2024

Opportunities and challenges posed by disruptive and converging information technologies for Australia's future defence capabilities: A horizon scan

Pi-Shen Seet
Edith Cowan University

Anton Klarin

Janice Jones

Mike Johnstone
Edith Cowan University

Helen Cripps
Edith Cowan University

See next page for additional authors

10.25958/0x5j-wd23
Seet, P-S., Klarin, A., Jones, J., Johnstone, M., Cripps, H., Sharafizad, J., Wilk, V., Suter, D., Marceddo, T., 2024. *Opportunities and Challenges posed by Disruptive and Converging information technologies for Australia's future defence capabilities: A Horizon Scan*. Strategic Policy Grant Program Final Report. Edith Cowan University, Joondalup, Western Australia. https://doi.org/10.25958/0x5j-wd23

Opportunities and Challenges posed by Disruptive and Converging information technologies for Australia's future defence capabilities: A Horizon Scan

Strategic Policy Grant Program Final Report

Pi-Shen Seet
Anton Klarin
Janice Jones
Mike Johnstone
Helen Cripps
Jalleh Sharafizad
Violetta Wilk
David Suter
Tony Marceddo

March 2024

Research note

The Strategic Policy Grants Program run by the Department of Defence is an open and competitive mechanism for Defence to support independent research, events and activities.

This document should be attributed as Seet, P-S., Klarin, A., Jones, J., Johnstone, M., Cripps, H., Sharafizad, J., Wilk, V., Suter, D., Marceddo, T., 2024. *Opportunities and Challenges posed by Disruptive and Converging information technologies for Australia's future defence capabilities: A Horizon Scan.* Strategic Policy Grant Program Final Report. Edith Cowan University, Joondalup, Western Australia. https://doi.org/10.25958/0x5j-wd23

COVER IMAGE: DALL-E, OPENAI

Phone +61 8 6304 2486
Email p.seet@ecu.edu.au **Web** < http://www.ecu.edu.au/schools/business-and-law>

Table of Contents

List of Figures and Tables

Executive Summary

Introduction. The research project's objective was to conduct a comprehensive horizon scan of Network Centric Warfare (NCW) technologies—specifically, Cyber, IoT/IoBT, AI, and Autonomous Systems. Recognised as pivotal force multipliers, these technologies are critical to reshaping the mission, design, structure, and operations of the Australian Defence Force (ADF), aligning with the Department of Defence (Defence)'s offset strategies and ensuring technological advantage, especially in the Indo-Pacific's competitive landscape.

Research process. Employing a two-pronged research approach, the study first leveraged scientometric analysis, utilising informetric mapping software (VOSviewer) to evaluate emerging trends and their implications on defence capabilities. This approach facilitated a broader understanding of the interdisciplinary nature of defence technologies, identifying key areas for further exploration. The subsequent survey study, engaging 415 professionals and six experts across STEM, law enforcement, and ICT, aimed to assess the impact, deployment likelihood, and developmental timelines of the identified technologies.

Findings. Key findings revealed significant overlaps in technology clusters, highlighting 11 specific technologies or trends as potential force multipliers for the ADF. Among these, Cyber and AI technologies were recognised for their immediate potential and urgency, suggesting a prioritisation for development investment. The analysis presented a clear imperative for urgent and prioritised technological investments, specifically in Cyber and AI technologies, followed by IoT/IoBT and autonomous systems technologies. The recommended strategic focus entails enhancing cyber security of critical infrastructure, optimising network communications, and harnessing smart sensors, among others.

Implications. To maintain a competitive edge, the ADF and the Australian government must commit to significant investments in these priority technologies. This involves not only advancing the technological frontier but also fostering a flexible, innovation-friendly environment conducive to leveraging non-linear opportunities in technology innovation. Such an approach requires a concerted effort from both public and private sectors to invest resources effectively, ensuring the ADF's adaptability and strategic overmatch in a rapidly changing technological landscape.

Conclusion. Ultimately, this research illuminates the path forward for the ADF and Defence at large, highlighting the need for strategic investments in emerging technologies. By identifying strategic gaps, potential alliances, and sovereign technologies of high potential, this report serves as a blueprint for enhancing Australia's defence capabilities and securing its strategic interests in the face of global technological shifts.

Acknowledgements

The authors would like to acknowledge the funding provided as part of this research by the Strategic Policy Grants Program of the Australian Department of Defence and for the Department's patience understanding and flexibility in facilitating the research during and after the COVID-19 pandemic period.

Chapter 1 - Introduction

Background

In an era of rapidly emerging disruptive technologies, the challenge is for strategic planners to remain current with technological advancements and their implications, given the uncertain nature of development in these rapidly changing technologies[1] and to translate this to strategic overmatch through successful adoption of emerging technologies.[2]

Two important topics of priority interest have been identified by the Australian Department of Defence (Defence), namely:

1. Emerging trends in Homeland Security (especially in cyber, critical infrastructure, and unmanned and autonomous systems); and
2. Opportunities / challenges posed by disruptive and converging technologies.

Various methodologies and techniques have been increasingly used by different countries to help identify emerging and disruptive technologies as force multipliers.[3] These methodologies and techniques can help foresee disruptive innovations which is the focus of this research project.

Aim of Research

The aim of the project is to conduct a horizon scan[4], an analytic method for future-oriented thinking, to examine the opportunities and challenges of disruptive and converging Network Centric Warfare (NCW) technologies of:

1. Cyber[5];
2. IoT/ IoBT[6];
3. AI[7]; and
4. Autonomous systems[8].

[1] Danneels, E 2004, 'Disruptive Technology Reconsidered: A Critique and Research Agenda', *Journal of Product Innovation Management*, vol. 21, no. 4, pp. 246-58, Seet, P-S, Jones, JT, Spoehr, J & Hordacre, A-L 2018, *The Fourth Industrial Revolution: the implications of technological disruption for Australian VET*, 1925717208, NCVER, Adelaide, Tellis, GJ 2006, 'Disruptive Technology or Visionary Leadership?', *Journal of Product Innovation Management*, vol. 23, no. 1, pp. 34-8.
[2] Pincombe, B, Ryan, A, Kempt, N, Stephens, A, Tomecko, N, Reid, DJ & Tang, K 2019, 'Systemic Design of a Force for the Australian Army in 2050', in AP Jackson (ed.), *Design Thinking: Applications for the Australian Defence Force*, Australian Defence Publishing Service, Canberra, vol. 3.
[3] Department of Defence 2016, *2016 Integrated Investment Program*, Commonwealth of Australia, Canberra, Hanson, F & Uren, T 2018, *Australia's Offensive Cyber Capability*, Australian Strategic Policy Institute,, Canberra, Simms, A 2019, 'Force Multiplier', *Impact*, vol. 2019, no. 1, pp. 35-8.
[4] Connery, D 2013, 'Horizon Scanning: Enhancing Strategic Insight for National Security Policymaking', *Security Challenges*, vol. 9, no. 3, pp. 11-30, Johnston, R & Cagnin, C 2011, 'The influence of future-oriented technology analysis: Addressing the Cassandra challenge', *Futures*, vol. 43, no. 3, pp. 313-6, Ramalingam, B & Jones, H 2007, *Strategic futures planning: a guide for public sector organisations*, Ark Group.
[5] Thompson, M 2016, 'The ADF and cyber warfare', *Australian Defence Force Journal*, no. 200, pp. 43-8.
[6] Abdelzaher, T, Ayanian, N, Basar, T, Diggavi, S, Diesner, J, Ganesan, D, Govindan, R, Jha, S, Lepoint, T & Marlin, B 2018, 'Toward an Internet of Battlefield Things: A Resilience Perspective', *Computer*, vol. 51, no. 11, pp. 24-36, Russell, S & Abdelzaher, T 2018, 'The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making', paper presented to MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM).
[7] Judd, GB, Szabo, CM, Chan, KS, Radenovic, V, Boyd, P, Marcus, K & Ward, D 2019, *Representing and reasoning over military context information in complex multi domain battlespaces using artificial intelligence and machine learning*, vol. 11006, SPIE Defense + Commercial Sensing, SPIE.
[8] Kua, C 2016, 'Autonomous weapon systems, international law and meaningful human control', *Australian Army Journal*, vol. 13, no. 1, pp. 21-34.

These four digital technology fields have been identified as force multipliers in policy and research papers[9] that will have an impact on the mission, design, structure and operations the Australian Defence Force (ADF)[10].

In so doing, the project will also help address Defence's offset and A2/AD strategies by understanding the potential trends in sustaining military-technological advantage in this new era of great power competition, especially in the Indo-Pacific region[11].

Research Method

As part of the horizon scan, the research involved the conduct of two studies using scientometrics and a survey to collect data and analyse emerging and disruptive trends which are relevant to the ADF to remain current with technological advancements and their implications, given the uncertain nature of development in these rapidly changing technologies[12] and to translate this to strategic overmatch through successful adoption of emerging technologies[13].

Study 1 – Scientometric Study.

The first study was a scientometric study supported by informetric mapping software. This focused on identifying opportunities and challenges in disruptive technologies for defence forces, utilising an online-based literature discovery approach to collect data and analyse opportunities and challenges posed by disruptive and converging technologies in the four specific, but overlapping, digital technology areas mentioned above.

To provide a taxonomy of the vastly interdisciplinary topic of emerging technologies and defence forces literature, this study employed scientometric research methods, which provide a bird's-eye view of the field and bridge gaps between the variety of disciplines. This study utilised VOSviewer, a scientometric mapping software, that demonstrates relationships between indicators based on citation analysis in a visual map.[14] This study followed established scientometric review protocols in carrying out this scoping review of the literature.[15] These steps include: 1) establishing the breadth of the review, 2) determining search criteria, 3) inclusion and exclusion of publications, 4) analysis of results, and 5) dissemination of findings. Literature review and scientific mapping using scientometric analysis of the R&D trends of technologies in these areas was carried out. This analysis presents a bird's-eye view on the state-of-the-art of a particular field[16].

Study 2 – Survey Study.

Subsequently, Study 2 built on the findings of the scientometric study to carry out to develop and execute a questionnaire that adapted methodology developed by the University of Hamburg's Institute of Peace Research

[9] Department of Defence 2016, *2016 Integrated Investment Program*, Commonwealth of Australia, Canberra, Hanson, F & Uren, T 2018, *Australia's Offensive Cyber Capability*, Australian Strategic Policy Institute,, Canberra, Simms, A 2019, 'Force Multiplier', *Impact*, vol. 2019, no. 1, pp. 35-8.

[10] Ryan, M 2019, *An Australian Intellectual Edge for Conflict and Competition in the 21st Century*, Strategic & Defence Studies Centre, Australian National University.

[11] Blizzard, TJ 2016, 'The PLA, A2/AD and the ADF Lessons for Future Maritime Strategy', *Security Challenges*, vol. 12, no. 3, pp. 61-82, Langford, I 2017, 'Australia's offset and A2/AD strategies', *Parameters*, vol. 47, no. 1, pp. 93-102, Thomas-Noone, B 2017, 'Mapping the Third Offset: Australia, the United States and future war in the Indo-Pacific', *United States Studies Centre*, vol. 5.

[12] Danneels, E 2004, 'Disruptive Technology Reconsidered: A Critique and Research Agenda', *Journal of Product Innovation Management*, vol. 21, no. 4, pp. 246-58, Seet, P-S, Jones, JT, Spoehr, J & Hordacre, A-L 2018, *The Fourth Industrial Revolution: the implications of technological disruption for Australian VET*, 1925717208, NCVER, Adelaide, Tellis, GJ 2006, 'Disruptive Technology or Visionary Leadership?', *Journal of Product Innovation Management*, vol. 23, no. 1, pp. 34-8.

[13] Australian Army 2019, *Soldier Combat System Program (SCSP) and Human-Machine Teams (HUM-T) Discussion Paper*, Australian Army HQ, viewed 19 November 2019 2019, <https://www.tenders.gov.au/Atm/Show/00a38659-49c0-40a3-94f5-8b8c264fb6b3>.

[14] Klarin, A, Inkizhinov, B, Nazarov, D & Gorenskaia, E 2021, 'International business education: What we know and what we have yet to develop', *International Business Review*, vol. 30, no. 5, p. 101833.

[15] Klarin, A & Suseno, Y 2023, 'An Integrative Literature Review of Social Entrepreneurship Research: Mapping the Literature and Future Research Directions', *Business & Society*, vol. 62, no. 3, pp. 565-611.

[16] Korom, P 2019, 'A bibliometric visualization of the economics and sociology of wealth inequality: a world apart?', *Scientometrics*, vol. 118, no. 3, pp. 849-68, van Eck, N & Waltman, L 2009, 'Software survey: VOSviewer, a computer program for bibliometric mapping', ibid.vol. 84, no. 2, pp. 523-38, van Eck, NJ & Waltman, L 2014, 'Visualizing Bibliometric Networks', in Y Ding, R Rousseau & D Wolfram (eds), *Measuring Scholarly Impact: Methods and Practice*, Springer International Publishing, Cham, pp. 285-320.

and Security Policy (IFSH)[17]. It asked various industry professionals to evaluate the potential impact, likelihood of deployment / utilisation, extensiveness of use, and novelty of use of the four general technology areas mentioned above in future conflicts. In addition, it also elicited responses as to the timeliness of development of these technologies and where defence forces like the ADF should be investing in the future.

Data was collected from 415 industry professionals in a panel sourced by a commercial survey company in the following three fields:

1. Science, technology, engineering and mathematics (STEM);
2. Law enforcement, defence, security or emergency services; and
3. Information and communication technology (ICT).

In addition, six experts with extensive experience in these fields were also surveyed concurrently.

Ethics approval

Before conducting this research, appropriate ethics approvals were obtained from the Edith Cowan University's Human Research Ethics Committee (REF: 2020-01485-SEET).

Key Findings and Implications

After carrying out an extensive analysis of over 6,300 research publications across the four highlighted technologies, Study 1 identified a number of significant overlapping clusters among the main technological areas. In terms of future technologies, the scientometric review also identified 11 specific technologies or technological trends for further investigation as force multiplies in defence as follows:

1. Cyber Security of critical infrastructure;
2. Network Communications and Information technologies (e.g. for the mission design, structure, and operations);
3. Swarm intelligence-related technologies and systems;
4. Industry 4.0 technologies where the cyber-physical domains merge;
5. Unmanned and autonomous systems;
6. Optimisation and other algorithms;
7. Neural Networks;
8. Smart Sensors;
9. Deep/Machine Learning;
10. Civil and military R&D and uses of these technologies; and
11. Convergence of technologies in strategic industries that support any phases of military operation.

In its survey of 415 professionals and six experts, Study 2 found that of the four main technology areas, cyber and AI offered more potential and urgency than IoT/IoBT and autonomous systems. Together with the research on 11 specific technologies or trends in technologies, priorities were developed for investing in development of these technologies.

[17] Favaro, M, Renic, N & Kühn, U 2022, *Negative multiplicity: Forecasting the future impact of emerging technologies on international stability and human security*, Institute of Peace Research and Security Policy at the University of Hamburg, Hamburg.

Implications

Overall, the research has the following main implications for military forces in general and for the Australian Defence Force.

1. **Urgent investment needed to develop and capitalise on these technologies**. Given the pace of technological development, some of the milestones in the recent 2023 Defence Strategic Review (DSR)[18] and 2024 Defence Industry Development Strategy (DIDS)[19] may need to be brought forward.

