allow for persistent, low-cost surveillance and communications between space and the earth's surface, supplementing and supporting space-based, and ground-based space infrastructure.

NEW EFFECTOR SYSTEMS WILL DELIVER A GRADUATED SPECTRUM OF OFFENSIVE AND DEFENSIVE EFFECTS

Cyber-Electromagnetic technologies will provide non-escalatory defensive and offensive options

Developments in autonomous technologies, ML, advanced computing, and quantum-based technologies will drive accelerated developments in cyber-electromagnetic operations capabilities. Cyber capabilities, electronic warfare, and spectrum management can work together, individually, or in concert to degrade or exert force over adversaries in the cyber-electromagnetic spectrum. Future defence forces will need capabilities to protect, and assure access to, critical functions such as Position, Navigation, and Timing (PNT) systems that underpin advanced defence capabilities.

Manipulation of electromagnetic signals can be used to compromise or jam an adversary's communications or threat detection systems for example, while computer network exploitation methods enable adversaries to access or disrupt vital cyber systems.

Quantum computing technology will be used to circumvent security to access protected networks, increasing the difficulty to detect or protect against hacking. ML and advanced computing are enabling capabilities like autonomous malware which will learn in real-time and adjust their intrusion and exfiltration methods accordingly.

At a minimum, future defence forces need to continue modernising their capabilities to defend against cyber-electromagnetic attacks. Adversaries in future conflicts will employ cyber-electromagnetic capabilities to interrupt the operation of military capabilities. For example, by introducing malware into an enemy's systems, adversaries could disable combat management systems, or conduct 'spoofing' that sends incorrect GPS data into drone swarms.

New digital defence systems increase a defence force's vulnerability by expanding the number and diversity of potential targets. For example, an AI-enabled effector presents a significantly broader attack surface than traditional systems. This includes not only the effector itself, but also its associated components, such as AI training datasets, data pipelines, real-time information feeds, data centres, edge devices, and the algorithms that drive its functionality. Each element introduces unique security challenges.

Covert, ambiguous, or deniable sub-threshold activity will likely target future effectors and defence systems to manipulate, compromise, or destroy them in ways that are beneath the threshold of kinetic conflict. This threat extends to civilian and dual-use infrastructure, such as electricity grids. To protect a force's expanding digital attack surface, investment in enabling technologies like AI-driven self-healing systems, secure computing, and post-quantum cryptography must be considered integral to capability development, not separate from it.

Possible scenario:

Maritime patrol responds to threats without further escalation

A long-range maritime patrol drone is tasked with monitoring illegal naval militia in a disputed maritime region.

The drone monitors radar emissions and communications traffic to build an understanding of the adversary's electronic systems, such as information on the frequencies used and identifying unsecured communications.

The information is communicated back to command centres using frequency hopping that makes it undetectable and encrypted satellite communication systems.

To evade adversarial radar tracking, the drone deploys electronic countermeasures to spoof its location or direction.

This provides valuable intelligence for diplomatic and potential military action, but without the risk of escalation or loss of capabilities.

Defending against such threats will require AI-driven autonomous capabilities able to detect, analyse, and respond to threats instantly. Given the trajectory of quantum technology developments, future defence forces will require quantum resistant encryption across many communication vectors to protect against technologically advanced adversaries. Importantly, employing such defensive capabilities will allow defence forces to remain in contested areas for longer.

As well as defensive uses, future defence forces will have the opportunity to consider offensive cyber-electromagnetic capabilities to disrupt adversarial communication networks or computer systems. Ultimately, incorporating these emerging technologies into a nation's defence capabilities could provide the force with more graduated and proportionate response options to threats, particularly in the sub-threshold zone between war and peace.

A word of caution

Any use of offensive cyber capabilities must comply with international humanitarian law and be nested within appropriate legal authorising frameworks.

Innovations in energetics will provide more precise and proportionate options

The convergence of innovative high-density energy storage and Directed Energy Weapon (DEW) technologies will enable the production, storage, and transportation of concentrated energy far above current levels. Energy will enable the increasing use of future DEW systems, reducing reliance on traditional projectiles such as bullets and artillery, in some circumstances.

DEWs focus energy in the form of light beams (lasers) or powerful radio waves (radio frequency systems) to disable or destroy threats.

A word of caution

DEW systems are highly sensitive to shock damage, often require long-cool down and ramp up periods, and depend on specific environmental conditions to be effective. Although the technology is improving, they are unlikely to be as robust, cheap, or plentiful as traditional projectile systems for the foreseeable future.

Laser systems can burn through metal, blind sensors, or disable engines. They can be highly precise and will greatly minimise collateral damage. These capabilities provide the advantage of safer and reduced ammunition holdings, higher speed strikes, and lower cost-per-fire rate compared to explosive munitions like missiles. Technology advances will allow the production of mobile laser systems small enough to be mounted on land, sea, airborne, and space-based capabilities.

Radio frequency systems use powerful radio waves to attack, disrupt, or destroy electronics. Using high-powered radio frequencies can jam, scramble, or disable electronic circuits of adversary systems. Such weapons have the advantage of stealth as well as being cost effective and highly targeted.

DEWs could help defend against attacks or prevent certain adversary actions, without escalating tensions or conflict situations. For instance, lasers could effectively disarm land mines or Improvised Explosive Devices from distance without risking untoward damage or loss of life. Radio frequency weapons could create zones where enemy drones or improvised explosive devices can't operate.

DEWs are highly suited to combatting many modern military threats. For example, lasers can shoot down drone swarms, or artillery shells, whereas infantry units can use radio frequency weapons to disable adversary electronic systems such as communications and sensors. Future radio frequency weapons could be used to render specified areas unusable for adversary drone or sensor systems.

Possible scenario:
Transportable energy weapons defend against drone ambush

An Army task group equipped with AI-enabled laser weapons is deployed as part of a stability operation. Hostile irregular forces are using drones for reconnaissance and targeting the task group with small explosive payloads.

The task group are ambushed by a large drone swarm. Lasers target the drones using AI-enabled tracking systems over 200 metres away, disabling 80% of them. The remaining 20% are jammed or destroyed using electronic warfare capabilities.

The threat is neutralised. Collateral damage is reduced, with activity conducted without requiring ammunition resupplies or exposing positions through gunfire.

Such capabilities will allow future defence forces to remain in contested areas and pursue interests for longer, without necessarily needing to use full kinetic force. For example, an airlift operation transporting supplies in support of combat forces could be equipped with energy weapons to defend itself against anti-air threats such as missiles.

> *"Lasers can strike targets with pinpoint accuracy, generating almost no collateral damage and at costs as low as a few euros per shot."* - European Policy Centre, 2025. (Kremidas-Courtney, 2025).

High-density energy storage will also enable emerging electromagnetic weapons, like railguns, which harness strong electromagnetic forces to launch projectiles instead of traditional chemical explosives. Railguns expel non-explosive projectiles at hypersonic (Mach 6-7) speeds, destroying targets through kinetic energy impact. Despite their limitations, electromagnetic weapons have the advantage of relatively low 'ammunition' cost, long range (beyond current naval artillery), and provide safer logistics and storage options (non-explosive inert munitions).

A word of caution

There are technical challenges to be overcome before railguns fulfil their potential, including the large power supply currently required, heavy weight, and the requirement for advanced cooling systems.

Emerging weapon systems will complement and integrate with traditional systems

It is worth noting that novel weapons will not fully replace traditional kinetic weapon systems like artillery, at least not in the medium-term. The war in Ukraine has demonstrated that traditional weapon systems continue to have a critical role, and the technology underpinning these capabilities will continue to improve. Many novel weapons, like lasers, currently have notable disadvantages around reduced range, the need for reliable power generation, and are yet to be truly tested under sustained real-life battlefield conditions.