2. **Prioritise the investment in technology.** The table below summarises the priorities for technological investments in the context of Australian defence.

Table 1.1 – Summary of Technology Investment Priorities

Priority	Main technology areas	Specific technologies
1	Cyber technologies, AI technologies	Cyber Security of critical infrastructure, network communications and IT, smart sensors
2	IoT/ IoBT technologies	Deep/ machine Learning technologies, unmanned and autonomous systems, optimisation and other algorithms, neural networks, industry 4.0 technologies, capitalising on the convergence of technologies in strategic industries, exploiting both civil and military R&D and uses of these technologies
3	Autonomous systems technologies	Swarm intelligence-related technologies and systems

3. **More explicit commitment of resources to invest in these technologies from both government and private sector**. To maintain its technological edge in this area, both the Australian government and the private sector will have to make clear and significant investments in these technologies.

4. **Higher flexibility is needed to exploit non-linear opportunities in technology innovation**. To capitalise fully on these technologies, the culture and nature of decision-making among the relevant defence stakeholders will have to change, especially to keep up with advancements in the private sector in areas of high technology and retention of skilled personnel.

These recommendations will help Defence and the ADF identify possible strategic gaps, promising alliance partners, and high-potential sovereign technologies to develop.

[18] Department of Defence 2023, *Defence Strategic Review*, Commonwealth of Australia, Canberra, ACT.
---- 2024, *Defence Industry Development Strategy*, Commonwealth of Australia, Canberra, ACT.

Chapter 2 - Study 1: Scientometric Study

Introduction

This chapter explains the research conducted for the scientometric study that examines the state-of-the-art literature of emerging and disruptive technologies and how they may impact on military and defence capabilities, in particular focusing on the following technology areas:

1. Cyber;
2. Internet-of-Things (IoT) / Internet of Battlefield Things (IoBT);
3. Artificial Intelligence (AI); and
4. Autonomous systems.

To analyse these technologies in the military domain, an understanding the complex systems that underpin these technologies in the wider environment is necessary. The ecosystem of the phenomena is best understood through the lens of a systems research perspective, which provides an interdisciplinary approach to study complex systems in society, nature, and designed systems.[20] Furthermore, a whole-of-systems approach will allow links and interrelationships between subsystems and constructs and chains of causality between constructs to surface.[21] This practice of analysing the whole rather than individual subsystems is referred to as holism.[22]

In the conduct of literature reviews, scientometric methods most often utilise software that positions and clusters terms, themes, and research directions based on algorithms, thus offering unbiased, transparent, and replicable results. These features provide robust and reliable results in mapping the literature. Scientometric methods, therefore, allow researchers to gain a bird's-eye perspective on the scholarship, in this case, automation in defence, where all published academic research on the topic is arranged under one map with distinct research streams.[23] Through this approach, the study of the themes and research streams will uncover those areas where research is abundant or limited, allowing a researcher to derive a deeper understanding of the subject's breadth and limitations and as a result, suggest avenues for more tailored research directions.[24]

Conduct of Research

Research method

A common saying is "we cannot see the forest for the trees", and therefore a big picture approach should be applied before we engage in in-depth study of a topic area. By providing a map of the scholarship and the clusters within, we can then see the entirety and complexity of the topic from an interdisciplinary perspective. Scientometric mapping with its taxonomies and typologies offered by review studies play an important role in many research disciplines and topics.[25] This study combines bibliometric author, publication, source, institution,

[20] Checkland, P 1999, *Systems thinking, systems practice*, John Wiley & Sons, New York.
[21] Jiang, H, Gai, J, Zhao, S, Chaudhry, PE & Chaudhry, SS 2022, 'Applications and development of artificial intelligence system from the perspective of system science: A bibliometric review', *Systems Research and Behavioral Science*, vol. 39, no. 3, pp. 361-78, Li, M, Xie, Y, Gao, Y & Zhao, Y ibid.'Organization virtualization driven by artificial intelligence', pp. 633-40.
[22] Nazarov, D & Klarin, A 2020, 'Taxonomy of Industry 4.0 research: Mapping scholarship and industry insights', ibid.vol. 37, no. 4, pp. 535-56, von Bertalanffy, L 1968, *General System Theory*, George Braziller, New York.
[23] Donthu, N, Kumar, S, Mukherjee, D, Pandey, N & Lim, WM 2021, 'How to conduct a bibliometric analysis: An overview and guidelines', *Journal of Business Research*, vol. 133, no. April, pp. 285-96, Klarin, A 2019, 'Mapping product and service innovation: A bibliometric analysis and a typology', *Technological Forecasting and Social Change*, vol. 149, p. 119776, Rafols, I, Leydesdorff, L, O'Hare, A, Nightingale, P & Stirling, A 2012, 'How journal rankings can suppress interdisciplinary research: A comparison between Innovation Studies and Business & Management', *Research Policy*, vol. 41, no. 7, pp. 1262-82.
[24] Ahmi, A, Elbardan, H & Raja Mohd Ali, RH 2019, 'Bibliometric analysis of published literature on Industry 4.0', *ICEIC 2019 - International Conference on Electronics, Information, and Communication*, pp. 1-6, Rossetto, DE, Bernardes, RC, Borini, FM & Gattaz, CC 2018, 'Structure and evolution of innovation research in the last 60 years: Review and future trends in the field of business through the citations and co-citations analysis', *Scientometrics*, vol. 115, no. 3, pp. 1329-63.
[25] Boyack, KW 2004, 'Mapping knowledge domains: Characterizing PNAS', *Proceedings of the National Academy of Sciences of the United States of America*, vol. 101, no. SUPPL. 1, pp. 5192-9.

keyword, and country-based analyses together with content-based analysis that is possible through an extraction and linkages of commonly occurring noun phrases to provide an overarching analysis of automation in defence literature.[26]

In conducting this scientometric review of the literature, this study was operationalised via the following steps: (1) identification of a research field and a research question, (2) identification of a review range, (3) establishing search criteria and data extraction, (4) results analysis and their interpretation, and (5) discussion of the results.[27]

Data analysis and visualisation was facilitated by the VOSviewer platform[28]. VOSviewer is capable of mapping large maps into distance-based clusters based on co-occurrence matrix, where items that have high similarities are algorithmically located close to each other are chosen for an unbiased outlook on the research.[29] A set of items that are closely related to each other are assigned to color-coded clusters, where each item can only occur in one cluster. This translates large maps into distance-based clusters based on a co-occurrence matrix where items that have high similarities are algorithmically located close to each other.[30] This approach provided an unbiased outlook on extant, published research. A set of items that are closely related to each other were assigned to colour-coded clusters with each item only occurring in one cluster.

Conduct of Research

This study began by identifying a dataset source with most the comprehensive and reliable results. Reliability of published work is typically ensured through a rigorous peer-to-peer review process. For the purposes of this research, publications indexed by Scopus were selected. Scopus is the world's largest bibliographic peer-to-peer publication extractable database, and the most established database for conducting scientometric reviews.[31] To afford a more holistic overview of the field, a large-sample thematic study of the entire scholarship is provided by utilising journal articles, books, book chapters, and conference proceedings.[32] This was applied to answer the question of *'What is the state-of-the-art of disruptive technologies (Cyber; Internet-of-Things (IoT) / Internet of Battlefield Things (IoBT); Artificial Intelligence (AI); Autonomous systems in defence and where do we go from here?*'.

In the second and third steps, we extracted all publications that contained relevant keywords in publications between 2016-2021 from Scopus. For example, this could include *"militar*" OR "department of defence" OR "department of defense" OR "defence department" OR "defense department" OR "defense industr*" OR "defence industr*" OR "defence sector*" OR "defense sector*" OR "army" OR "navy" OR "air force" OR "defence force*" OR "defense force*"*. The context search string was combined with the second search string : *"cyber" OR "Internet-of-Things" OR "Internet of Battlefield Things" OR "artificial intelligence" OR "autonomous" OR "automation"*.

In steps four and five, the data were analysed using VOSviewer software.

[26] Klarin, A, Inkizhinov, B, Nazarov, D & Gorenskaia, E 2021, 'International business education: What we know and what we have yet to develop', *International Business Review*, vol. 30, no. 5, p. 101833.
[27] Petticrew, M & Roberts, H 2006, *Systematic Reviews in the Social Sciences: A Practical Guide*, Blackwell Publishing, Oxford, Siddaway, AP, Wood, AM & Hedges, LV 2019, 'How to do a systematic review: A best practice guide for conducting and reporting narrative reviews, meta-analyses, and meta-syntheses', *Annual Review of Psychology*, vol. 70, pp. 747-70, Tranfield, D, Denyer, D & Smart, P 2003, 'Towards a methodology for developing evidence-informed management knowledge by means of systematic review', *British Journal of Management*, vol. 14, no. 3, pp. 207-22.
[28] www.vosviewer.com
[29] Korom, P 2019, 'A bibliometric visualization of the economics and sociology of wealth inequality: a world apart?', *Scientometrics*, vol. 118, no. 3, pp. 849-68, van Eck, N & Waltman, L 2009, 'Software survey: VOSviewer, a computer program for bibliometric mapping', ibid.vol. 84, no. 2, pp. 523-38, van Eck, NJ & Waltman, L 2014, 'Visualizing Bibliometric Networks', in Y Ding, R Rousseau & D Wolfram (eds), *Measuring Scholarly Impact: Methods and Practice*, Springer International Publishing, Cham, pp. 285-320.
[30] van Eck, N & Waltman, L 2009, 'Software survey: VOSviewer, a computer program for bibliometric mapping', *Scientometrics*, vol. 84, no. 2, pp. 523-38.
[31] Nazarov, D & Klarin, A 2020, 'Taxonomy of Industry 4.0 research: Mapping scholarship and industry insights', *Systems Research and Behavioral Science*, vol. 37, no. 4, pp. 535-56.
[32] van Eck, NJ & Waltman, L 2014, 'Visualizing Bibliometric Networks', in Y Ding, R Rousseau & D Wolfram (eds), *Measuring Scholarly Impact: Methods and Practice*, Springer International Publishing, Cham, pp. 285-320.

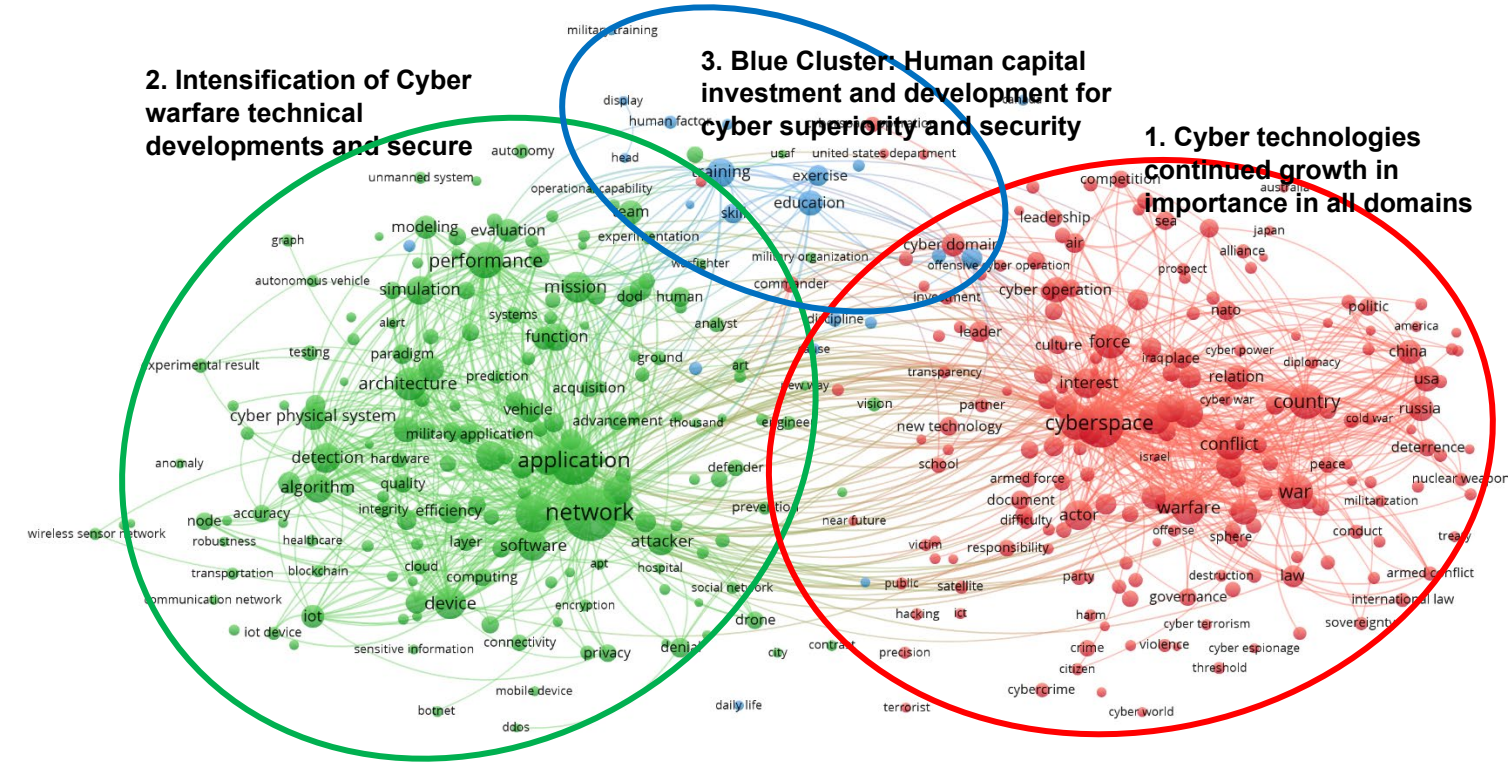
Results

In this section we explicate the findings under the four technology areas: Cyber, Internet-of-Things (IoT) / Internet of Battlefield Things (IoBT), Artificial Intelligence (AI), and Autonomous systems.

Cyber technologies

The dataset of 1,471 publications included in this scientometric review process on cyber technologies were algorithmically assigned into three research streams by the VOSviewer software (we note these as “clusters”): 1) the red cluster indicating cyber technologies continued growth in importance in all domains, 2) the green cluster denoting intensification of cyber warfare technical developments and secure solutions electronic warfare capabilities, and 3) the blue cluster highlighting the need for Human capital investment and development for cyber superiority and security (Figure 2.1).

Figure 2.1: The scientometric mapping of cyber technologies and defence scholarship



Red Cluster: Cyber technologies continued growth in importance in all domains

The research in this cluster concerns the systems of ensuring safe and secure environments as well as gaining strategic advantages through cyber warfare. Harknett and Smeets argue that cyberwar is increasingly replacing traditional warfare tactics to more strategically oriented outcomes without the need for military hostilities.[33]

Considering the developments in the field of combat systems, much research is devoted to developing resilient combat system-of-systems based on interconnections between multiple systems.[34] Ahmad et al. propose using disinformation as a response to cyberthreats to distort the situational awareness and decision-making of an attacking party, for example using twins and simulations to disorient or mislead attackers.[35]

[33] Harknett, RJ & Smeets, M 2020, 'Cyber campaigns and strategic outcomes', *Journal of Strategic Studies*, vol. 00, no. 00, pp. 1-34, ---- 2022, 'Cyber campaigns and strategic outcomes', *Journal of Strategic Studies*, vol. 45, no. 4, pp. 534-67.
[34] Li, J, Zhao, D, Ge, B, Jiang, J & Yang, K 2018, 'Disintegration of operational capability of heterogeneous combat networks under incomplete information', *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 12, pp. 5172-9.
[35] Ahmad, A, Webb, J, Desouza, KC & Boorman, J 2019, 'Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack', *Computers and Security*, vol. 86, pp. 402-18.

At the policy level, strategic competitiveness of countries is much dependent on cyberspace technologies including its security. Branch demonstrates how cyberspace is a new dominant domain comparable to land, water, air, and outer space.[36] Aggarwal and Reddie argue that the new economic statecraft that focuses on how government–firm relations affect geostrategic competitiveness replaces the old economic statecraft that depended on policies related to economic sanctions.[37] Deterring cyber-attacks on political states including voting systems requires policy responses, working with media, raising public awareness, and state cooperation in deterring these attacks.[38] Schneider explains how centralisation of nations' strategic systems creates vulnerabilities and room for cyberattacks, while less centralised and more resilient systems reduce these vulnerabilities.[39]

Countries ought to develop and maintain advanced industrial, scientific, and technological bases in order to remain competitive in today's technological environment especially considering cyber offensive and defensive systems. While emerging countries have demonstrated an impressive development of advanced technologies, Gilli and Gilli argue that there are significant entry barriers due to proprietary technologies, increased complexity, and increasingly tacit knowledge that is less likely to diffuse, all of which prevent technological catch-up of other countries to the US.[40]

Finally, there are only voluntary international rules and norms to govern cyberspace conflicts. Eilstrup-Sangiovanni argues that cyberwarfare potential is immense as shown in international incidents and that there is a dominance of cyber defence strategies, which in turn implies the need for an effective international agreement on cyber warfare.[41]

Green Cluster: Intensification of cyber warfare technical developments and secure solutions

There is an increasing intensification on leveraging on cyber technological developments for military operations. As such, Farooq and Zhu suggest an algorithm-based framework for secure and reconfigurable design of IoBT networks by adjusting deployment density of combat units or by changing transmission powers or both these options based on changing field conditions.[42] Pajic et al. demonstrate that machine's control systems (state estimators) need to be resilient in order to detect unusual performance of other components and processes.[43] Considering the rising requirement for resilient systems, cyber defence frameworks are becoming prevalent in the literature.[44]

While most static vulnerability analysis systems require available source code (which is generally not distributed for proprietary industrial IoT software) to detect software vulnerabilities, Liu et al. utilise deep learning mechanisms to detect vulnerabilities from the executable binary codes.[45] Machine learning techniques demonstrate superior results in malware detection in stacked long short-term memory (LSTM) as opposed to the standard LSTM methods.[46] Machine learning is further utilised to encrypt data including images to be used

[36] Branch, J 2021, 'What's in a name? Metaphors and cybersecurity', *International Organization*, vol. 75, no. 1, pp. 39-70.
[37] Aggarwal, VK & Reddie, AW 2020, 'New economic statecraft: Industrial policy in an era of strategic competition', *Issues and Studies*, vol. 56, no. 2, pp. 1-30.
[38] Hansen, I & Lim, DJ 2019, 'Doxing democracy: influencing elections via cyber voter interference', *Contemporary Politics*, vol. 25, no. 2, pp. 150-71.
[39] Schneider, J 2019, 'The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war', *Journal of Strategic Studies*, vol. 42, no. 6, pp. 841-63.
[40] Gilli, A & Gilli, M 2019, 'Why China has not caught up yet: Military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage', *International Security*, vol. 43, no. 3, pp. 141-89.
[41] Eilstrup-Sangiovanni, M 2018, 'Why the world needs an international cyberwar convention', *Philosophy and Technology*, vol. 31, no. 3, pp. 379-407.
[42] Farooq, MJ & Zhu, Q 2017, 'Secure and reconfigurable network design for critical information dissemination in the Internet of Battlefield Things (IoBT)', *arXiv*, vol. 17, no. 4, pp. 2618-32.
[43] Pajic, M, Weimer, J, Bezzo, N, Sokolsky, O, Pappas, GJ & Lee, I 2017, 'Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators', *IEEE Control Systems*, vol. 37, no. 2, pp. 66-81.
[44] Choi, S, Kwon, OJ, Oh, H & Shin, D 2020, 'Method for effectiveness assessment of electronic warfare systems in cyberspace', *Symmetry*, vol. 12, no. 12, pp. 1-16, Madan, BB, Banik, M & Bein, D 2019, 'Securing unmanned autonomous systems from cyber threats', *Journal of Defense Modeling and Simulation*, vol. 16, no. 2, pp. 119-36, Thompson, B & Morris-King, J 2018, 'An agent-based modeling framework for cybersecurity in mobile tactical networks', ibid.vol. 15, pp. 205-18.
[45] Liu, S, Dibaei, M, Tai, Y, Chen, C, Zhang, J & Xiang, Y 2020, 'Cyber vulnerability intelligence for internet of things binary', *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2154-63.
[46] Jahromi, AN, Hashemi, S, Dehghantanha, A, Parizi, RM & Choo, KKR 2020, 'An enhanced stacked LSTM method with no random initialization for malware threat hunting in safety and time-critical systems', *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 4, no. 5, pp. 630-40.

in IoT systems through statistical parameters to prevent cyber theft.[47] In general, deep/machine learning algorithms are deemed efficient at deterring cyberattacks.[48] For algorithms to be effective, the source of data and its quality are pertinent. Importantly, big data predictive analytics using security log data allow to predict and prevent cyberattacks.[49]

Gupta et al. suggest utilising blockchain technology for security, 5G networks to reduce latency, and artificial intelligence (AI) for automation of drones to secure against cyberattacks.[50] While much research has been evident in the past several years into the variety of intrusion detection systems (IDSs), it is shown that hybrid IDSs combining two or more detection systems (for example, signature and anomaly IDSs) are better at rates of detection of known and unknown threats.[51]

Finally, the game theory approach is an emergent methodology utilised to model defences and decision-making against cyberattacks.[52]

Blue Cluster: Human capital investment and development for cyber superiority and security

This smaller cluster represents research concerning training and education to reduce the risks and the impact of cyberattacks. Social engineering techniques, including spear phishing, baiting, and pretexting via people interactions, allow malicious attackers to breach security. As such, Ghafir et al. propose a security awareness training framework that allows a reduction in such threats, which includes monitoring the use of computers that send prompting informative messages, tracking statuses of training progress, and management of the training programs.[53] De Escalada Álvarez argues for the need to create and train cyber defence armies equal in capabilities to land, naval, and air counterparts.[54] Considering that some nations already have military development programs for cyber education, Knox et al. demonstrates how slow education techniques including reflective pondering, self-regulation, and metacognition provide significant positive impacts on cognitive agility in military cyberspace operations and in the hybrid space.[55] It is generally agreed that training and education play an increasingly important role in developing resilient cyber environments.[56]

---

[47] Shakya, AK, Ramola, A, Pokhariya, HS & Kandwal, A 2019, 'Fusion of IoT and machine learning approach to prevent confidential data from digital crimes and cyber mugging for covert transmission', in S Mishra, Y Sood & A Tomar (eds), pp. 563-79.

[48] Azmoodeh, A, Dehghantanha, A & Choo, KKR 2019, 'Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning', *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 88-95, Choudhary, G, Sharma, V & You, I 2019, 'Sustainable and secure trajectories for the military Internet of Drones (IoD) through an efficient Medium Access Control (MAC) protocol', *Computers and Electrical Engineering*, vol. 74, pp. 59-73, Ferdowsi, A, Challita, U & Saad, W 2019, 'Deep learning for reliable mobile edge analytics in intelligent transportation systems: An overview', *IEEE Vehicular Technology Magazine*, vol. 14, no. March, pp. 62-70.

[49] Amalina, F, Targio Hashem, IA, Azizul, ZH, Fong, AT, Firdaus, A, Imran, M & Anuar, NB 2020, 'Blending big data analytics: Review on challenges and a recent study', *IEEE Access*, vol. 8, pp. 3629-45, Landon-Murray, M 2016, *Big data and intelligence: Applications, human capital, and education*, vol. 9.

[50] Gupta, R, Kumari, A & Tanwar, S 2021, 'Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications', *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, pp. 1-20.

[51] Khraisat, A, Gondal, I, Vamplew, P, Kamruzzaman, J & Alazab, A 2020, 'Hybrid intrusion detection system based on the stacking ensemble of C5 decision tree classifier and one class support vector machine', *Electronics (Switzerland)*, vol. 9, no. 1, Stan, O, Cohen, A, Elovici, Y & Shabtai, A 2020, 'Intrusion detection system for the MIL-STD-1553 communication bus', *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 4, pp. 3010-27.

[52] Colbert, EJM, Kott, A & Knachel, LP 2020, 'The game-theoretic model and experimental investigation of cyber wargaming', *Journal of Defense Modeling and Simulation*, vol. 17, no. 1, pp. 21-38, Kusyk, J, Uyar, MU, Ma, K, Samoylov, E, Valdez, R, Plishka, J, Hoque, SE, Bertoli, G & Boksiner, J 2020, 'Artificial intelligence and game theory controlled autonomous UAV swarms', *Evolutionary Intelligence*, no. 0123456789, Shan, XG & Zhuang, J 2020, 'A game-theoretic approach to modeling attacks and defenses of smart grids at three levels', *Reliability Engineering and System Safety*, vol. 195, no. September 2019, pp. 106683-.

[53] Ghafir, I, Saleem, J, Hammoudeh, M, Faour, H, Prenosil, V, Jaf, S, Jabbar, S & Baker, T 2018, 'Security threats to critical infrastructure: the human factor', *Journal of Supercomputing*, vol. 74, no. 10, pp. 4986-5002.

[54] De Escalada Álvarez, Cg 2019, 'Online distance learning as a factor of disruptive innovation in military education', *Campus Virtuales*, vol. 8, no. 1, pp. 87-98.

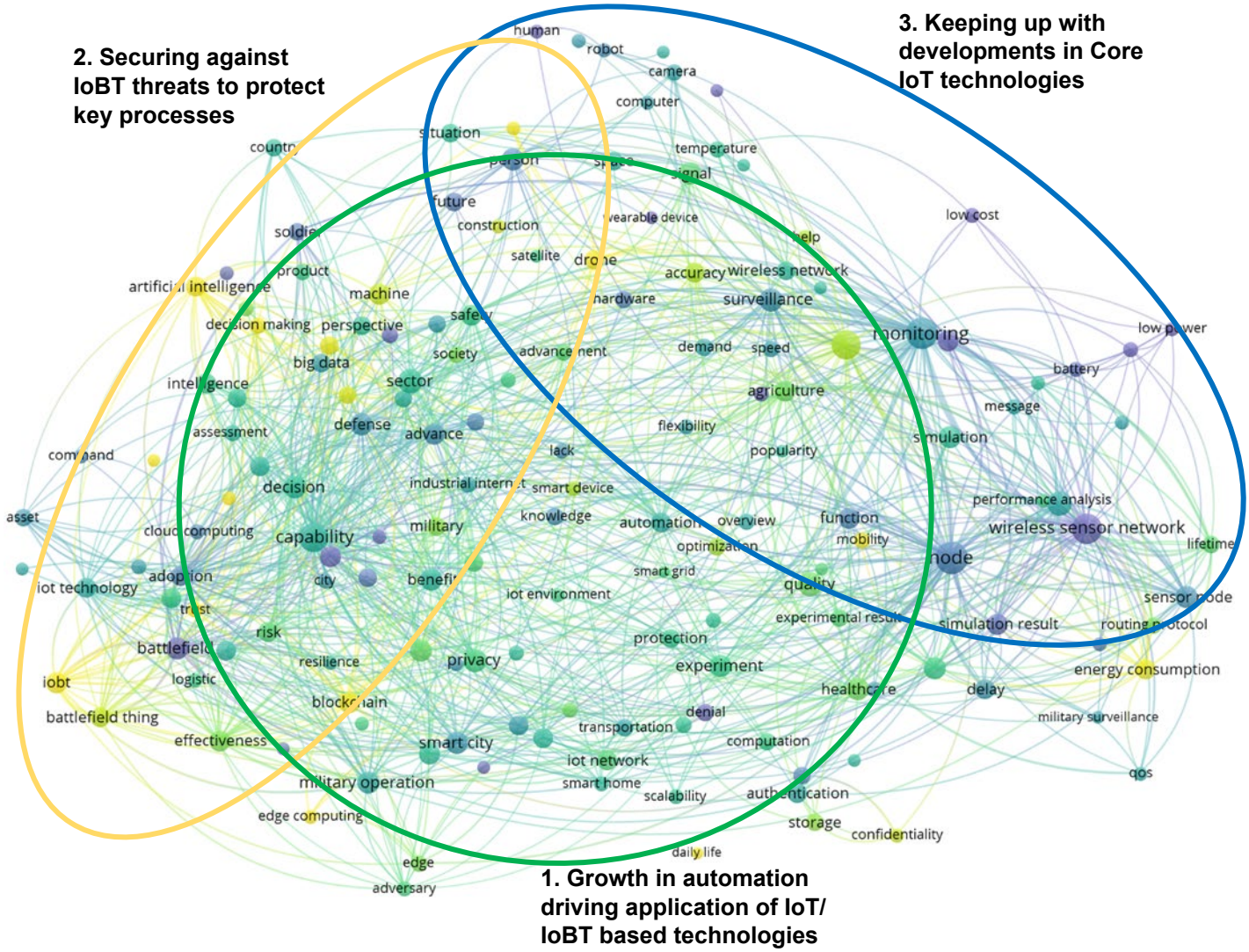
[55] Knox, BJ, Lugo, RG, Helkala, K & Sütterlin, S 2019, 'Slow education and cognitive agility: Improving military cyber cadet cognitive performance for better governance of cyberpower', *International Journal of Cyber Warfare and Terrorism*, vol. 9, no. 1, pp. 48-66.

[56] Jøsok, Ø, Knox, BJ, Helkala, K, Lugo, RG, Sütterlin, S & Ward, P 2016, 'Exploring the hybrid space', in D Schmorrow & C Fidopiastis (eds), Lecture No edn, Springer, Cham, pp. 178-88.

IoT/ IoBT

As IoT/ IoBT is a relatively newer and more specific term than cyber technologies, there were only 617 publications included in this scientometric review process. While cyber technologies had clear coloured clusters, the integrated nature of IoT/ IoBT technologies means that the clusters are less distinct algorithmically based on the VOSviewer software. There are three clusters of research streams: 1) the red cluster indicating cyber technologies continued growth in importance in all domains, 2) the green cluster denoting intensification of cyber warfare technical developments and secure solutions electronic warfare capabilities, and 3) the blue cluster highlighting the need for Human capital investment and development for cyber superiority and security (Figure B). This also points to important links and overlaps with cyber technologies.