Similarly, cyber-electromagnetic capabilities will not completely replace traditional military capabilities either. They too will become increasingly integrated with traditional systems being equipped with both offensive and defensive modern cyber-electromagnetic capabilities that support and complement their tasks.

Strike capabilities will be more networked and adaptive

In the future, defence forces will possess enhanced strike capabilities such as missiles and UAV strike capabilities that incorporate AI/ML technologies to autonomously identify targets, coordinate with each other in real-time, and adapt navigation and targeting mid-flight.

Future kinetic strike systems will also incorporate cyber-electromagnetic payloads with the capability to, for example, disable enemy sensors or disrupt adversary targeting systems. Converging kinetic and non-kinetic effects in this way can deceive and overwhelm the adversary.

Importantly, core AI/ML-enabled command and control capabilities will form the backbone critical for the effective engagement of next-generation strike capabilities. Defence forces will need to consider the pros and cons of future strike capabilities that use AI/ML to make strike recommendations based on real-time ISR data, rules of engagement, and legality. This is especially where defence forces may have a limited number of fires and where precision is important.

Possible scenario: Neutralising an anti-ship missile system

In a contested coastal environment, an amphibious army unit employs UAVs to project force and provide covering fires as they approach an adversary missile system.

A reconnaissance drone detects enemy radar and radio emissions, geolocating targets using onboard sensors and satellite data.

Strike UAVs are launched. The first wave delivers electronic warfare effects to disrupt enemy radar, followed by kinetic strikes. UAVs adapt mid-flight based on real-time intelligence, such as changes in radar frequency or emitter location.

This allows other tailored effects conducted by an amphibious special forces unit to be delivered with precision, neutralising the missile system.

Loitering munitions and strike UAVs are rapidly evolving to recognise targets and adjust in real-time based on advanced AI/ML systems, network advances, advanced materials, and high-density storage. Such weapons will provide increasingly smaller but deadlier strike weapons. More passive examples include smart sea minefields that can be remotely operated and configured to only target adversaries, unlike its indiscriminate predecessors.

Such systems could be useful for defence forces operating without large numbers of large-scale platforms and operating expeditionary forces in highly contested environments. where control over the precision, scale, and nature of strikes is important.

Defensively, future defence forces will need to anticipate their capabilities being increasingly vulnerable to next-generation adversary missile systems that are longer range, more precise, stealthier, and faster (hypersonic). Missiles, Manoeuvrable Re-entry Vehicles, as well as ‘swarms’ of drones and loitering munitions will be increasingly utilised in conflict. Defence forces need to rapidly consider how best to counter these capabilities to remain combat-capable. The proliferation of such advanced strike capabilities, alongside advancements in adversarial C5ISRT capabilities, even among non-state actors, are likely to make large, expensive platforms, increasingly vulnerable.

CHAPTER CONCLUSION

Advances in energetics, electromagnetics, autonomous systems, AI/ML, cyber, space technologies, and information warfare capabilities are widening the continuum of effectors available to defence forces.

The spaces where conflict occurs are expanding, as next-generation effectors are being increasingly applied to new or potential conflict areas like space, cyberspace, and the information environment. These expansions will not replace traditional kinetic weapons but will complement and integrate with them, enabling defence forces to respond precisely and proportionately to a range of future threats.

These developments will provide future defence forces with an increased spectrum of proportionate military options, with greater range, speed, and precision than conventional methods. Innovations in effectors will enable a future defence force to remain in contested contexts for longer, or deter actions, without always relying on kinetic force.

The war in Ukraine has shown that modern warfare will see a broadening range of weapons and effectors across the spectrum of conflict and competition to achieve defensive and offensive ends. The delivery of some military effects are evolving almost weekly, accelerated by rapid hardware innovations, or over-the-air updates to software-defined capabilities.

Expected advances in energetics, electromagnetics, autonomous systems, AI/ML, cyber, computing, quantum, and space technologies, will have a particular influence on Defence investments in:

Offensive & defensive cyber

Information warfare

Space

Directed Energy

Sub-threshold effects

Test & development infrastructure

SUSTAINING EXPEDITIONARY FORCES

WHAT IS EXPEDITIONARY SUSTAINMENT

Expeditionary sustainment refers to the capabilities that support defence forces to operate across extended distances, often in remote or austere environments.

The effectiveness of military operations can depend on a defence force’s ability to sustain its deployed elements, making this one of the most complex and strategically significant challenges in defence logistics.

In a nutshell

The wicked problem of supporting expeditionary defence forces will be assisted, but not solved, by technologies that enhance the agility, survivability, responsiveness, and efficiency of military sustainment functions.

THE PRODUCTION OF ENERGY AND MATERIEL WILL BECOME MORE DISPERSED AND PORTABLE

Sustainable, reliable, and portable energy will be required for sustaining the next-generation of defence capabilities. This will be enabled by emerging technologies that are already changing how energy is generated, stored, distributed, and used. In particular, the miniaturisation of energy sources and advanced material science will provide alternative power generation options, opening opportunities for novel military capabilities.

Innovations in renewable energy technologies are creating a range of options for producing energy at the place it is consumed. Space-based or atmosphere-based solar power, for example, could revolutionise how expeditionary forces utilise energy beyond 2035, by receiving solar power transmitted to earth from satellites through microwaves or lasers. Deployable solar microgrids will be able to power field camps and sensor and communication systems in remote environments. The portability of future renewable energy production such as wind and river turbines, alongside high-density storage capacity, will help sustain defence forces in a variety of different operating environments, such as tropical Pacific environments or in Antarctica.

There are also several emerging technologies that could work for camps and bases. Examples could include advanced energy-shaving techniques during peak demand, thermal energy storage systems, and electrochemical fuel cells, among others.

Possible scenario: Energy efficient bases

Instead of relying on diesel generators or grid power, a future forward operating base runs on hybrid renewable microgrids.

The system includes solar panels, small wind turbines, and space-based solar, to generate electricity that is stored in large battery banks.

Backup synthetic-fuel generators remain on-site as emergency or peak-load backups.

An AI/ML informed control system manages energy flows, deciding when to charge/discharge batteries.

As a result, the base is more resilient, needing far fewer diesel fuel convoys, reducing cost and vulnerability.

Another technology developing quickly is electrochemical energy conversion fuel cells. Electrochemical fuel cells convert the chemical energy of a fuel (including hydrogen or alternatives like methanol, ammonia or ethanol) directly into electricity through electrochemical reactions, not combustion. Future fuel cells will be highly portable and generate much more power per kilo of input than diesel technologies which is greatly reducing the reliance on bulk fuel resupply. Portable cells will provide power to infrastructure like forward operating bases, mobile hospitals, and communications systems. Autonomous capabilities like long endurance drones will be powered by fuel cells and soldiers will carry compact hydrogen or methanol cells to power equipment such as radios and sensors, reducing battery load.

Energy generation will be accompanied by breakthroughs in storage technology. These could include, high-density energy storage batteries such as next-generation lithium solid-state batteries, and small portable modular energy packs that soldiers will carry.

Traditionally, defence forces have relied on diesel fuel which requires expensive, slow, and vulnerable supply chains. In future, some expeditionary force elements will carry energy generation capability, enabling them to operate for longer durations independent of fuel supply lines, with the further advantages of being less detectable (due to emitting less noise, heat, smoke, vibrations, and being generally smaller) and lower maintenance.

A word of caution

It's important to highlight that diesel will still be required to fuel many military capabilities and vehicles, at least in the medium-term.

Large, exquisite capabilities such as ships and aircraft are unlikely to become fully propelled by electricity for some time (perhaps several decades) due to the need for long range and speed, often with heavy loads.