Figure 2.2: The scientometric mapping of IoT/ IoBT technologies and defence scholarship



Green Cluster: Growth in automation driving application of IoT/ IoBT technologies

The most recent developments in autonomous flight systems i.e. unmanned aerial vehicles (UAVs)/drones, affect all sectors including agriculture, logistics, construction and the defence sector, and are currently trending in industry and research. With further development of algorithms and the resulting autonomy of these

technologies, research is intending to fully autonomise UAVs without the need for ground control systems.[57] At the intersection with the second research stream (ensuring secure IoBT), it is demonstrated that blockchain-based access control system allows secure communication between drones and ground station servers.[58]

A practical application of wearables is high on the agenda, and there is research into the development and utilisation demonstrates cost-effective and efficient carbon black and latex rubbers wearables that allow efficient nonverbal communication, which is of value to the military and civil applications.[59] Satellite technologies offer effective ways of communication in battlefield scenarios[60] that can offer superior IoT coverage[61], with research increasingly interested in the avoidance of satellite systems being compromised.[62] Developments in radar technologies allow portable radars that can be integrated into the Internet of Radars through the use of joint radar-communication system thus allowing communication between radars which is inevitable in the near future.[63]

The three streams of research intersect around one concept of automation of systems at the centre of the green cluster which is enabled via the IoT. As such research revolves around increasing automation of technologies in the IoBT, which requires security, privacy, and dependability.[64]

Other research may end up in the centre of the diagram in discussing topics that belong to each of the research streams. For example, swarm of UAVs (IoT technologies stream) technologies require blockchain distributed networks not only for security (ensuring secure IoBT), but also to purchase energy from charging stations (core IoT technologies), thus increasing security and cost-effectiveness.[65]

Yellow Cluster: Securing against IoBT threats to protect key processes

The yellow cluster shows that IoT/ IoBT, through its integration of sensors and decision-making platforms combined with automation facilitated by artificial intelligence, can form a major Achilles heel that can be targeted by hostile elements.

The interconnection between IoT/ IoBT and cyber technologies can be seen in that combat equipment and other battlefield resources require robustness and security against threats including cyber and physical warfare. A review study carried out by Zhu et al. finds that there are three common types of cyberattacks (single and multiple entry device hacking, UAV hacking, and collateral damage that involves systems outside the military) and three common defence types (comply to connect, blockchain, and AI defender systems).[66]

Most developed countries are commencing infrastructural developments into cloud computing which will facilitate the IoBT, which is prone to various cyber threats and thus calling for advanced security infrastructure.[67] As such, simulation results demonstrate that currently there are no standardised defence mechanisms against

[57] Han, J & Oh, D 2020, 'Fisheye-based smart control system for autonomous UAV operation', *Sensors (Switzerland)*, vol. 20, no. 24, pp. 1-19.
[58] Bera, B, Chattaraj, D & Das, AK 2020, 'Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment', *Computer Communications*, vol. 153, no. February, pp. 229-49.
[59] Ajeev, A, Javaregowda, BH, Ali, A, Modak, M, Patil, S, Khatua, S, Ramadoss, M, Kothavade, PA & Arulraj, AK 2020, 'Ultrahigh sensitive carbon-based conducting rubbers for flexible and wearable human–machine intelligence sensing', *Advanced Materials Technologies*, vol. 5, no. 12, pp. 1-10.
[60] Shuai, W, Han, Z & Yongli, Y 2018, 'Simulation and performance analysis of tactical battlefield communication network', *Proceedings of 2018 IEEE 3rd International Conference on Cloud Computing and Internet of Things, CCIOT 2018*, pp. 472-8.
[61] Routray, SK, Javali, A, Sahoo, A, Sharmila, KP & Anand, S 2020, 'Military applications of satellite based IoT', *Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology, ICSSIT 2020*, no. Icssit, pp. 122-7.
[62] Han, C, Liu, A, Wang, H, Huo, L & Liang, X 2020, 'Dynamic anti-jamming coalition for satellite-enabled army IoT: A distributed game approach', *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 10932-44, Kapalidis, C 2019, 'Cyber risk management in satellite systems', *IET Conference Publications*, vol. 2019, no. CP756, pp. 1-8.
[63] Akan, OB & Arik, M 2020, 'Internet of Radars: Sensing versus Sending with Joint Radar-Communications', *IEEE Communications Magazine*, vol. 58, no. 9, pp. 13-9.
[64] Pradhan, M & Noll, J ibid.'Security, privacy, and dependability evaluation in verification and validation life cycles for military IoT systems', no. 8, pp. 14-20.
[65] Hassija, V, Chamola, V, Krishna, DNG & Guizani, M 2020, 'A distributed framework for energy trading between UAVs and charging stations for critical applications', *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5391-402.
[66] Zhu, L, Majumdar, S & Ekenna, C 2020, 'An invisible warfare with the internet of battlefield things: A literature review', *Human Behavior and Emerging Technologies*, no. June, pp. 1-6.
[67] Koo, J, Oh, SR, Lee, SH & Kim, YG 2020, 'Security architecture for cloud-based command and control system in IoT environment', *Applied Sciences (Switzerland)*, vol. 10, no. 3.

these threats, and possible solutions include blockchain-based information exchanges[68] and the need to adjust the defence strategies in time to deal with threats.[69] Blockchain technology is further offered for the use in drone technologies for efficiencies, security and cost-effectiveness.[70] Increasingly machine learning is being utilised to counter evolving cyber security threats, for example, a deep recurrent neural network solution with a pre-training is used to neutralise malware[71], which points to the effectiveness of automated machine learning mechanisms as security systems against cyberattacks.[72]

The US Navy already utilises wireless communications and tagging technologies to track locations and other attributes of equipment, personnel, spaces, and other situational awareness scenarios.[73]

At the intersection of IoT in defence and Core IoT technologies, researchers realise the risks associated with the introduction of quantum computing in the future that poses threats to the security of IoT communications, and thus various solutions are offered for the quantum computing age implications.[74] Particle swarm optimisation algorithms are shown to perform better than generic and ant colony algorithms through a good IoT service combination, and can maintain load balance of smart devices that prolongs the entire network life cycle.[75]

Blue Cluster: Keeping up with developments in Core IoT technologies

This research aims to demonstrate the use of core technologies that underpin the IoT including sensors, wireless sensor networks (WSNs) and their effectiveness. As such, WSNs are able to detect threats including radiological pollutants that may deliberately or unintentionally be present in cost-effective and available technologies.[76] Underwater WSNs are gaining increasing attention in research as these assist civilian needs e.g. environmental protection and military needs like reconnaissance. Complex algorithms such as lossy and lossless data compression algorithms are proposed to prolong lifetime of underwater nodes, while Elliptic Curve-ElGamal and elliptic curve digital signature algorithms are proposed to ensure confidentiality, reliability, and integrity of data transmission.[77] Energy consumption[78] as well as data security (through, for example, Intelligent

[68] Sharma, A, Shoval, S, Sharma, A & Pandey, JK 2022, 'Path planning for multiple targets interception by the swarm of UAVs based on swarm intelligence algorithms: a review', *IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India)*, vol. 39, no. 3, pp. 675-97, Sobb, T, Turnbull, B & Moustafa, N 2020, 'Supply chain 4.0: A survey of cyber security challenges, solutions and future directions', *Electronics (Switzerland)*, vol. 9, no. 11, pp. 1-31, Yazdinejad, A, Parizi, RM, Dehghantanha, A, Zhang, Q & Choo, KKR 2020, 'An energy-efficient SDN controller architecture for IoT networks with blockchain-basedsecurity', *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 625-38.

[69] Feng, Y, Li, M, Zeng, C & Liu, H 2020, 'Robustness of internet of battlefield things (IoBT): A directed network perspective', *Entropy*, vol. 22, no. 10, pp. 1-15.

[70] Alladi, T, Chamola, V, Sahu, N & Guizani, M 2020, 'Applications of blockchain in unmanned aerial vehicles: A review', *Vehicular Communications*, vol. 23, pp. 100249-, Bera, B, Saha, S, Das, AK, Kumar, N, Lorenz, P & Alazab, M 2020, 'Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled internet of drones environment', *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9097-111, Ge, C, Ma, X & Liu, Z 2020, 'A semi-autonomous distributed blockchain-based framework for UAVs system', *Journal of Systems Architecture*, vol. 107, no. January, pp. 101728-.

[71] Jahromi, AN, Hashemi, S, Dehghantanha, A, Parizi, RM & Choo, KKR 2020, 'An enhanced stacked LSTM method with no random initialization for malware threat hunting in safety and time-critical systems', *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 4, no. 5, pp. 630-40.

[72] Liu, S, Dibaei, M, Tai, Y, Chen, C, Zhang, J & Xiang, Y 2020, 'Cyber vulnerability intelligence for internet of things binary', *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2154-63.

[73] Archer, D, August, MA, Bouloukakis, G, Davison, C, Diallo, MH, Ghosh, D, Graves, CT, Hay, M, He, X, Laud, P, Lu, S, Machanavajjhala, A, Mehrotra, S, Miklau, G, Pankova, A, Sharma, S, Venkatasubramanian, N, Wang, G & Yus, R 2020, 'Transitioning from testbeds to ships: an experience study in deploying the TIPPERS Internet of Things platform to the US Navy', *Journal of Defense Modeling and Simulation*.

[74] Fernandez-Carames, TM 2020, 'From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the internet of things', *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457-80.

[75] Zhu, X 2020, 'Energy optimization of the configurable service portfolio for IoT systems', *Computer Communications*, vol. 154, no. February, pp. 491-500.

[76] Lo Moriello, RS, Tocchi, A, Liccardo, A, Bonavolonta, F & De Alteriis, G 2020, 'Exploiting IoT-oriented technologies for measurement networks of environmental radiation', *IEEE Instrumentation and Measurement Magazine*, vol. 23, no. 9, pp. 36-42.

[77] Hu, C, Pu, Y, Yang, F, Zhao, R, Alrawais, A & Xiang, T 2020, 'Secure and efficient data collection and storage of IoT in smart ocean', *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9980-94.

[78] Zhang, J, Wu, Y, Min, G, Hao, F & Cui, L 2020, 'Balancing energy consumption and reputation gain of UAV scheduling in edge computing', *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 4, pp. 1204-17.

Personal Assistant software agents using privacy-preserving scheme)[79] of UAVs are an increasingly potent research direction to ensure autonomous UAVs operate securely, efficiently and cost-effectively.

Energy efficiencies of sensors is ever pertinent when discussing IoT networks, thus research and a consequent range of solutions is growing.[80] Such solutions include energy harvesting from radio frequencies in the surrounding environment to power the self-powered electronics in order to achieve safe, self-sufficient and maintenance-free systems.[81] Along these lines, IoT is famously vulnerable to jamming attacks due to hardware constraints and the broadcast nature of wireless communications, and various solutions are available in the literature, one of which is to leverage the power of advanced reactive jammers by creating fake transmissions, which not only undermines the jamming power but also harvests energy or utilises jamming signals as communication means.[82]

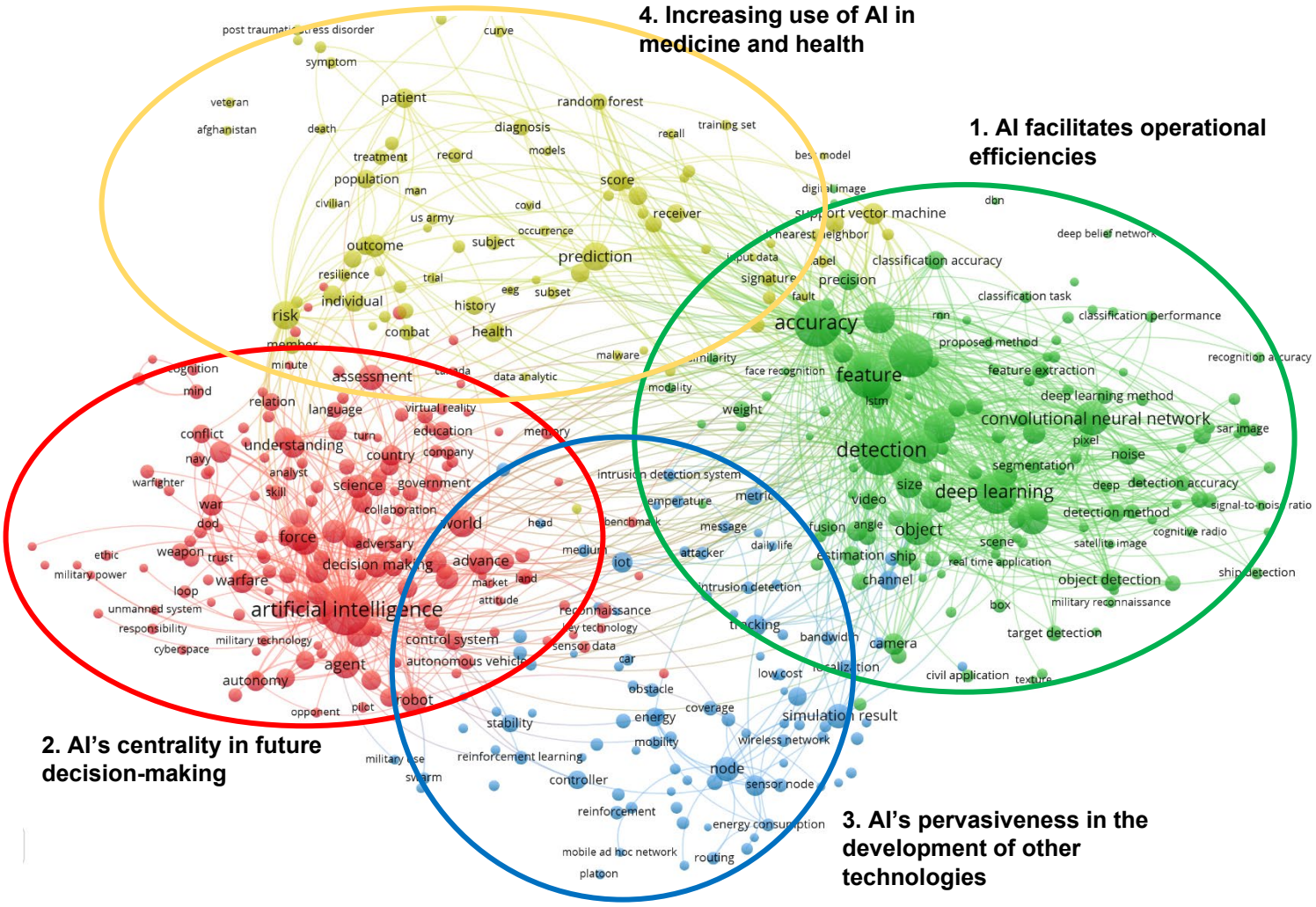
The need for miniaturisation of technologies drives researchers towards nano-scale experimentation, which inevitably will be the norm for civilian and military technologies thus creating the Internet of Nano-Things (IoNT).[83] IoNT research is in its nascent stages and is slowly but surely replacing the IoT.

Artificial Intelligence (AI)

Unsurprisingly, AI had the largest dataset of 2,189 publications included in this scientometric review process. AI technologies were algorithmically assigned into four research streams by the VOSviewer software: 1) the green cluster indicating AI as a facilitator of operational efficiencies, 2) the red cluster denoting AI's centrality in future decision-making, 3) the blue cluster highlighting AI's pervasiveness in the development of other technologies, and 4) the yellow cluster identifying the increasing use of AI in medicine and health (Figure 2.3).

[79] Deebak, BD & Al-Turjman, F 2020, 'A smart lightweight privacy preservation scheme for IoT-based UAV communication systems', *Computer Communications*, vol. 162, no. June, pp. 102-17.
[80] Dwivedi, AK, Sharma, AK & Mehra, PS 2020, 'Energy efficient sensor node deployment scheme for two stage routing protocol of wireless sensor networks assisted iot', *ECTI Transactions on Electrical Engineering, Electronics, and Communications*, vol. 18, no. 2, pp. 158-69.
[81] Ibrahim, HH, Singh, MSJ, Al-Bawri, SS & Islam, MT 2020, 'Synthesis, characterization and development of energy harvesting techniques incorporated with antennas: A review study', *Sensors (Switzerland)*, vol. 20, no. 10.
[82] Hoang, DT, Nguyen, DN, Alsheikh, MA, Gong, S, Dutkiewicz, E, Niyato, D & Han, Z 2019, '"Borrowing arrows with thatched boats": The art of defeating reactive jammers in IoT networks', *arXiv*, no. June, pp. 79-87.
[83] Chen, F, Wu, Y, Ding, Z, Xia, X, Li, S, Zheng, H, Diao, C, Yue, G & Zi, Y 2019, 'A novel triboelectric nanogenerator based on electrospun polyvinylidene fluoride nanofibers for effective acoustic energy harvesting and self-powered multifunctional sensing', *Nano Energy*, vol. 56, no. October 2018, pp. 241-51, Sicari, S, Rizzardi, A, Piro, G, Coen-Porisini, A & Grieco, LA 2019, 'Beyond the smart things: Towards the definition and the performance assessment of a secure architecture for the Internet of Nano-Things', *Computer Networks*, vol. 162, pp. 106856-, Sun, H, Yin, M, Wei, W, Li, J, Wang, H & Jin, X 2018, 'MEMS based energy harvesting for the Internet of Things: a survey', *Microsystem Technologies*, vol. 24, no. 7, pp. 2853-69.

Figure 2.3: The scientometric mapping of AI technologies and defence scholarship



Green cluster – AI facilitates operational efficiencies

This cluster is the largest cluster as it covers progress in AI technologies and how efficiencies are gained using these technologies. Below are some examples of how various technologies have been utilised.

Additive manufacturing technologies are increasingly important in the defence sector, to minimise defects that arise due to inherent features of the manufacturing process in additive manufacturing and Chen et al. demonstrate the effectiveness of DL techniques.[84]

Adversarial learning is becoming a pertinent topic of discussion since intelligent and adaptive adversaries may hinder the operations of ML systems by manipulating data. Miller et al. review various defence systems against these types of attacks including the need for human supervision of the process and data for the ML systems to actively learn from human behaviour.[85]

There are difficulties in the transmission of real time video from UAVs to operators, and Xiao et al. propose a sensor-augmented system that allows the delivery of adaptive bitrate algorithms with the assistance of sensor data that are used to pilot UAVs.[86] This system delivers a higher quality of video output.

[84] Chen, Y, Peng, X, Kong, L, Dong, G, Remani, A & Leach, R 2021, 'Defect inspection technologies for additive manufacturing', *International Journal of Extreme Manufacturing*, vol. 3, no. 2.
[85] Miller, DJ, Xiang, Z & Kesidis, G 2020, 'Adversarial learning targeting deep neural network classification: A comprehensive review of defenses against attacks', *Proceedings of the IEEE*, vol. 108, no. 3, pp. 402-33.
[86] Xiao, X, Wang, W, Chen, T, Cao, Y, Jiang, T & Zhang, Q 2020, 'Sensor-augmented neural adaptive bitrate video streaming on UAVs', *IEEE Transactions on Multimedia*, vol. 22, no. 6, pp. 1567-76.

Convolutional NNs (CNNs) are applied for general object recognition, and while access to large training data increases the accuracy of CNNs, in military applications this is often impractical. Yang et al. propose transference of learning data from an existing NN to a new NN upon which the new NN will build its knowledge relatively more efficiently and accurately, which is of significant value in the military sector.[87] Skeletal tracking of human movement using radars is important in civilian and military domains, as seen in the research by Sengupta et al. who utilised CNNs to predict movements in 3D space using radar-to-image representations.[88]

IoT devices are prone to cyberattacks, as shown by HaddadPajouh et al. who successfully utilised recurrent NN (RNN) deep learning to detect IoT malware, where Long Short Term Memory (LTSM) delivered the best possible detection results.[89]

Considering large training data and the need for time efficiencies in malware detection in IoBT, DNNs are impractical, thus research targets systems which are time and resource efficient in securing against malware are required.[90]

Red cluster – AI's centrality in future decision-making

Much of this cluster's discussions relate to increasing automation of decision-making (which also forms a major part of autonomous systems research covered in a separate analysis). We thus expand on the other themes prevalent in this cluster, namely international relations and political states related to AI and its development.

In general, a survey of AI experts predicts that in 45 years, there is a 50% chance that AI will outperform humans in all tasks and will automate all human jobs in 120 years, with tasks including language translation, essay writing, driving, and retail assistance replacing humans during the 2020s.[91] Jensen et al. argue that technological developments detach human agency and thus possess great risks. Preventing these risks involves educating decision makers and promoting accountability and responsible actions.[92] AI systems used in strategic sectors including defence are required to be transparent and trustworthy, thus naturally, the research is centred around the creation of explainable AI systems.[93]

Technological advancement is crucial in maintaining power in political relations. The rise of China and other emerging economies and their technological capabilities create a multipolar power world.[94] In the age of AI, we see the ever increasing role of informational warfare strategies complemented by military, political, economic, and civil instruments. Yan suggests that technological prowess has an immense potential in developing Defence and Security Ecosystems.[95] However, at the moment, the breadth of technological advances and dissemination does not provide any clear winners or losers. Instead, the AI race narrative creates risks for society as a whole, thus there is a need for multilateral treaties in regard to safeguarding international security.[96]

While AI-related strategic competitiveness is at its nascent stage, Raska contends that we are currently entering the sixth revolution in military affairs (RMA), with several nation states leading this research, including the US,

[87] Yang, Z, Yu, W, Liang, P, Guo, H, Xia, L, Zhang, F, Ma, Y & Ma, J 2019, 'Deep transfer learning for military object recognition under small training set condition', *Neural Computing and Applications*, vol. 31, no. 10, pp. 6469-78.
[88] Sengupta, A, Jin, F, Zhang, R & Cao, S 2020, 'mm-Pose: Real-time human skeletal posture estimation using mmWave radars and CNNs', *IEEE Sensors Journal*, vol. 20, no. 17, pp. 10032-44.
[89] HaddadPajouh, H, Dehghantanha, A, Khayami, R & Choo, KKR 2018, 'A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting', *Future Generation Computer Systems*, vol. 85, pp. 88-96.
[90] Namavar Jahromi, A, Hashemi, S, Dehghantanha, A, Choo, KKR, Karimipour, H, Newton, DE & Parizi, RM 2020, 'An improved two-hidden-layer extreme learning machine for malware hunting', *Computers and Security*, vol. 89.
[91] Grace, K, Salvatier, J, Dafoe, A, Zhang, B & Evans, O 2018, 'Viewpoint: When will ai exceed human performance? Evidence from ai experts', *Journal of Artificial Intelligence Research*, vol. 62, pp. 729-54.
[92] Jensen, BM, Whyte, C & Cuomo, S 2020, 'Algorithms at war: The promise, peril, and limits of artificial intelligence', *International Studies Review*, vol. 22, no. 3, pp. 526-50.
[93] La Gatta, V, Moscato, V, Postiglione, M & Sperlì, G 2021, 'CASTLE: Cluster-aided space transformation for local explanations', *Expert Systems with Applications*, vol. 179, no. August 2020, pp. 115045-.
[94] Johnson, J 2021, 'The end of military-techno Pax Americana? Washington's strategic responses to Chinese AI-enabled military technology', *Pacific Review*, vol. 34, no. 3, pp. 351-78.
[95] Yan, G 2020, 'The impact of Artificial Intelligence on hybrid warfare', *Small Wars and Insurgencies*, vol. 31, no. 4, pp. 898-917.
[96] Cave, S & ÓhÉigeartaigh, SS 2018, 'An AI race for strategic advantage: Rhetoric and risks', *AIES 2018 - Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, pp. 36-40, Garcia, D 2018, 'Lethal artificial intelligence and change: The future of international peace and security', *International Studies Review*, vol. 20, no. 2, pp. 334-41.

China, and Russia.[97] This AI-RMA results in a disruptive shift in warfare, in technology, practices, and organisational force structures. Turchin and Denkenberger provided a classification of potential risks to humanity associated with adoption of AI, which include risks related to human errors, AI errors, the relationship between AI and people, an interaction and lack of interaction between different agents across narrow, young, and mature AI systems.[98] Most of these risks will involve the defence sector in the process or the outcomes.

Blue Cluster– AI's pervasiveness in the development of other technologies

The blue cluster has the most overlap with the other clusters and points to AI's pervasiveness in the development of other technologies.

With the advent of IoT systems and applications in various spheres including IoBT, industrial IoT, and others Batth et al. propose Internet of Robotic Things classification that utilises mobile, flying, swarm, and humanoid robotic systems based on AI, cloud computing, IoT technologies.[99]

Latest research demonstrates interest in AI-based drone technologies. One such example is utilising deep reinforcement learning (DRL) systems in UAV technologies which demonstrates that autonomous path planning, navigation, and control are only at the experimental level (for example, indoor testing) and are currently being researched rather than applied (Azar et al., 2021). Nevertheless, researchers realise the potential of drone technologies in indoor environments for rescue operations and inventory tracking, thus autonomous operations are being proposed, and one such approach is using deep convolutional neural network (CNN)-based architecture (Chhikara et al., 2021). CNNs are also being tested for UAVs operating in traditional outdoor areas (Kraft et al., 2021). With the advent of technology, it is now possible to coordinate a number of UAVs using animal colony perception techniques based on ML to localise and track moving targets (Gu et al., 2018). Aadil et al. (2018) offer K-Means Density clustering algorithm which performs better than the current state-of-the-art Ant Colony and Grey Wolf Optimisation-based clustering algorithms in preserving energy and mobility of micro UAVs.

The IoT efficiencies are not only gained in aerial machines. Surface vehicles optimisation is also part of this cluster discussion. For example, autonomous vehicle platoon efficiencies will mean a better future for civilian and military safety and effectiveness of transportation. Hu et al. propose a two-layer distributed control scheme to maintain effective transmission of data and operation of autonomous vehicles moving in one direction and maintenance of constant spacing policy.[100]

Yellow cluster – Increasing use of AI in medicine and health

As much of non-military government-funded research is channelled into medical and health sciences, it is unsurprising that AI-based technologies have also featured in developments and publications in this field.

Digital technologies based on ML have a great potential in treating various medical conditions. For example, Germain et al. demonstrate the effectiveness of ML support systems and modern technologies that allow scalability and cost-effectiveness in treating insomnia based on a sample of military service personnel.[101] ML demonstrated superior detection of acute kidney injuries sustained while on military duty via tests on blood drawn from the patient, compared to traditional tests that utilise urine or creatinine samples.[102] Huang et al. demonstrate that DL neural network imaging techniques are more effective than traditional neuroimaging

[97] Raska, M 2020, 'The sixth RMA wave: Disruption in military affairs?', *Journal of Strategic Studies*, vol. 00, no. 00, pp. 1-24.
[98] Turchin, A & Denkenberger, D 2020, 'Classification of global catastrophic risks connected with artificial intelligence', *AI and Society*, vol. 35, no. 1, pp. 147-63.
[99] Batth, RS, Nayyar, A & Nagpal, A 2019, 'Internet of robotic things: Driving intelligent robotics of future - concept, architecture, applications and technologies', *Proceedings - 4th International Conference on Computing Sciences, ICCS 2018*, pp. 151-60.
[100] Hu, J, Bhowmick, P, Arvin, F, Lanzon, A & Lennox, B 2020, 'Cooperative control of heterogeneous connected vehicle platoons: An adaptive leader-following approach', *IEEE Robotics and Automation Letters*, vol. 5, no. 2, pp. 977-84.
[101] Germain, A, Markwald, RR, King, E, Bramoweth, AD, Wolfson, M, Seda, G, Han, T, Miggantz, E, O'Reilly, B, Hungerford, L, Sitzer, T, Mysliwiec, V, Hout, JJ & Wallace, ML 2021, 'Enhancing behavioral sleep care with digital technology: study protocol for a hybrid type 3 implementation-effectiveness randomized trial', *Trials*, vol. 22, no. 1, pp. 1-14.
[102] Rashidi, HH, Makley, A, Palmieri, TL, Albahra, S, Loegering, J, Fang, L, Yamaguchi, K, Gerlach, T, Rodriquez, D & Tran, NK 2021, 'Enhancing military burn- and trauma-related acute kidney injury prediction through an automated machine learning platform and point-of-care testing', *Archives of Pathology and Laboratory Medicine*, vol. 145, no. 3, pp. 320-6.

techniques in detecting brain injury related disabilities (tested on military personnel and veterans).[103] The authors recommended further longitudinal research on larger samples. Military personnel are considerably more prone to suicide compared to general population. Lin et al. utilised dix ML techniques (logistic regression, decision tree, random forest, gradient boosting regression tree, support vector machine, and multilayer perceptron) among which multilayer perceptron and support vector machines provide the best predictions of suicide ideation at 100% accuracy.[104]

Post-traumatic stress disorder (PTSD) is an acute issue in today's society, particularly in the military. Schultebraucks et al. demonstrate a possible ML prediction and prevention of deployment-related PTSD in the pre-deployment period by analysing neurocognitive, clinical, and biological markers of military personnel.[105] Leightley et al. demonstrate that self-reported PTSD is feasible and hence creates implications for a possibility for early intervention before the onset.[106]

Autonomous Systems

The increasing research and application of autonomous systems in defence has seen a concomitant rise in publications in this technology area. A total of 2,087 publications were included in this scientometric review process, slightly less than the publications in artificial intelligence. There are three clusters of research streams: 1) the red cluster indicating cyber technologies continued growth in importance in all domains, 2) the green cluster denoting intensification of cyber warfare technical developments and secure solutions electronic warfare capabilities, and 3) the blue cluster highlighting the need for Human capital investment and development for cyber superiority and security (Figure 2.4).