However, light vehicles such as small patrol boats, uncrewed surveillance vessels, and light aircraft will be increasingly hybrid or, depending on task, fully electric.

This will be particularly important for emerging and future defence capabilities requiring large amounts of energy. These could include, future ISR functions relying on AI/ML at the edge, advanced computation, docking stations for RAS, directed energy weapons, cyber, and electronic warfare capabilities that all require sizeable, and reliable energy supplies (see earlier sections on the use of data and HMT).

TRANSPORT METHODS WILL BE FASTER, MORE EFFICIENT, AND BETTER PROTECTED

More things will be produced on site rather than transported

Additive manufacturing (3D printing) will allow future defence forces to produce a range of critical supplies on site, reducing logistical burden and enabling greater speed, flexibility, and resilience for defence forces in contested environments.

Advanced 3D printers will increasingly work with a fuller range of materials including metals, ceramics, and biological materials for medical uses. This will enable, for example, the 'printing' of spare parts and componentry, tools, food, or medical supplies on demand. Meanwhile, future advances into areas such as 4D printing, nano 3D printing, and integration with other emerging technologies including robotics and ML have the potential to exponentially increase the utility of additive manufacturing.

A word of caution

Additive manufacturing 'in the field' faces a variety of challenges that will not be resolved in the short term. Notably the inability for some materials to be worked with outside of a controlled environment (e.g. highly flammable, toxic, or explosive materials).

Additionally, not everything can be printed due to certification restrictions, where the scale or size requirements are beyond printers, and quality control and testing requirements.

4D printing could enable the production of smart materials that assemble themselves autonomously, such as a flat-packed shelter airdropped into a disaster zone that assembles into a rigid tent and adapts when it encounters a particular environmental effect. 3D nano printing could be used for fabricating extremely small, precise structures such as micro-sensors or nano-drones.

Additive manufacturing will be increasingly utilised by defence forces, particularly as the cost of military equipment becomes more expensive and more challenging to acquire. Military inflation is significantly higher than regular inflation, and the cost and availability of spare parts, ammunition, and artillery is currently being impacted by higher raw material costs, surging demand, and production bottlenecks.

At the same time, additive manufacturing is providing increasingly effective options to ‘print’ capabilities that could be used to achieve similar effects. For example, UAV airframes with mission specific payloads can be produced on or close to the battlefield. Such options have the potential to be more affordable, expendable, and less reliant on protracted supply chains and global markets.

> *“Developments in additive manufacturing (3D printing) and other advanced forms of production could increase the ability of defence and security forces to operate untethered from their supply bases”* - UK Ministry of Defence, 2024.

Novel materials will lighten the load on sustainment functions

Ultra-light weight, high strength, and more durable composites will be applied to an extensive range of capabilities and equipment from clothing to aircraft. Such materials will drastically reduce the burden on expeditionary supply chains, including through:

- Lower fuel consumption with lighter capabilities using less fuel.
- Longer life materials reducing the requirements for spare parts or replacements.
- Modular materials for easier transportation.
- Composite materials designed for faster and simpler repairs in the field.

Technology breakthroughs are also delivering self-healing materials. This could include coatings, armour, or technical components that automatically repair after damage. A patrol vehicle may incur small arms damage that heals itself, for example, allowing it to remain in the field until more comprehensive repairs can be conducted.

Autonomous air capabilities will transport cargo and supplies

A range of future sustainment capabilities may complement traditional airlift capabilities like fixed-wing and rotary wing logistics aircraft. Future alternatives will be especially useful in dispersed or contested environments. Autonomous airships, balloons, specialised RAS, and supersonic airframes, among others, present transformative opportunities for enhancing logistics, medical support, and humanitarian aid functions in remote and austere operating environments. The next-generation airships will be able to hover for long periods of time, even days, using combinations of future technologies such as distributed electric propulsion and tilting rotor technologies. These will allow for sustained loitering near supply points or operations in disaster zones without refuelling.

Possible scenario: Reusable logistic rockets deliver supplies to a forward operating base

A future Army is operating a forward operating base on an island. A cyclone has caused significant damage and injury and cut access to critical supplies.

A high-speed logistics rocket has a modular cargo bay containing medical kits, batteries, and communication equipment. It flies autonomously at extreme speed from land-based distribution centres and delivers its payload with precision via parachute drop before returning to base.

Extended loitering capacity combined with autonomous cargo handling systems means they will be able to deliver large volumes of critical supplies—like food, water, and medical equipment—directly to areas lacking airstrip infrastructure, including disaster zones or remote operational theatres. Such airships will be developed with innovative lightweight materials and technology advances in propulsion system technologies, autonomous flight technologies, and robotics.

Rapid developments in drone technology are improving drones' utility to deliver cargo and supplies. Drones can reach areas that current capabilities struggle to access, for example, over destroyed roads, rugged terrain, or narrow or shallow water ways. Many drones working in unison can deliver cargo reducing reliance on crewed and expensive capabilities like helicopters or trucks.

Future propulsion systems for airframes have the potential to offer future defence forces the ability to transport loads, very quickly, over long distances. Future scramjet and/or supersonic technologies for example, will likely offer the ability to deliver urgent medical supplies, ammunition, or spare parts out to isolated defence forces in the at unprecedented speeds.

Alternatively, high-altitude vehicles such as balloons can support persistent communications and environmental monitoring over crisis regions, facilitating coordination during humanitarian relief operations. They can also deliver light cargo including communications equipment or medical supplies via glide vehicles or steerable parachutes.

Together, these systems enable agile, distributed logistics, and responsive systems that reduce dependency on traditional fixed-wing or rotary platforms. Importantly, they offer options for delivering high-frequency 'just-in-time' supplies and point-to-point distribution, rather than large supply drops on fixed schedules. This allows more dynamic options for sustaining defence forces such as rapid delivery of urgent medical items like blood, vaccines, and surgical kits, particularly in contested or hard-to-reach environments.

Small boats and autonomous littoral systems will increase accessibility

Small boats and autonomous littoral systems are likely to offer greater accessibility options for sustaining land forces, particularly in coastal regions or island nations.

Future capabilities will be enabled by the integration of advances in autonomous systems, AI/ML, and advanced C5ISRT systems, hybrid and renewable propulsion systems, and advanced hull designs informed by durable and lightweight composite materials.

Future capabilities will enable covert insertion, extraction, and resupply in contested or denied littoral zones. These systems enhance mobility, reduce operator risk, and support distributed operations by operating in shallow, cluttered, or mined waters where traditional naval platforms are less useful.

When operating in austere coastal or riverine forward positions, future defence forces could be supported by autonomous boats that conduct persistent ISR, force protection, and decoy missions, while also delivering logistics and medical supplies. The ability of such craft to integrate with broader multi-domain command and control networks makes them key enablers of flexible, agile force posturing in coastal conflict theatres.

LOGISTICS AND INVENTORY SYSTEMS WILL BE OPTIMISED FOR BETTER PERFORMANCE

A wider range of capabilities will deliver more responsive supply and logistics systems

Earlier chapters described how the integration of advanced sensor systems, AI/ML, computing technologies, and information and signal processing are likely to transform core C5ISRT functions. These capabilities will be game changing when applied to the logistical task of projecting an expeditionary force over large distances.

Advanced C5ISRT technologies will provide future sustainment functions informed predictions and optimised delivery options for required cargo and supplies. For example, AI/ML capabilities will monitor supply use and reserve stocks in real-time, integrating this with live satellite and drone feeds to optimise supply routes for increased delivery speeds or protection.

Such capabilities could prove decisive when planning and executing precise logistics operations in dynamic conflict or disaster zones.