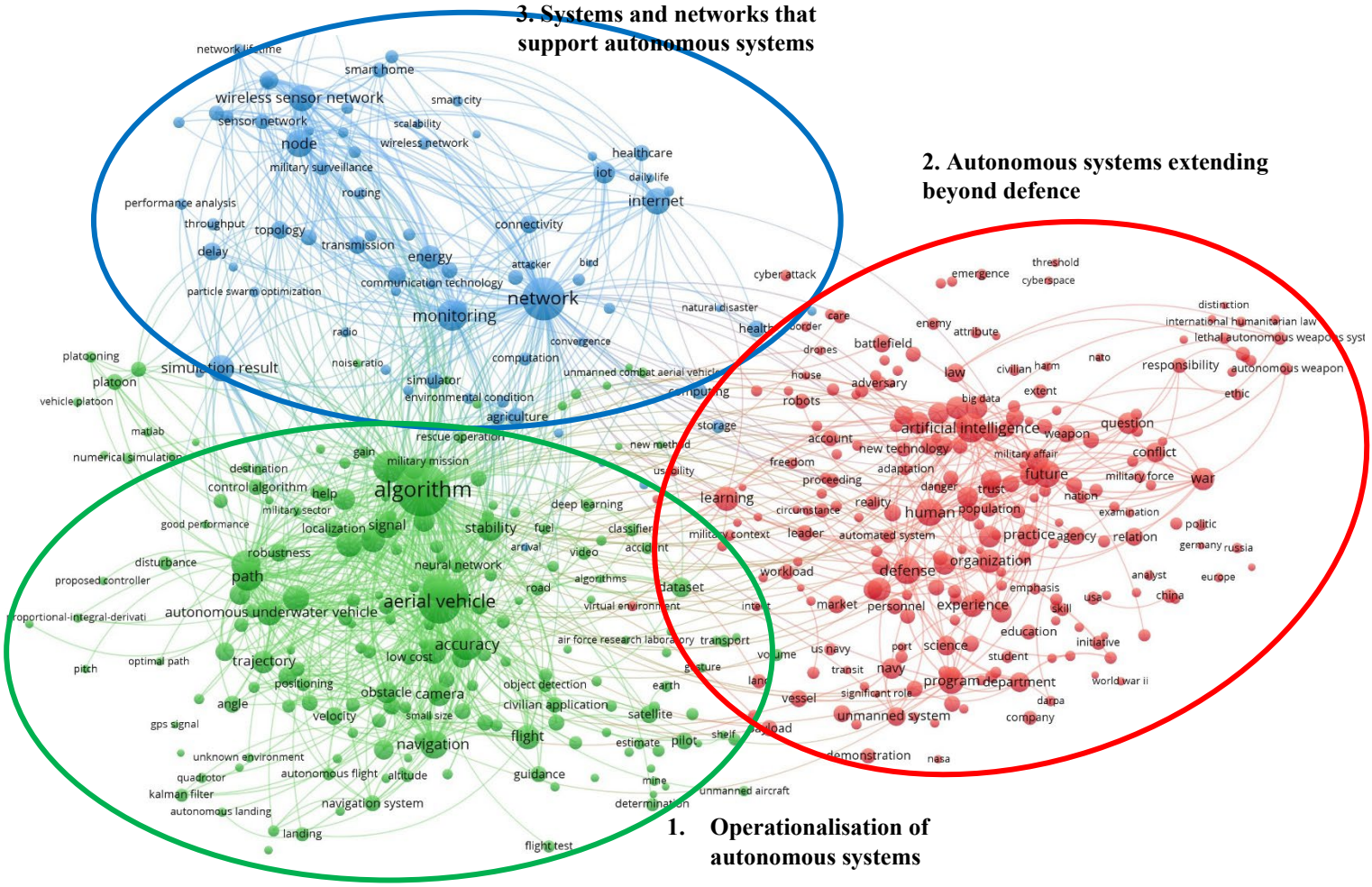
[103] Huang, MX, Huang, CW, Harrington, DL, Robb-Swan, A, Angeles-Quinto, A, Nichols, S, Huang, JW, Le, L, Rimmele, C, Matthews, S, Drake, A, Song, T, Ji, Z, Cheng, CK, Shen, Q, Foote, E, Lerman, I, Yurgil, KA, Hansen, HB, Naviaux, RK, Dynes, R, Baker, DG & Lee, RR 2021, 'Resting-state magnetoencephalography source magnitude imaging with deep-learning neural network for classification of symptomatic combat-related mild traumatic brain injury', *Human Brain Mapping*, vol. 42, no. 7, pp. 1987-2004.

[104] Lin, GM, Nagamine, M, Yang, SN, Tai, YM, Lin, C & Sato, H 2020, 'Machine learning based suicide ideation prediction for military personnel', *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 7, pp. 1907-16.

[105] Schultebraucks, K, Qian, M, Abu-Amara, D, Dean, K, Laska, E, Siegel, C, Gautam, A, Guffanti, G, Hammamieh, R, Misganaw, B, Mellon, SH, Wolkowitz, OM, Blessing, EM, Etkin, A, Ressler, KJ, Doyle, FJ, Jett, M & Marmar, CR 2020, 'Pre-deployment risk factors for PTSD in active-duty personnel deployed to Afghanistan: a machine-learning approach for analyzing multivariate predictors', *Molecular Psychiatry*.

[106] Leightley, D, Williamson, V, Darby, J & Fear, NT 2019, 'Identifying probable post-traumatic stress disorder: applying supervised machine learning to data from a UK military cohort', *Journal of Mental Health*, vol. 28, no. 1, pp. 34-41.

Figure 2.4: The scientometric mapping of autonomous systems technologies and defence scholarship



Green cluster – Operationalisation of autonomous systems

This cluster essentially discusses how autonomous systems are researched and developed, and which algorithms are utilised in the development of these systems and how they are utilised.

Autonomous systems come in all shapes and sizes, and as such, Kim et al. installed gas sensors on safety goggles that rapidly detect biological and chemical substances, which has great applicability in civilian and military sectors.[107] Coudron et al. developed a fully integrated portable air sampling platform, which shows strong potential toward future in-field deployable bio-detection systems being used in military and civil environments.[108] An automated convolutional network run on the Grey Wolf Optimisation algorithm is a state-of-the-art automatic identification software used in clinical imaging which is currently applied in detecting COVID-19 using X-ray images, and has great potential for both civilian and military use.[109] To enable the most efficient machine vision system for semantic recognition of objects and surroundings, Jalal et al. utilised modified Fuzzy C-Mean for the segmentation of object locations and recognition of scenes via Maximum Entropy thus reaching superior results over existing autonomous vision systems.[110] Considering the complexities of

[107] Kim, I, Kim, WS, Kim, K, Ansari, MA, Mehmood, MQ, Badloe, T, Kim, Y, Gwak, J, Lee, H, Kim, YK & Rho, J 2021, 'Holographic metasurface gas sensors for instantaneous visual alarms', *Science Advances*, vol. 7, no. 15.
[108] Coudron, L, McDonnell, MB, Munro, I, McCluskey, DK, Johnston, ID, Tan, CKL & Tracey, MC 2019, 'Fully integrated digital microfluidics platform for automated immunoassay; A versatile tool for rapid, specific detection of a wide range of pathogens', *Biosensors and Bioelectronics*, vol. 128, no. June 2018, pp. 52-60.
[109] Goel, T, Murugan, R, Mirjalili, S & Chakrabartty, DK 2021, 'OptCoNet: an optimized convolutional neural network for an automatic diagnosis of COVID-19', *Applied Intelligence*, vol. 51, no. 3, pp. 1351-66.
[110] Jalal, A, Ahmed, A, Rafique, AA & Kim, K 2021, *Scene semantic recognition based on modified Fuzzy C-mean and maximum entropy using object-to-object relations*.

autonomous vehicles, it becomes difficult to achieve successive waypoint tracking, so to solve this problem, Wang and Karimi proposed a bridging trajectory that could predict and track a completely autonomous system in unpredictable environments.[111]

Much research has been conducted in ensuring efficient and effective unmanned aerial vehicles (UAVs). Manoeuvrability of UAVs is a pertinent area of research, and as such, Yang et al. suggest an autonomous system based on deep reinforcement learning, where the simulation results demonstrate effective decision-making in short-range air combat situations.[112] Similarly, Xu et al. suggest reinforcement learning techniques and deep neural networks that allow autonomous aircraft morphing during all flight conditions including take-offs, landings, manoeuvring, hovering, attack, etc. based on the ability of birds to stretch wings and contract them dependent on the required action.[113] Yang et al. propose utilising hierarchical multi-objective evolutionary algorithm (HMOEA) that combines qualitative tactical experience and quantitative manoeuvre decision optimisation methods to effectively avoid air-to-air missile threats.[114] Ferdaus et al.'s review of autonomous quadcopters details comparisons of various fuzzy logic-based algorithms to advise on the current state-of-the-art technologies in controlling UAVs.[115]

When reviewing autonomous underwater vehicle (AUV) technologies, Panda et al. conclude that the catfish-, turtle-, and boxfish-shaped AUVs are currently the most effective designs that create minimum drag, maximum thrust, and highest propeller efficiency.[116] The review also shows that dynamic obstacle avoidance and formation switching are still under-researched. Rahmati and Pompili offer a probabilistic space division multiple access method that considers the angular position of other AUVs via a two-step estimation and by keeping the transmitter antenna's beamwidth of each AUV at an optimal value to ensure an effective coordination of AUVs in distances up to 2 kms.[117]

A review of robots and their operation concluded that along with a good network, visual and force feedback are necessary for operators to feel present in the robot's environment for the best situational awareness and efficient use.[118] Budiharto et al. propose utilising PID controllers on military robots that actively search for the best position to eliminate threats based on the upper body positioning of a target.[119]

Red cluster – Autonomous systems extending beyond defence

The early developers and users of autonomous systems have largely been in defence-related fields (e.g. UAVs, bomb disposal robots). However, as this cluster shows, autonomous systems development has extended rapidly to other fields and has a growing impact on countries, international relations, and society in general.

We begin with an insightful special issue by Lawless et al. that discuss human-machine teams that are necessary to deliver explainable AI and ensure trust within the society.[120] The authors argue that it is possible to estimate the amount of interaction between humans and machines mathematically to prevent unethical outcomes and ensure maximised operational efficiency. For example, for safety measures, the machines will

[111] Wang, N & Karimi, HR 2020, 'Successive waypoints tracking of an underactuated surface vehicle', *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 898-908.
[112] Yang, Z, Zhou, D, Piao, H, Zhang, K, Kong, W & Pan, Q 2020, 'Evasive maneuver strategy for UCAV in beyond-visual-range air combat based on hierarchical multi-objective evolutionary algorithm', *IEEE Access*, vol. 8, pp. 46605-23.
[113] Xu, D, Hui, Z, Liu, Y & Chen, G 2019, 'Morphing control of a new bionic morphing UAV with deep reinforcement learning', *Aerospace Science and Technology*, vol. 92, pp. 232-43.
[114] Yang, Z, Zhou, D, Piao, H, Zhang, K, Kong, W & Pan, Q 2020, 'Evasive maneuver strategy for UCAV in beyond-visual-range air combat based on hierarchical multi-objective evolutionary algorithm', *IEEE Access*, vol. 8, pp. 46605-23.
[115] Ferdaus, MM, Anavatti, SG, Pratama, M & Garratt, MA 2020, 'Towards the use of fuzzy logic systems in rotary wing unmanned aerial vehicle: a review', *Artificial Intelligence Review*, vol. 53, no. 1, pp. 257-90.
[116] Panda, JP, Mitra, A & Warrior, HV 2021, 'A review on the hydrodynamic characteristics of autonomous underwater vehicles', *Proceedings of the Institution of Mechanical Engineers Part M: Journal of Engineering for the Maritime Environment*, vol. 235, no. 1, pp. 15-29.
[117] Rahmati, M & Pompili, D 2020, 'Probabilistic spatially-divided multiple access in underwater acoustic sparse networks', *IEEE Transactions on Mobile Computing*, vol. 19, no. 2, pp. 405-18.
[118] Opiyo, S, Zhou, J, Mwangi, E, Kai, W & Sunusi, I 2021, 'A review on teleoperation of mobile ground robots: Architecture and situation awareness', *International Journal of Control, Automation and Systems*, vol. 19, no. 3, pp. 1384-407.
[119] Budiharto, W, Irwansyah, E, Suroso, JS & Gunawan, AAS 2020, 'Design of object tracking for military robot using PID controller and computer vision', *ICIC Express Letters*, vol. 14, no. 3, pp. 289-94.
[120] Lawless, WF, Mittu, R, Sofge, D & Hiatt, L 2019, 'Artificial intelligence, autonomy, and human-machine teams: Interdependence, context, and explainable ai', *AI Magazine*, vol. 40, no. 3, pp. 5-13.

be programmed to intervene when human operators are deemed unfit, for example in situations of deliberate harm such as suicide, or when humans get distracted or experience such other issues.

Autonomous Weapon Systems (AWSs) are rapidly developing, thus accountability for AWSs' actions are to be distributed on three major levels – technical, socio-technical, and governance - to ensure solid accountability and controllability of the deployment of AWSs.[121] Others opine that AWSs violate human dignity, but this is not the only reason why these systems should be scrutinised in their use including conformity to humanitarian laws, the need for human judgement in lethal situations, and the ability of AWSs to cause global instabilities.[122] Horowitz discusses the implications of the use of lethal autonomous weapons systems (LAWS) by nations, where it is difficult to control whether nations utilise these technologies or not.[123] Even if regulation against the use of such systems prevails, it is unlikely there will be complete elimination of such use as it is difficult to prove the use or the absence of such systems. Therefore, this is an interesting and critical area for future strategic research.

France's involvement in international affairs is at its highest level, and the country realises the importance of international strategic cooperation with other countries, including Australia, in navigating the turbulent environment, whilst at the same time integrating AI systems for defence.[124]

Drone technologies have wide implications for both military and civilian uses. As such, Poljak and Šterbenc predict a gradual increase in the use of drones for medical transportation purposes due to significant advantages in costs and effectiveness in the near future.[125] With advancements in technology, it is now possible to create military wearables with autonomous pixels that serve as cloaking devices for both visible and infra-red spectra by reading the environment and temperature to effectively merge with the environment.[126]

Blue cluster – Systems and networks that support autonomous systems

This cluster discusses communication networks and the related research in the operation of autonomous systems.

Wireless sensor networks (WSNs) are usually static and thus result in coverage redundancy and coverage holes. Mobile WSNs are proposed that operate using particle swarm optimisation that allows them to remain static or go to sleep modes and awaken when required.[127] A reliable and energy efficient routing of mobile WSNs is achieved through dynamic directional routing (DDR), which demonstrates an enhanced packet delivery rate and energy consumption and shows improvement in network lifetime by 13% and maintains shorter routes towards sink by 33% when compared to the state-of-the-art T-LEACH protocol.[128]

WSNs require state-of-the-art batteries, and Sah and Amgoth suggest and review various methods of using renewable energy harvesting systems including solar and wind, which are necessary for autonomous systems development. Underwater acoustic sensor networks (UASNs) are used for data collection in monitoring, auxiliary navigation, and military defence.[129] However, as UASNs are prone to inefficiencies and errors, Han et al. propose a district partition-based data collection algorithm with event dynamic competition, which essentially

[121] Verdiesen, I, Santoni de Sio, F & Dignum, V 2021, 'Accountability and control over autonomous weapon systems: A framework for comprehensive human oversight', *Minds and Machines*, vol. 31, no. 1, pp. 137-63.
[122] Sharkey, A 2019, 'Autonomous weapons systems, killer robots and human dignity', *Ethics and Information Technology*, vol. 21, no. 2, pp. 75-87.
[123] Horowitz, MC 2019, 'When speed kills: Lethal autonomous weapon systems, deterrence and stability', *Journal of Strategic Studies*, vol. 42, no. 6, pp. 764-88.
[124] Pannier, A & Schmitt, O 2019, 'To fight another day: France between the fight against terrorism and future warfare', *International Affairs*, vol. 95, no. 4, pp. 897-916.
[125] Poljak, M & Šterbenc, A 2020, 'Use of drones in clinical microbiology and infectious diseases: current status, challenges and barriers', *Clinical Microbiology and Infection*, vol. 26, no. 4, pp. 425-30.
[126] Lee, J, Sul, H, Jung, Y, Kim, H, Han, S, Choi, J, Shin, J, Kim, D, Jung, J, Hong, S & Ko, SH 2020, 'Thermally controlled, active imperceptible artificial skin in visible-to-infrared range', *Advanced Functional Materials*, vol. 30, no. 36, pp. 1-11.
[127] Wang, J, Ju, C, Kim, Hj, Sherratt, RS & Lee, S 2019, 'A mobile assisted coverage hole patching scheme based on particle swarm optimization for WSNs', *Cluster Computing*, vol. 22, no. s1, pp. 1787-95.
[128] Almesaeed, R & Jedidi, A 2021, 'Dynamic directional routing for mobile wireless sensor networks', *Ad Hoc Networks*, vol. 110, no. September 2020, pp. 102301-.
[129] Sah, DK & Amgoth, T 2020, 'Renewable energy harvesting schemes in wireless sensor networks: A Survey', *Information Fusion*, vol. 63, no. July, pp. 223-47.

demonstrates a significant reduction in energy consumption to guarantee load balancing whilst reducing transmission delays.[130]

Communication amongst autonomous vehicles suffers from information congestion and interferences, and as such Wang et al. propose a cooperative adaptive cruise control (CACC) technology based on an optimised information flow topology (IFT), which optimise the platoon's performance in terms of string stability under ambient traffic conditions.[131] Li et al. propose a reliable consensus-based cooperative control for multi-platoons of connected vehicles.[132]

Smart transportation based on IoT technologies continues to improve due to the significant amount of research being undertaken in this area. Paranjothi et al., for example, offer a superior congestion-aware load-balancing routing algorithm that uses statistical inference to analyse congestion and thus derive the best results in vehicle communication, driver safety, traffic efficiency, which pave the way for full automation of transport.[133]

Scientometric study summary

Besides providing a review of the four main technology areas (Cyber, IoT/IoBT, AI, and Autonomous Systems), the scientometric review also identified eleven specific technologies or technology trends that merit further exploration as follows:

1. Cyber Security of critical infrastructure;
2. Network Communications and Information technologies (e.g. for the mission design, structure, and operations);
3. Swarm intelligence-related technologies and systems;
4. Industry 4.0 technologies where the cyber-physical domains merge;
5. Unmanned and autonomous systems;
6. Optimisation and other algorithms;
7. Neural Networks;
8. Smart Sensors;
9. Deep/Machine Learning;
10. Civil and military R&D and uses of these technologies; and
11. Convergence of technologies in strategic industries that support any phases of military operation

These technologies and trends are related to the four main technology areas and they were incorporated into the survey questionnaire as part of Study 2.

[130] Han, G, Tang, Z, He, Y, Jiang, J & Ansere, JA 2019, 'District partition-based data collection algorithm with event dynamic competition in underwater acoustic sensor networks', *IEEE Transactions on Industrial Informatics*, vol. 15, no. 10, pp. 5755-64.
[131] Wang, C, Gong, S, Zhou, A, Li, T & Peeta, S 2020, 'Cooperative adaptive cruise control for connected autonomous vehicles by factoring communication-related constraints', *Transportation Research Part C: Emerging Technologies*, vol. 113, no. November 2018, pp. 124-45.
[132] Li, Y, Tang, C, Li, K, He, X, Peeta, S & Wang, Y 2019, 'Consensus-based cooperative control for multi-platoon under the connected vehicles environment', *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 6, pp. 2220-9.
[133] Paranjothi, A, Khan, MS, Patan, R, Parizi, RM & Atiquzzaman, M 2020, 'VANETomo: A congestion identification and control scheme in connected vehicles using network tomography', *Computer Communications*, vol. 151, no. December 2019, pp. 275-89.

Chapter 3 - Study 2: Survey Research Study

Introduction

Effective horizon scanning combines tools, methods and networks to collect and analyse weak signals and emerging issues.[134] These may include web-based searches, expert reviews, surveys, visits to conferences and seminars, active use of blogging and/or micro-blogging, text-mining, and stakeholder workshops among other methods.[135] The scientometric study involved the combination of web-based search (using the Scopus database) and text-mining. To complement this and informed by Study 1, the second study involved a survey of 415 respondents.

Conduct of research

Survey development and data collection

The survey questionnaire (see Appendix 1) was adapted from research conducted by the University of Hamburg's Institute of Peace Research and Security Policy (IFSH)[136]. It asked various industry professionals with relevant experience in these technology areas or fields to evaluate the potential impact, likelihood of deployment / utilisation, extensiveness of use, and novelty of use of the four general technology areas mentioned above in future conflicts.

However, the IFSH study did not identify potential insights with reference to timeframes, an important aspect of horizon scanning.[137] Horizon scanning should deliver insights and pinpoint potential challenges within a timeframe that is appropriately distanced from the present—neither too remote nor too immediate—to effectively fulfill the purpose of the exercise. To address this, the questionnaire also elicited responses as to the timeliness of development of these technologies in the future (near term: less than 5 years, medium term: 5-10 years, long term: more than 10 years). In addition, respondents were also asked about their perceptions of capability gaps within the ADF in these technologies and where defence forces like the ADF should be investing in the future.

There were also few open-ended questions that allowed respondents to discuss what were technologies that the survey did not cover but should be considered.

Following the method of participant recruitment widely recognised in the social sciences research among private and public-sector professionals[138], we engaged with PureProfile, an Australian-based research company, to send out our surveys to a panel which was selected from the following three industry fields.

1. Science, technology, engineering and mathematics (STEM);
2. Law enforcement, defence, security or emergency services; and
3. Information and communication technology (ICT)

[134] Könnölä, T, Salo, A, Cagnin, C, Carabias, V & Vilkkumaa, E 2012, 'Facing the future: Scanning, synthesizing and sense-making in horizon scanning', *Science and Public Policy*, vol. 39, no. 2, pp. 222-31.
[135] Amanatidou, E, Butter, M, Carabias, V, Könnölä, T, Leis, M, Saritas, O, Schaper-Rinkel, P & van Rij, V ibid.'On concepts and methods in horizon scanning: Lessons from initiating policy dialogues on emerging issues', pp. 208-21.
[136] Favaro, M, Renic, N & Kühn, U 2022, *Negative multiplicity: Forecasting the future impact of emerging technologies on international stability and human security*, Institute of Peace Research and Security Policy at the University of Hamburg, Hamburg.
[137] Tsakalidis, A, Boelman, E, Marmier, A, Gkoumas, K & Pekar, F 2021, 'Horizon scanning for transport research and innovation governance: A European perspective', *Transportation Research Interdisciplinary Perspectives*, vol. 11, p. 100424.
[138] Lux, AA, Grover, SL & Teo, STT 2023, 'Reframing commitment in authentic leadership: Untangling relationship–outcome processes', *Journal of Management & Organization*, vol. 29, no. 1, pp. 103-21, Pugh, SD, Groth, M & Hennig-Thurau, T 2011, 'Willing and able to fake emotions: a closer examination of the link between emotional dissonance and employee well-being', *Journal of Applied Psychology*, vol. 96, no. 2, p. 377, Teo, STT, Pick, D, Xerri, M & Newton, C 2016, 'Person–Organization Fit and Public Service Motivation in the Context of Change', *Public Management Review*, vol. 18, no. 5, pp. 740-62.

Data was collected from 415 industry professionals.

In addition, six experts with extensive experience in these fields and defence were also surveyed.

Quantitative data analysis

Besides categorical data analysis, cross-tabulation analysis was carried out on the data.[139] Cross-tabulations have been recommended as useful in horizon scanning for visualising data analyses in understanding the relationship of technologies or issues identified with other factors like timeliness.[140]

Qualitative data analysis

Thematic content analysis is the systematic process of identifying and reporting textual meanings, consistencies and patterns in qualitative data.[141] Furthermore, thematic content analysis assists in identifying true meanings attached to qualitative data.[142] This type of analysis involves identifying recurring themes or patterns that may provide insight into the research questions or topics under investigation. The focus is on allowing themes to emerge from the data itself in this process.

Several recent studies have revealed that the use of computer assisted qualitative data analysis software (CAQDAS), such as Leximancer, reduces the researcher's bias compared to manual methods.[143] In addition, using a computer driven tool, such as Leximancer, enables effective analysis of the data by reducing the epistemological influence of the researcher. Therefore, to explore the qualitative dataset for key thematic insights, a machine-learning based program, Leximancer, was used in this research.

Leximancer is a qualitative, machine-driven, AI-based, data analysis tool which is used for text mining, thematic and content analysis. It uses a Bayesian algebra-based algorithm to seed word definitions through an iterative process assessing the frequency and co-occurrence of words within the dataset. It identifies key concepts and clusters of concepts which form themes. Leximancer identifies frequencies and co-occurrences of words in text blocks, through an iterative process of seeding word definitions.[144] Primarily, Leximancer recognises key themes in big qualitative data sets, maps the linkage between themes and concepts, and generates a visual concept map.[145] In the concept map, themes are colour coded from hottest to coolest, where red represents the most prominent or hot theme and purple represents the least prominent or cool theme.[146] Notably, Leximancer has the ability to extract insights from unstructured texts using natural language processing techniques.

The results of the Leximancer analysis are shown in the Insight Dashboard Report (Table 3). This includes prominence scores (PS) for both, ranked single key concepts and compound concepts, where PS equal to or above 1 for single key concepts and PS equal to or above 3 for compound concepts, is deemed satisfactory.[147]

---

[139] Momeni, A, Pincus, M & Libien, J 2018, 'Cross Tabulation and Categorical Data Analysis', in *Introduction to Statistical Methods in Pathology*, Springer International Publishing, Cham, pp. 93-120.
[140] Hines, A, Baldwin, BP, Bengston, DN, Crabtree, J, Christensen, K, Frankowski, N, Schlehuber, L, Westphal, LM & Young, L 2021, 'Monitoring Emerging Issues: A Proposed Approach and Initial Test', *World Futures Review*, vol. 13, no. 3-4, pp. 195-213.
[141] Neuendorf, KA 2018, 'Content analysis and thematic analysis', in *Advanced research methods for applied psychology*, Routledge, pp. 211-23.
[142] Angus, D, Rintel, S & Wiles, J 2013, 'Making sense of big text: a visual-first approach for analysing text data using Leximancer and Discursis', *International Journal of Social Research Methodology*, vol. 16, no. 3, pp. 261-7.
[143], Wilk, V, Soutar, GN & Harrigan, P 2019, 'Tackling social media data analysis', *Qualitative Market Research: An International Journal*, vol. 22, no. 2, pp. 94-113.
[144] Angus, D, Rintel, S & Wiles, J 2013, 'Making sense of big text: a visual-first approach for analysing text data using Leximancer and Discursis', *International Journal of Social Research Methodology*, vol. 16, no. 3, pp. 261-7, Wilk, V, Soutar, GN & Harrigan, P 2019, 'Tackling social media data analysis', *Qualitative Market Research: An International Journal*, vol. 22, no. 2, pp. 94-113.
[145] Krishen, AS & Petrescu, M 2017, 'The world of analytics: interdisciplinary, inclusive, insightful, and influential', *Journal of Marketing Analytics*, vol. 5, no. 1, pp. 1-4.
[146] Leximancer 2024, LexiPortal 5 User Guide, Available at: https://www.leximancer.com/resources, Accessed on: 1.03.2024.
[147] Wilk, V, Soutar, GN & Harrigan, P 2019, 'Tackling social media data analysis', *Qualitative Market Research: An International Journal*, vol. 22, no. 2, pp. 94-113.

Results: Survey Research Study

Profile of respondents

Main survey panel

The original sample of respondents in the quantitative study was 425 respondents. However, 10 were incomplete and therefore excluded, leaving a total usable sample of 415. A detailed description of the demographic profile of the participants is presented in Table 3.1.

Table 3.1 – Summary of personal profile characteristics of the respondents.

Personal Profile	Category	Respondents	%
Industry of work	Information or communication technology (ICT)	191.00	46.02
	Law enforcement, defence, security or emergency services	70.00	16.87
	Postal & Telecommunications	35.00	8.43
	Science, technology, engineering, mathematics (STEM)	119.00	28.67
Number of years of experience in the industry	< 2 years	38.00	9.16
	2-5 years	109.00	26.27
	6-10 years	96.00	23.13
	10+ years	172.00	41.45
Technology-related area of expertise	Cyber/ ICT	168.00	40.48
	Artificial Intelligence (AI)	26.00	6.27
	The Internet-of-(battlefield)-things (IoT/IoBT)	21.00	5.06
	Autonomous Systems	12.00	2.89
	Defence	14.00	3.37
	Engineering	41.00	9.88
	Law enforcement or Emergency Services	50.00	12.05
	Science	48.00	11.57
	Other (please specify)	35.00	8.43
Current age	18-24 years	37.00	8.92
	25-34 years	113.00	27.23
	35-44 years	115.00	27.71
	45-54 years	74.00	17.83
	55-64 years	49.00	11.81
	65+ years	27.00	6.51
Gender	Male	148	35.66
	Female	264	63.61
	Prefer not to tell	3	0.72
Current place of residence	Australia	257.00	61.93
	Canada	86.00	20.72
	USA	29.00	6.99
	Other	44	10.36
Highest educational level	Doctorate	12.00	2.89
	Postgraduate Degree	126.00	30.36
	Undergraduate Degree	153.00	36.87
	Diploma	46.00	11.08
	Technical or Trade Qualification	38.00	9.16
	High school graduate	37.00	8.92
	Less than high school	3.00	0.72

Most of the respondents are in the ICT (46%) or STEM (29%) industries. However, there were 17% who had law enforcement, defence, security or emergency services experience. A large proportion (41%) had significant experience in their industry (>10 years). In terms of technology experience, the largest group (41%) had Cyber/ ICT experience. Most of the respondents were from Australia but about 38% were from other countries (mainly Canada and the USA). About 70% had a university degree or higher education.

Expert respondents

To validate our survey findings and for deeper insights, a small expert group of six respondents with significant experience in defence and/or technology was sourced. Table 3.2 below provides a description of the sample.

Table 3.2 – Summary of personal profile characteristics of the expert respondents.

Personal Profile	Category	Respondents	%
Industry of work	Information or communication technology (ICT)	3	50
	Defence	3	50
Number of years of experience in the industry	6-10 years	3	50
	10+ years	3	50
Technology-related area of expertise	Cyber/ ICT	2	33.3
	The Internet-of-(battlefield)-things (IoT/IoBT)	1	16.7
	Autonomous Systems	1	16.7
	Defence	2	33.3
Current age	45-54 years	4	66.7
	55-64 years	2	33.3
Gender	Male	6	100
Current place of residence	Australia	3	50
	Singapore	2	33.3
	Denmark	1	16.7
Highest educational level	Postgraduate Degree	6	100

As compared to the survey sample, the expert sample had at least 50% of the respondents working in the defence sector (two of whom achieved Brigadier/ Colonel rank) and all had postgraduate qualifications.