"We're entering a new era where real-time data, AI, and unmanned systems are transforming sustainment from a reactive effort into a predictive, proactive capability. We will anticipate, needs before they're voiced, prevent failures before they happen, and move thousands of pounds of cargo without risking a single soldier. It's not just about efficiency, it's about readiness, resilience, and rethinking what's possible on the battlefield" - U.S. Brigadier General Upton. Director, CL CFT. (Jones, 2025).

Possible scenario: Logistics support after a tropical cyclone

AI enabled systems help to coordinate and optimise the delivery of aid and supplies to island nations following a tropical cyclone.

AI-enabled inventory management, weather, and navigational systems cohesively monitors supply levels, monitor weather conditions, and identify damaged infrastructure or isolated communities to generate mission plans showing optimal delivery routes, resource allocations, and risks.

The plans are continuously updated as new data arrives, freeing up personnel to focus on human tasks such as strategic coordination, supporting traumatised victims, and maintaining communication with the local community, international partners, host nation governments, and other stakeholders.

Advances in technologies such as AI/ML and information and signal processing will equip machines to provide near-instant information to decision makers on complex issues, leading to reduced uncertainty and better human decision making. For example, soldiers with wearable smart equipment which monitors their body could provide real-time information to commanders on the health of personnel including fatalities, fatigue, injuries, stress, and how well-placed units are to respond to commands. Real-time AI-enabled analytical systems will better estimate how long supplies will last, based on combat tempo, weather, terrain, losses, and past consumption, ordering supplies ahead of time and optimising force sustainment.

TECHNOLOGY ADVANCES WILL IMPROVE THE CARE PROVIDED TO CASUALTIES

Technology advances in medical robotics will enable more responsive care for casualties closer to the front line, both increasing survivability and mission continuity. For example, a surgeon could remotely diagnose, triage, or operate a robotic care unit to administer care for injured personnel. Such capabilities will be enabled by high-fidelity cameras and sensors, haptic-enabled robotic equipment, and on-site diagnostics such as ultrasound and blood testing.

Significant research is also underway on how autonomous platforms like UAVs could be used to evacuate casualties. Longer-term developments could include robotic capabilities on board autonomous platforms that start life-saving treatment during transportation. This could include surgery and robotic prosthetics.

As with so many capability innovations, it is the convergence of several cutting-edge technologies that will drive novel capabilities. In this case, these include advanced AI/ML and autonomous technologies, biotechnologies, miniaturised sensors and actuators, advanced materials, high communication bandwidth and fidelity (such as space-based C5ISRT communication networks), compact power systems, and more.

Many advances in biomedical fields will have particular value for future defence forces. These include:

- Synthetic biology technologies - developing biological parts including synthetic human joints, artificial muscles, tissue engineering, and other complex gene networks. These underpin improved health outcomes for deployed and returning critical care personnel.
- Chemical, biological, radiological, and nuclear hazard (CBRN) protection combined with nano-technologies – developing solutions for rapid sensing of CBRN threats, next-generation protective clothing that heals and cleans itself, and materials that can rapidly decontaminate gear or spaces. These technologies bolster force protection and adaptive responses to unconventional threats.

Possible scenario: Digital Twins supporting special forces deployments

Special Operations teams are deployed wearing advanced biomonitoring systems that monitors their physical state including heart rate, blood pressure, oxygen levels, injury markers etc. The data is collected from biosensors in their clothing, on skin patches, or implanted into their body.

A cloud-based AI system maintains and develops a personalised digital twin for each soldier. When injury occurs, the digital twin updates in near real-time to reflect indicators of blood loss, organ stress, predicted deterioration rates, and other useful information for medics to assess.

Medics (human or robotic) access the twin and recommend the best interventions, such as drug administration, when to evacuate, and other treatment measures.

Digital twins are used to assist in triaging multiple casualties.

CHAPTER CONCLUSION

Advances in technologies will provide solutions to some expeditionary sustainment challenges, especially over the medium-term. Technology innovations are likely to enable more dispersed material production, portable energy whilst also increasing the efficiency, speed, and protection of transport and distribution methods. These will allow many force elements to become increasingly self-reliant and sustain their activities more independently from central supply provisions.

Opportunities lie in harnessing AI/ML and the power of data will mean that defence logistics functions, like resource optimisation and supply chain management, will be better optimised and utilise more efficient, responsive, and resilient systems to support operations.

Despite many promising use cases, technology innovations are unlikely to solve the fundamental physical challenges faced by remote geography, at least not in the medium-term. Future defence forces will continue to sustain complex and resource intensive operations from a distance by moving heavy quantities of people and equipment over extreme distances.

Although technology innovations are unlikely to fundamentally reshape expeditionary sustainment reality, it will positively impact the persistence, survivability, and independence of future defence forces in the face of an increasingly complex and resource-intensive battlespace.

For expeditionary sustainment, innovations in energetics, propulsion, meta-materials, production methods, miniaturisation, quantum computing, AI/ML, and autonomy will have a particular influence on defence investments in:

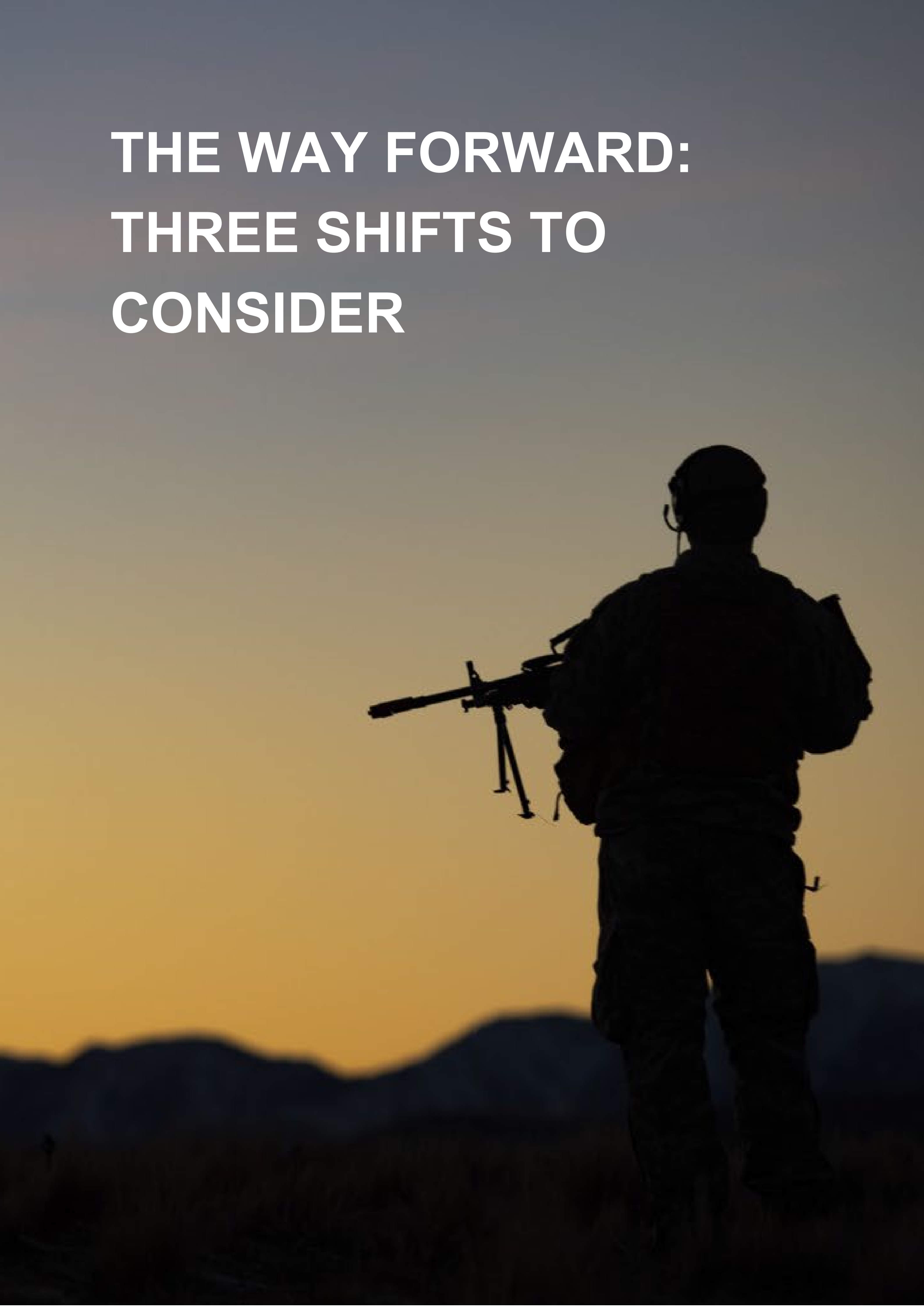
Research & Development

Energetics

Advanced logistics management

Robotic Autonomous Systems

THE WAY FORWARD: THREE SHIFTS TO CONSIDER



THE THREE SHIFTS

Adapting to these four technology themes will create significant change and is not without challenges, risks, and uncertainty for Defence. The research identified **three shifts** that carry operational, policy, and system level implications for defence forces.

All three shifts are positioned within a context where defence systems operate within legal boundaries, with appropriate human controls, and with political oversight.

Understanding the challenges and opportunities within these shifts is critical as Defence considers its future capabilities.

1. FROM HUMAN ACCOUNTABILITY BY DEFAULT, TO HUMAN ACCOUNTABILITY BY DESIGN

When acquiring advanced military capabilities that leverage emerging disruptive technologies (EDTs), human accountability, and adherence to international law, will need to be built into the system design.

Armed conflict is governed by International Humanitarian Law (IHL) and the UN Charter that set binding legal obligations around the use of force and the conduct of hostilities. Violations of these obligations give rise to legal responsibility. The emergence of autonomous defence systems incorporating AI/ML technologies that learn, decide, and have the potential to act independent of humans, has prompted significant debate about how responsibility and accountability operate when such systems are involved in conduct that may breach international law.

New Zealand is a strong supporter and upholder of the International Rules Based Order. While international humanitarian law and international human rights law already impose binding obligations, New Zealand has long advocated for norms and binding rules that EDTs are governed in a manner that upholds these frameworks in practice. Any future capabilities that harness EDTs will need to comply with domestic and international law obligations, including the New Zealand Nuclear Free Zone, Disarmament, and Arms Control Act 1987, and IHL.

Building accountability into system design should include capability acquisition processes that adequately test capabilities for adherence to IHL. Similarly, commercial arrangements will need to ensure Defence fully understands how capabilities operate, including the ability to interrogate the data used for training any AI/ML-enabled capabilities.

As military advantage increasingly relies on compressed decision cycles, the ability for humans to maintain oversight and control of risk escalation will be challenged. To account for this, de-escalatory and explanatory functions must be embedded in the system design to ensure humans retain appropriate control in autonomous decision-making processes. New Zealand’s proactive stance on managing the risks of autonomous systems and military applications of AI/ML on the international stage is useful in this respect but depends in part on other nations taking a similar approach.

2. FROM SOFTWARE SUPPORTING HARDWARE, TO HARDWARE SUPPORTING SOFTWARE

Defence forces will be increasingly defined not by the platforms and capabilities they own, but by the software that operates and connects them.

The future defence capability planning and management systems will increasingly focus on the acquisition of the latest software. Enhancing capabilities through frequent software upgrades and continually ensuring algorithmic superiority will be decisive in delivering military advantage.

Future investment priorities will increasingly reflect the critical role of software and data in generating a combat-capable force. This will create a shift from capital expenditure focussed investment to lifelong capability investment that accounts for regular software updates, technology refreshes, software licencing, cybersecurity, algorithm maintenance, and secure network and data infrastructure standards.

Software capabilities can be iterated in months, or even weeks, and will be the benchmark for how defence forces remain modern and interoperable.

A word of caution: ⚠

The pace of technology change will challenge the ability of policy, regulatory, and legal systems to adapt.

This will require policy, regulatory, and legislative settings that provide appropriate constraints on the use of technology to reduce harm, while not inadvertently limiting the options available for future Governments to utilise its defence capabilities – including overseas.

The rise of cheap precision mass (e.g. low-cost drones) will increasingly require capability procurement and management systems that are capable of quickly adjusting to changes in context, innovations, and user requirements.

Aircraft, ships, and other high-end capabilities will still be needed and must be upgraded or replaced over time. But growing costs, especially from investing in advanced software and hardware, along with rising military inflation, will stretch future budgets. Making investment choices that balance the investments needed for future technology while also managing short-term capability gaps will be increasingly difficult.

Defence procurement and assurance systems will also need to manage the complexities of ensuring future systems comply with international and domestic law. For example, understanding and testing AI/ML systems designed to identify targets will require new approaches to evaluation and testing prior to introduction into service.

From a future defence force design perspective, software will enable the assembly of capabilities across domains into networked systems. Future defence forces could take advantage of technology to produce a networked force able to deliver effects in future multi-domain conflicts.

Despite the range of technology innovations on the horizon, future defence endeavours will remain intrinsically human-centric. The people within defence forces will continue to be its most valuable capability, and the 'human domain' will remain paramount in discussions about innovative defence capabilities. Capitalising on technology innovations will require future workforce models that appropriate for a force using software as the unifying and foundational capability.

A word of caution ⚠

Defence forces may struggle to find, train, and/or retain personnel with the necessary STEM (Science, Technology, Engineering, Mathematics) skills required to manage and operate future capability systems.

3. FROM PUBLIC ENGAGEMENT, TO PUBLIC INCLUSION

Public trust in defence forces is earned, not assumed. Ensuring Defence maintains public trust will remain essential, and possibly more challenging, in an environment defined by increased contestation and technological change.

As the rate of technological change in defence capabilities accelerates, it will be important to ensure that long-standing democratic, legal, humanitarian, and military norms, rules, and conventions continue to apply. Technology is merely a tool by which human intent can be realised.

FINAL THOUGHT

This briefing has provided insights into how technology innovations, spanning across four core technology themes, are likely to influence future defence capabilities beyond 2035. Policy, operational, and system-level implications for the future defence forces have been broadly captured by the three shifts, which will become increasingly relevant and challenging for Defence to navigate.

Looking ahead, technology innovations are providing new ways to deepen interoperability and technical integration. Keeping pace with technology innovations will be critical for defence force interoperability as well as meeting minimum theatre-entry standards of the future.

Although technology-driven interoperability will increasingly become a foundation for defence partnerships, any benefits must carefully balance the considerations around cost, sovereignty, legality, and social licence.

Also, future technologies, coupled with a changing geo-strategic context, will increase considerations of resilience and the role of national industrial bases in supporting technologically modern and resilient defence forces.

Prediction is very difficult, especially about the future. This briefing is merely one contribution to technology-driven foresight to support discussion about how government, citizens, and defence forces might prudently grapple with the changes which are already occurring and are likely to accelerate.

APPENDIX ONE: RESULTS FROM PUBLIC CONSULTATION

PROPOSED LTIB TOPIC: 29 April – 27 May 2025

Key statistics:

The Ministry of Defence received 14 responses:

- A mix of members of the public (3), academics (1), and businesses (10).
- All submissions supported the Ministry's proposed topic and agreed that it was worth investigating further.
- All responses provided insights that help shape the research.

Digital technologies, sub-threshold conflict and maintaining legality were emphasised

Technologies that help harness the power of data, such as AI/ML, quantum computing, and cyber technologies like cloud infrastructure, were highlighted by nearly every submission as being highly influential for the future of New Zealand's future defence capabilities.

The importance of advanced sensors, and secure, integrated data infrastructure in shaping the development of autonomous systems was another prominent theme, as well as the growing centrality of the space domain and space-relevant capabilities.

Many submissions noted the importance of retaining combat capability in sub-threshold conflict. Innovations in cyber defence, electronic warfare, and directed energy weapons were some examples referenced by submitters that reinforced the importance of possessing a variety of graduated response options in a future sub-threshold environment.

Innovations in manufacturing and engineering were also highlighted by several submitters. Additive manufacturing (3D printing) and advancements in material science were regarded as being transformative in areas such as logistics and energy conservation, for example. Advances in energy storage and sustainable energy production, were also reinforced as critical for any future data-enabled defence force.

The importance of keeping within domestic and international law or developing new standards to govern novel technologies was another relevant area highlighted by submitters.

All of these insights were considered by the Ministry during the development of this briefing.

DRAFT BRIEFING DOCUMENT: 4 November – 25 November 2025

Key statistics:

The Ministry of Defence received 14 responses:

- A mix of members of the public (2), business (7), public entities (4) and a multilateral defence organisation (1)
- All submissions were supportive of the Ministry's briefing and were consistent with the general analysis and assessments.
- All submissions provided insights that reinforced existing analysis and inspired minor amendments to the final briefing.

Rapid adoption, growing human capital, and increasing resilience were emphasised

Submissions emphasised the importance of rapid adoption and integration of future defence capabilities. The rapid evolution of technology is narrowing the window in which to capitalise on investments before they become outdated. This can create tensions with traditional procurement methods. Adopting innovative processes that embrace rapid prototyping, greater openness to failure and the learning that comes with that, and novel commercial relationships were also emphasised.

Submissions outlined a need to grow human capital and update workforce policy settings to better enable defence personnel to leverage future innovations. Whilst defence workforce isn’t a focus of the LTIB, it is a critically important factor for future forces that wish to remain combat-capable in modern battlefields.

Resilience was another key theme emphasised by submissions, particularly in areas like cyber, operating in the context of electronic warfare, and defence supply chains. Ensuring that future forces are resilient against a variety of novel effectors, environmental factors, and sustainment challenges were highlighted as important areas for future innovation. Feedback extended into the idea of increasing national resilience, a theme which underpins the Ministry’s 2025 defence industry strategy, with some respondents highlighting that both civilian and military infrastructure, such as those supported by space technology, are likely to become increasingly at risk.

These areas are important to New Zealand’s security interests. Although some of the implications for these areas are examined throughout the LTIB, the need for further long-term research to deepen New Zealand’s understanding will continue to grow in importance.

The importance of keeping within domestic and international law when developing new standards to govern novel technologies, particularly when applied to autonomy and AI, was commonly highlighted by submissions.

APPENDIX TWO: BIBLIOGRAPHY

- Bendett, S. (2023, July 20). Roles and implications of AI in the Russian Ukrainian conflict. Russia Matters. https://www.russiamatters.org/analysis/roles-and-implications-ai-russian-ukrainian-conflict
- Bentham, J. (2025). Subsea advances and challenges for the Asia-Pacific. IISS. https://www.iiss.org/online-analysis/online-analysis/2025/05/subsea-advances-and-challenges-for-the-asia-pacific/
- Bierzynski, et al. (2021). AI at the Edge 2021 (White paper) (European Technology Platform on Smart Systems Integration, p. 6).
- Bitzinger, A., & Evron, Y. (2023). The fourth industrial revolution and military civil fusion. Cambridge University Press.
- Center for Strategic & International Studies. (2025). Mesh sensing for air and missile defence: A vision for passive, proliferated sensor networks (pp. 4–5).
- Dahlgren, et al. (2025). Mesh sensing for air and missile defence: A vision for passive, proliferated sensor networks (Center for Strategic & International Studies, pp. 4–5).
- Defence Engage. (2023). Submerged solutions: uncovering the next-generation of military underwater technology.
- ECSSR. (2024). High-Altitude Platform Stations (HAPS): Their Importances and Military Applications. https://www.ecssr.ae/en/research-products/reports/2/198378
- European Defence Agency. (2023). Enhancing EU military capabilities beyond 2040. https://eda.europa.eu/docs/default-source/eda-publications/enhancing-eu-military-capabilities-beyond-2040.pdf
- European Defence Agency, & Isdefe. (2021). EDA Technology Foresight Exercise 2021. https://eda.europa.eu/docs/default-source/eda-publications/edatechnologyforesightexercise-finalresults.pdf
- European Technology Platform on Smart Systems Integration. (2021). AI at the Edge (White paper, p. 6).
- Harding, E., & Ghoorhoo, H. (2023). Seven critical technologies for winning the next war. CSIS. https://www.csis.org/analysis/seven-critical-technologies-winning-next-war
- International Committee of the Red Cross. (2025). Artificial intelligence in the military domain: ICRC submits recommendations to UN Secretary General. https://www.icrc.org/en/article/artificial-intelligence-military-domain-icrc-submits-recommendations-un-secretary-general
- Jones, A. (2025). Redefining logistics: Army demonstrates breakthrough in autonomous ship to shore resupply. United States Army.
- Krause, J. (2021). Trusted autonomous systems in defence: A policy landscape review (King’s College London & The Policy Institute, p. 8).
- Kremidas Courtney, C. (2025). Directed energy weapons and the future of European defence (p. 1). European Policy Centre.
- Langford, I. (2025). Accelerated change – the evolving character of society and conflict in an age of speed, uncertainty and transformation. In D. P. Baker & M. Hilborne (Eds.), War 4.0.

- Lt. Col. Tingle, A. (2019). When the Balloon Goes Up: High-Altitude for Military Application. Army University Press. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Tingle-High-Alt-Balloon/

- Marape, J. (2025, September). Prime Minister Marape Urges Europe to Strengthen Trade with Pacific at EU-Pacific Islands Leaders Meeting. Department of Prime Minister and National Executive Council. Papua New Guinea Government.

- Manson, K. (2024, February). AI warfare is already here. Bloomberg. https://www.bloomberg.com/features/2024-ai-warfare-project-maven/?embedded-checkout=true

- Ministry of Business, Innovation and Employment, New Zealand. (2019). Deepening our understanding of business innovation: Main report from a study based on interviews with New Zealand business.

- Nouwens, M., Singh, P., & Soare, S. (2023). Software defined defence: Algorithms at war. The International Institute for Strategic Studies. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/iiss_software-defined-defence_17022023.pdf

- Office of the Director of National Intelligence. (2021). Global Trends 2040: The future battle-field. https://www.dni.gov/index.php/gt2040-home/gt2040-deeper-looks/future-of-the-battlefield

- Sayler, K. M. (2020). Artificial intelligence and national security (Congressional Research Service, p. 28).

- Seet, et al. (2024). Opportunities and challenges posed by disruptive and converging information technologies for Australia's future defence capabilities: A horizon scan. Edith Cowan University. https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=4802&context=ecuworks2022-2026#page22

- Stebbins, D., et al. (2024). Exploring artificial intelligence use to mitigate potential human bias within U.S. Army Intelligence Preparation of the Battlefield processes. RAND Corporation. iii.

- United Kingdom Ministry of Defence. (2024). Global Strategic Trends out to 2055. United Kingdom Government.

- United Kingdom Ministry of Defence. (2025). Strategic Defence Review, making Britain safer: Secure at home, strong abroad. United Kingdom Government. https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad

APPENDIX THREE: GLOSSARY

Term	Definition	Source (if applicable)
4D printing	The process of 4D printing is essentially the same as 3D printing, where a structure is built layer by layer. However, 4D printing uses unique, programmable 'smart' materials and novel designs to allow the finished product to respond to stimuli in a predictable way. This adds the fourth dimension – time. 4D printed materials could be developed to self-assemble, self-repair, adapt to their environment, or transform in response to specific triggers. The combination of different 'smart' materials (for example shape-memory alloys which can be deformed and then return to their original shape when heated) that respond to one or more stimuli allows complex structures and behaviours.	UK Government
Acoustic sensors	Acoustic sensors are devices that use sound waves to remotely sense and communicate in underwater environments. Unlike optical or electromagnetic waves, which attenuate rapidly in water, acoustic waves can travel long distances, making them ideal for ocean sensing. These sensors are used for mapping oceanographic and biological processes, tagging and tracking marine life, measuring environmental features like fish distributions and ice thickness and supporting underwater communication and navigation systems.	Massachusetts Institute of Technology
Advanced computing	Advanced computing, also known as high-performance computing, refers to the use of supercomputers, or computer clusters functioning as a supercomputer, to undertake very large-scale projects.	European Union
Advanced radio frequency technologies	Advanced Radio Frequency Communication refers to the use of sophisticated technologies and systems that transmit and receive data across the electromagnetic spectrum, particularly in the radio and microwave frequency bands. Key advancements include software-defined radio, millimetre-wave systems, beamforming, dynamic spectrum access, and secure low-probability-of-intercept communications. These innovations enable faster, more reliable, and more secure wireless connectivity, even in complex or contested environments.	Global Institute for National Capability

Aerostat radars	An aerostat radar is a radar system mounted on an aerostat, which is a lighter-than-air aircraft (like a tethered balloon or blimp) that uses buoyant gas (typically helium) to stay aloft. These radars are used for persistent surveillance, especially in military and border security contexts.	Massachusetts Institute of Technology
AI (Artificial Intelligence) (AI/ML)	The ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalise, or learn from past experience.	United Nations
AI at the edge	The deployment of artificial intelligence algorithms on edge devices, where data is generated, rather than relying on centralised cloud computing. This enables real-time data processing, reduced latency, and improved privacy.	Institute of Electrical and Electronics Engineers
Attack surface	The attack surface refers to the sum of all possible points where an unauthorised user can try to enter or extract data from an environment. This includes all exposed and vulnerable software, network, and hardware points.	Palo Alto Networks
Augmented reality	Augmented reality (AR) refers to the real-time integration of digital information into a user's environment. AR technology overlays content onto the real world, enriching a user's perception of reality rather than replacing it.	IBM
Bio-chemical sensors	A bio-chemical sensor is a device that measures biological or chemical reactions by generating signals proportional to the concentration of an analyte (e.g. glucose) in the reaction. Bio-chemical sensors are employed in application such as disease monitoring, drug discovery, and detection of pollutants, disease-causing microorganisms and markers that are indicators of disease in bodily fluids (blood, urine, saliva, sweat).	National Center for Biotechnology Information
C5ISRT	Command, Control, Communications, Combat Systems, Cyber, Intelligence, Surveillance and Reconnaissance (ISR) and Targeting.	NZDF
Cognitive systems	Cognitive systems are natural or artificial information processing systems, including those responsible for perception, learning, reasoning, decision-making, communication, and action.	UK Government

Combat tempo	The rate or rhythm of military activity relative to the enemy, within tactical engagements and battles and between major operations.	NZDF
Command and Control	The process and means for exercising of authority over assigned forces and lawful direction of them.	NZDF
Composante Spatiale Optique (CSO)	A French military reconnaissance satellite programme.	Airbus
Cyberspace	The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.	NZDF
Cyber-electromagnetic	Activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system.	US Department of the Army Headquarters
Data fusion	Data fusion is a process that joins together different sources of data. The main concept of using a data fusion methodology is to synthesise data from multiple sources in order to create collective information that is more meaningful than if only using one form or type of data.	Encyclopaedia of Big Data
Docking stations	A device used to connect one appliance to another.	Dictionary
(Operational) Domain	Defined areas with discrete characteristics where manoeuvre, targeting, fires, and other military activities are performed to create effects or achieve objectives in the engagement space of the operating environment. Note: The operational domains are maritime, land, air, space, and cyber/electromagnetic.	NZDF
Drone	A craft without a human pilot on board.	The Economist A-Z list of military terms
Edge computing	Edge computing is a distributed computing framework that brings enterprise applications closer to data sources such as Internet of Things devices or local edge servers. This proximity to data at its source can deliver strong business benefits, including faster insights, improved response times and better bandwidth availability.	IBM

Electronic warfare	Military action that exploits electromagnetic energy to provide situational awareness and create offensive and defensive effects.	NZDF
Energetics	The branch of science concerned with energy and its transformation.	Collins Dictionary
Encryption	The process of transforming data into an unintelligible form to enable secure transmission.	Protective Security Requirements NZ
Frigate	The smallest type of warship capable of prolonged independent and sustained operations and “main combat-capable ships of the Navy that can combat simultaneous threats from the air, surface and sub-surface.	NZDF
Force multiplier	The effect produced by a capability that, when added to and employed by a combat force, significantly increases the combat potential of that force and thus enhances the probability of successful mission accomplishment.	Oxford reference
Force protection	All measures and means to minimise the vulnerability of personnel, facilities, materiel, operations, and activities from threats and hazards to preserve freedom of action and operational effectiveness of the force.	NZDF
Forward operating base	A base established forward of a main operating base from which tactical operations are mounted and supported.	NZDF
Haptic-enabled	Systems that simulate touch through vibration, motion, or other forces. The term haptic is derived from the Greek word *haptikós*, meaning “to touch” or “to grasp.” Haptic technology can also be used to enhance how users interact with and manipulate virtual objects.	Britannica
High-density energy storage	High-density storage refers to methods that maximise the amount of energy or material stored per unit volume. In hydrogen storage, this means developing systems that can store hydrogen at high pressure or in compact solid forms to achieve greater energy density, which is crucial for applications like transportation and portable power.	US Department of Energy
Information warfare	Provision, assured use, and protection of information, processes, systems, and networks, and the limiting, degrading, and denying that of adversaries to achieve operational advantage across the battlespace.	NZDF

Intelligence	The product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, to identify threats and offer opportunities for exploitation by decision-makers.	NZDF
Intelligence, Surveillance, and Reconnaissance	An activity that synchronises and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function.	NZDF
Intelligence, surveillance, target acquisition and reconnaissance	The prioritised integration, coordination, and synchronisation of capabilities and activities to acquire, process, and disseminate information and intelligence to support planning and executing operations.	NZDF
Interoperability	The ability of systems, units, or forces to provide services to and accept services from other systems, units and, forces and to use the services so exchanged to enable them to operate effectively together	NZDF
Irregular forces	Irregular forces are armed individuals or groups who are not members of the regular armed forces, police, or other internal security forces. Irregular forces can be insurgent, guerrilla, or criminal organisations or any combination thereof.	Headquarters U.S Army Training and Doctrine Command
ISR	Intelligence, surveillance, and reconnaissance	NATO
Littoral	Coastal sea areas and that portion of the land which is susceptible to influence or support from the sea.	NZDF
Logistics	The process of moving personnel, equipment, and other military supplies from one place to another, and of maintaining said equipment.	The Economist A-Z list of military terms
Loitering drones/munitions	Loitering munitions are autonomous missiles that can stay airborne for some time, identify a target, and then attack.	Brookings Institute

Machine Learning (ML)	Machine learning is a type of artificial intelligence that allows machines to learn from data without being explicitly programmed. It does this by optimising model parameters (i.e. internal variables) through calculations, such that the model's behaviour reflects data or experience. The learning algorithm then continuously updates the parameter values as learning progresses, enabling the ML model to learn and make predictions or decisions based on data science.	International Standards Organisation
Machine speeds	Machine speed analysis is the ability to process vast amounts of data to examine or determine their relationship or value much quicker than could be done by humans and to produce a statement of findings.	Trilateral Research
Multi-static radar	A radar system having two or more transmitting or receiving antennae with all antennae separated by large distances when compared to the antennae sizes.	Science Direct
Nano 3D printing	Nano 3D printing refers to additive manufacturing techniques that enable the creation of three-dimensional microstructures with nanometer-scale resolution.	University of Birmingham
Nano-drones	Nano-drones are unmanned aerial systems with dimensions ranging between 15 cm and 2.5 cm and weighing between 50 g and 3 g. These insect-sized drones are designed for stealthy surveillance, intelligence gathering, and operations in enclosed or sensitive environments. Due to their small size and low radar cross section, they are difficult to detect using conventional radar systems and pose emerging challenges in defence and security contexts.	Cranfield University Centre for Electronic Warfare, Information and Cyber
Nuclear fusion	Nuclear fusion is the process by which two light atomic nuclei combine to form a single heavier one while releasing massive amounts of energy.	International Atomic Energy Agency
Open-source data	Data that anyone can use or share. It is openly accessible and is both human-readable and machine readable.	Data.govt.nz

Photonic computing	Photonic computing leverages the speed and efficiency of light. Photons can transmit data faster than electrons and work in low-energy environments, which makes them perfect for processing intensive workloads like scientific computations, machine learning and optimisation problems.	World Economic Forum
Photonic technologies/ communication	Photonic technologies involve the design, study, and development of materials and systems that control light-matter interactions. Photonic technologies are used in fields such as telecommunications, sensing, data storage, next-generation lasers and LEDs, optical computing, and secure quantum communication.	Newcastle University
Platform	The specific vehicles or facilities which host and use equipment that has a particular military or intelligence task that is needed in the field.	BAE Systems
Position, Navigation, and Timing (PNT)	A PNT service is any system, network, or capability that provides a reference to calculate or augment the calculation of longitude, latitude, altitude, or transmission of time or frequency data, or any combination thereof.	U.S. National Institute of Standards and Technology
Predictive analytics	Predictive analytics is a branch of advanced analytics that makes predictions about future outcomes using historical data combined with statistical modelling, data mining techniques and machine learning.	IBM
Propulsion technology	Propulsion technology refers to the engineering and scientific principles behind systems that generate thrust to move vehicles—especially aircraft and spacecraft—through air or space. It encompasses a wide range of systems including rocket engines (solid and liquid fuel), air-breathing engines such as ramjets, scramjets, and pulse jets, gas turbines (turbojets, turbofans, turboprops) and electric and hybrid propulsion systems.	University of Sheffield
Quantum Key Distribution	Quantum key distribution (QKD) utilises the unique properties of quantum mechanical systems to generate and distribute cryptographic keying material using special purpose technology. Quantum cryptography (QC) uses the same physics principles and similar technology to communicate over a dedicated communications link. Published theories suggest that physics allows QKD or QC to detect the presence of an eavesdropper, a feature not provided in standard cryptography.	US National Security Agency

Quantum technologies	Quantum technologies are based on the control of quantum systems at the scale of atoms, molecules, and electrons. They enable next-generation capabilities in imaging and sensing, computing and modelling and secure communication. These technologies rely on advances in physics, materials science, computer science, and engineering, and are expected to revolutionise fields from medicine to cybersecurity.	US National Science Foundation
Radio frequency sensors	A radio frequency (RF) sensor is a device used to detect, analyse, and locate radio signals across a range of frequencies. These sensors are essential for spectrum analysis, signal detection, direction finding and interference monitoring.	US Department of Homeland Security
Reconnaissance	A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an adversary or to obtain data concerning the meteorological, hydrographical or geographic characteristics of a particular area.	NZDF
Robotic Autonomous systems (RAS)	RAS can be viewed as the application of software, artificial intelligence and advanced robotics to perform tasks as directed by humans. Simply, autonomy is the ability of a machine to perform a task without human input. Thus, an autonomous system is a machine, whether hardware or software, which, once activated, performs some task or function on its own.	Australian Army
Scramjet	An air-breathing engine, like a jet, that works at hypersonic speed—Mach 5 or faster. It uses oxygen from the air to combust with fuel and generate thrust. Unlike rockets, which carry their own oxygen, scramjets are much more efficient because they rely on atmospheric oxygen.	University of Queensland
Seismic micro sensors	A seismic micro sensor is a sensitive device that detects ground motion. Modern versions are electronic and can detect movements as small as 1/10 million centimetres, making them suitable for detecting micro-seismic events.	US Geological Survey
Sentry	A sentry is a person assigned to stand watch for security purposes, such as a pier sentry or roving patrol. The sentry is responsible for maintaining vigilance, preventing unauthorised access, and ensuring safety and security of personnel and property.	US Department of Defence - Watch Standing Manual

Signal	A type of message, the text of which consists of one or more letters, words, characters, signal flags, visual displays, or special sounds, with prearranged meaning and which is conveyed or transmitted by visual, acoustic, or electrical means.	NZDF
Signal processing	Signal processing is the transformation of collected signals into a recognisable format, such as signal characteristics, letters, numbers, pictures or speech.	Australian Signals Directorate
Software-defined radios	Software-defined radio (SDR) is defined as a radio communication system that utilizes software for the modulation and demodulation of radio signals, allowing for reconfiguration and upgrade capabilities in real time to accommodate various radio protocols. SDR systems typically involve significant signal processing performed by general-purpose computers or reconfigurable digital electronics.	Science Direct
Speech and natural language processing	Speech and natural language processing deals with how computers understand, process, and manipulate human languages. It can involve things like interpreting the semantic meaning of language, translating between human languages, or recognising patterns in human languages. It makes use of statistical methods, machine learning, neural networks and text mining.	US National Library of Medicine
Stability and support operations	Operations that impose security and control over an area while employing military capabilities to restore services and support civilian agencies.	NZDF
Supersonic	Greater than the speed of sound (Mach 1).	NASA
Surveillance	The systematic observation across all domains, places, persons or objects by visual, electronic, photographic, or other means.	NZDF
Sustainment	The provision of personnel, logistics, and other support required to maintain and prolong operations or combat until successful accomplishment of the mission or the national objective.	NZDF

Synthetic environments	A synthetic environment (SE) is a computer simulation that represents activities at a high level of realism, from simulation of theatres of war to factories and manufacturing processes. These environments may be created within a single computer or a vast distributed network connected by local and wide area networks and augmented by super-realistic special effects and accurate behavioural models. SE allows immersion into the environment being simulated.	US Department of Defence Modelling and Simulation Glossary
Target acquisition	The detection, identification, and location of a target in sufficient detail to permit the effective employment of weapons.	NZDF
Targeting	The process of selecting and prioritising targets and matching the appropriate response to them by taking into account operational requirements and capabilities.	NZDF
Theatre	A designated geographic area for which an operational-level joint or combined commander is appointed and in which a campaign or series of major operations is conducted.	NZDF
Theatre entry standards	Training, medical, administrative, equipment, or other requirements necessary to prepare supporting personnel and forces for the tactical and environmental conditions in theatre.	US Department of Defence Instruction 1322.32
Unmanned Aerial Vehicle (UAV)	An air vehicle that flies under remote pilot control or autonomous programming without a human on board in control.	NZDF
Unmanned Surface Vehicle (USV)	A surface vessel machine that does not require, or usually support, a human on-board.	Australian Navy RAS-AI Strategy 2024

MANATŪ KAUPAPA WAONGA
NEW ZEALAND MINISTRY OF DEFENCE

defence.govt.nz