Quantitative Data Analysis – Main Technology Areas

As noted above, the survey asked the professionals to evaluate the potential impact, likelihood of deployment / utilisation, extensiveness of use, and novelty of use with reference to the timeliness of development of these technologies in the future (near term: less than 5 years, medium term: 5-10 years, long term: more than 10 years). Table 3.3 also compares the highest-ranked responses between panel and expert respondents.

Table 3.3 – Comparison of highest-ranked responses on General Technology Areas between panel and expert respondents

Technology type	Criteria	Panel	Experts
Cyber	**Impact**	High/ Near term	Very High/ Near term
	Likelihood of deployment/ utilisation	Very High/ Near term	Very High/ Near term
	Extensiveness of Use	Very High/ Near term	Very High/ Near term
	Novelty of Use	Moderate/ Medium term	Moderate/ Near term
IoT/ IoBT	**Impact**	Moderate/ Medium term	High/ Near term
	Likelihood of deployment/ utilisation	Moderate/ Medium term	High/ Near term
	Extensiveness of Use	Moderate/ Medium term	High/ Near term
	Novelty of Use	Moderate/ Medium term	Moderate/ Medium term
AI	**Impact**	Very High/ Near term	Very High/ Near term
	Likelihood of deployment/ utilisation	Very High/ Near term	Very High/ Near term
	Extensiveness of Use	Very High/ Near term	High/ Near term
	Novelty of Use	Moderate/ Medium term	High/ Medium term
Autonomous Systems	**Impact**	Moderate/ Medium term	High/ Medium term
	Likelihood of deployment/ utilisation	Moderate/ Medium term	High/ Medium term
	Extensiveness of Use	Moderate/ Medium term	Moderate/ Medium term
	Novelty of Use	Moderate/ Medium term	High/ Near term

Responses from Survey Panel

Cyber technologies

The largest number of respondents rated the Likelihood of Deployment/ Utilisation and extensiveness of cyber technologies as very high and in the near term. This is not unexpected given the background of many of the respondents in the ICT industry and the growing challenges of cyber-technologies in the entire spectrum of conflict.[148] In terms of impact, the respondents rated cyber technologies as high and also in the near term. Interestingly, they only rated the novelty of cyber technologies as moderate. This may be because the pervasiveness of such technologies is apparent today.[149]

[148] Demchak, CC 2020, 'Cybered conflict, hybrid war, and informatization wars', in *Routledge Handbook of International Cybersecurity*, Routledge, pp. 36-51.
[149] Whyte, C, Thrall, AT & Mazanec, BM 2021, *Information warfare in the age of cyber conflict*, Routledge London & New York.

IoT/ IoBT technologies

The highest number of respondents rated the impact, Likelihood of Deployment/ Utilisation, extensiveness and novelty of IoT/ IoBT technologies as moderate and in the medium term. This may be because the full realisation of IoT technologies in civil applications is yet to be seen in many countries and may take some time to mature.[150]

AI technologies

The highest number of respondents rated the impact, Likelihood of Deployment/ Utilisation and extensiveness of AI technologies as very high and in the near term. This may be because of the high impact that AI technologies have been having on non-military aspects of life in recent years.[151] Interestingly, respondents only rated the novelty of cyber technologies as moderate, which may also reflect on the pervasiveness of the technology in everyday life.

Autonomous systems technologies

The highest number of respondents rated the impact, Likelihood of Deployment/ Utilisation, extensiveness and novelty of autonomous systems technologies as moderate and in the medium term. This may be because of the over-promise and under-delivery of these types of technologies in recent years like self-driving cars and similar platforms.[152]

Responses from Experts

Overall, the responses were very similar to that of the survey panel. The main difference was that in more than half of the criteria, the experts either rated the technologies slightly higher in impact, Likelihood of Deployment/ Utilisation, extensiveness or novelty or they saw the technology being deployed faster than the panel did (light green). For example, under IoT/ IoBT, their timelines were in the near term i.e. that these technologies were going to be impactful, extensive, etc. in the next 5 years. In the case of the impact of Cyber technologies (dark green), the experts rated this as very high and near term, higher than the panel responses. Only one criteria (AI – Novelty of Use) was ranked lower than the panel (High/ Near term) (orange). This may be because the experts had a more specific understanding of what AI meant in the defence context than the panel respondents.[153]

Quantitative Data Analysis – Specific Technologies

Eleven specific technologies/ trends of technologies

Besides providing a review of the four main technology areas (Cyber, IoT/IoBT, AI, and Autonomous Systems), the scientometric review also identified eleven specific technologies or trends of technologies that merit further exploration as follows:

1. Cyber Security of critical infrastructure;
2. Network Communications and Information technologies;
3. Swarm intelligence-related technologies and systems;
4. Industry 4.0 technologies where the cyber-physical domains merge;
5. Unmanned and autonomous systems;
6. Optimisation and other algorithms;

[150] Ahn, S-J 2020, 'Three characteristics of technology competition by IoT-driven digitization', *Technological Forecasting and Social Change*, vol. 157, p. 120062.
[151] Andrada, G, Clowes, RW & Smart, PR 2023, 'Varieties of transparency: exploring agency within AI systems', *AI & SOCIETY*, vol. 38, no. 4, pp. 1321-31.
[152] Agrawal, S, Schuster, AM, Britt, N, Mack, EA, Tidwell, ML & Cotten, SR 2023, 'Building on the past to help prepare the workforce for the future with automated vehicles: A systematic review of automated passenger vehicle deployment timelines', *Technology in Society*, vol. 72, p. 102186.
[153] Neri, H & Cozman, F 2020, 'The role of experts in the public perception of risk of artificial intelligence', *AI & SOCIETY*, vol. 35, no. 3, pp. 663-73.

7. Neural Networks;
8. Smart Sensors;
9. Deep/Machine Learning;
10. Civil and military R&D and uses of these technologies; and
11. Convergence of technologies in strategic industries that support any phases of military operation

The survey asked the professionals to evaluate the potential impact, likelihood of deployment / utilisation, extensiveness of use, and novelty of use with reference to the timeliness of development of these specific technologies in the future (near term: less than 5 years, medium term: 5-10 years, long term: more than 10 years).

Results

Table 3.4 compares the highest-ranked responses between panel and expert respondents.

Table 3.4 – Comparison of highest-ranked responses on Specific Technologies between panel and expert respondents

Technology type	Criteria	Panel	Experts
Cyber Security of critical infrastructure	**Impact**	Very High/ Near term	Very High/ Near term
	Likelihood of deployment/ utilisation	Very High/ Near term	Very High/ Near term
	Extensiveness of Use	Moderate/ Medium term	Very High/ Near term
	Novelty of Use	Moderate/ Medium term	High/ Near term
Network communications and IT	**Impact**	High/ Near term	High/ Near term
	Likelihood of deployment/ utilisation	Moderate/ Medium term	Very High/ Near term
	Extensiveness of Use	Moderate/ Medium term	Very High/ Near term
	Novelty of Use	Moderate/ Medium term	High/ Near term
Deep/ Machine Learning	**Impact**	Moderate/ Medium term	High/Near-term
	Likelihood of deployment/ utilisation	Moderate/ Medium term	High/ Near term
	Extensiveness of Use	Moderate/ Medium term	Moderate/ Near term
	Novelty of Use	Moderate/ Medium term	High/ Near term
Swarm intelligence-related technologies	**Impact**	Moderate/ Medium term	Moderate/ Medium term
	Likelihood of deployment/ utilisation	Moderate/ Medium term	Moderate/ Medium term
	Extensiveness of Use	Moderate/ Medium term	Moderate/ Medium term
	Novelty of Use	High/ Near term	Moderate/ Medium term
Industry 4.0 technologies	**Impact**	Moderate/ Medium term	High/ Medium term
	Likelihood of deployment/ utilisation	Moderate/ Medium term	High/ Medium term
	Extensiveness of Use	Moderate/ Medium term	High/ Medium term
	Novelty of Use	Moderate/ Medium term	Moderate/ Near term
Unmanned and autonomous systems	**Impact**	Moderate/ Medium term	Very high/ Near term
	Likelihood of deployment/ utilisation	Moderate/ Medium term	High/ Medium term
	Extensiveness of Use	Moderate/ Medium term	High/ Near term
	Novelty of Use	Moderate/ Medium term	High/ Near term
	Impact	Moderate/ Medium term	High/ Near term

Optimisation and other algorithms	**Likelihood of deployment/ utilisation**	Moderate/ Medium term	High/ Near term
	Extensiveness of Use	Moderate/ Medium term	High/ Near term
	Novelty of Use	Moderate/ Medium term	Moderate/ Near term
Neural Networks	**Impact**	Moderate/ Medium term	Moderate/ Medium term
	Likelihood of deployment/ utilisation	Moderate/ Medium term	High/ Medium term
	Extensiveness of Use	Moderate/ Medium term	High/ Medium term
	Novelty of Use	Moderate/ Medium term	High/ Near term
Smart Sensors	**Impact**	Moderate/ Medium term	High/ Near term
	Likelihood of deployment/ utilisation	Moderate/ Medium term	High/ Near term
	Extensiveness of Use	Moderate/ Medium term	High/ Near term
	Novelty of Use	Moderate/ Medium term	High/ Near term
Civil and military R&D and uses of these technologies	**Impact**	Moderate/ Medium term	High/ Medium term
	Likelihood of deployment/ utilisation	Moderate/ Medium term	High/ Near term
	Extensiveness of Use	Moderate/ Medium term	Moderate/ Medium term
	Novelty of Use	Moderate/ Medium term	Moderate/ Near term
Convergence of technologies in strategic industries	**Impact**	Moderate/ Medium term	Very high/ Near term
	Likelihood of deployment/ utilisation	Moderate/ Medium term	High/ Medium term
	Extensiveness of Use	Moderate/ Medium term	High/ Medium term
	Novelty of Use	Moderate/ Medium term	Moderate/ Near term
Technology type	**Criteria**	**Panel**	**Experts**

Responses from Survey Panel

Besides the first item of cyber security for critical infrastructure, all the other 10 technologies scored moderate/ medium term. These are generally lower than the scores they assigned to the four general technology areas. This may be due to a few reasons. First, cyber security for critical infrastructure has been featured relatively extensively as compared to the rest in the media and also in workplaces. This means that the respondents are more familiar and more aware of the specifics of this technology vis-à-vis the other technologies. Second, while the respondents may have been able to recognise the four main general technology areas, they may have been less aware of the specific technologies based on their education and professional experience, and whether or how this can be applied in the military context. Third, and as a result of the first two points, the respondents may therefore resort to central tendency bias, whereby respondents in survey research become less willing or unwilling to answer with extreme responses, choosing to answer using more towards the middle.[154]

Responses from Experts

Following the trend from the main technology areas, the experts either rated the technologies slightly higher in impact, Likelihood of Deployment/ Utilisation, extensiveness or novelty or they saw the technology being deployed faster than the panel did in part because of developments in the non-defence sectors. For example, one of the experts with both defence and technology expertise noted,

"The Defence sector will struggle to keep up with advancements in the private sector in areas of high technology and retention of HR; dual-use technologies will become commonplace".

Again, this may be because the experts had a more specific understanding of what AI meant in the defence context than the panel respondents.

[154] Akbari, K, Eigruber, M & Vetschera, R 2024, 'Risk attitudes: The central tendency bias', *EURO Journal on Decision Processes*, vol. 12, p. 100042.

Qualitative Data Analysis

The Leximancer Insight Dashboard Report for the concept of "Technology" (Table 3.5) based on the analysis of open-ended questions related to future disruptive technologies, revealed several valuable insights.

Table 3.5: Study 2 Insight dashboard report (Technology)

Category	Concept	Prominence scores (PS)	Compound concept	Prominence scores (PS)
Technology	defence	14.1	capabilities & battlefield	499.8
	capabilities	12.7	capabilities & warfare	416.5
	cyber	11.6	defence & battlefield	416.5
	battlefield	11.3	defence & capabilities	312.4
	warfare	10.6	defence & cyber	245.0
	defence	8.9	warfare & defence	219.2
	robotics	8.6	capabilities & robotics	217.3
	security	4.5	cyber & battlefield	196.0
			cyber & robotics	170.4
			battlefield & robotics	144.9
			capabilities & cyber	98.0
			defence & robotics	90.5
			capabilities & defence	87.7
			cyber & security	78.4
			robotics & security	58.0

First, the Dashboard highlights that the most prominent word in relation to technology is "defence (14.1)", indicating the importance of technology to defence forces. In the context of cyber, AI, IoT/ IoBT and Autonomous Systems technologies, "capabilities and battlefield (499.8)" is the top-ranked compound concept, or pair of concepts most strongly related to technology. For example:

"Information and Communication Technology (ICT) and Artificial Intelligence (AI) will rapidly and widely develop in the field of robotics, which will enhance the development of human intellectual capabilities on the battlefield."

And

"Resulting in overwhelming cognition demand for sense making, rapid decision cycle on wide range of technical expertise, and requiring large and diversified coordinated actions. Protective capabilities such Counter drone, Early Warning, harden protection Cyber hacking, cyber snooping, cyber protection Digital twin of battlefield Man unmanned system pairing AI in decision making."

Another compound concept prominently related to technology includes "capabilities and warfare (416.5)". This indicates the need for militaries like the ADF to develop technological capabilities to be successful on the battlefield and in conducting warfare in general. For example:

"Defence forces should focus on investing in cybersecurity measures to safeguard against cyberattacks, enhancing IoT/IoBT capabilities for improved situational awareness and communication, developing autonomous systems for unmanned missions to reduce risks to personnel, and advancing AI for predictive analytics to anticipate and counter emerging threats effectively. These investments are crucial for maintaining operational superiority, reducing vulnerabilities, and adapting to modern warfare dynamics."

Table 3.6: Study 2 Insight dashboard report (Threats/ Opportunities)

Category	Concept	Prominence scores (PS)	Compound concept	Prominence scores (PS)
Threats/ Opportunities	cyber	13.4	capabilities & warfare	336.4
	defence	9.6	cyber & security	253.3
	capabilities	6.8	cyber & defence	197.9
	warfare	5.7		
	security	3.6		
	defence	2.8		

As for the Leximancer Insight Dashboard Report for Threats/ Opportunities (Table 3.6), the report findings highlight that the most frequently used word is "cyber (13.4)", which corroborates the findings from the scaled questions. This means that respondents see the opportunities and threats in the development of capabilities in cyber technologies as most important among cyber, AI, IoT/ IoBT and Autonomous Systems technologies. This is reinforced by "capabilities and warfare (336.4)" and "cyber and security (253.3)" as the top-ranked compound concepts. For example:

"Defence forces should be investing heavily in the rapidly emerging (and continuously improving) AI systems, technologies and intellectual property that have been developed in the past couple of years. They should also be investing in developing more advanced security and safety measures to protect against cyber threats."

Table 3.7: Study 2 Insight dashboard report (Defence)

Category	Concept	Prominence scores (PS)
Defence	drones	13.4
	future	10.6
	threats	9.6
	capabilities	3.9
	invest	3.9
	security	3.4

In terms of defence specifically, the Leximancer Insight Dashboard revealed that "drones", "future", "threats", "capabilities", "invest", and "security", were the most prominent concepts which the respondents mentioned in this context (Table 3.7).

For example, **defence and drones** were discussed as in this comment: *"The defence forces should be investing in computer networks combined with robotics and AI. This combination makes great robotic weapons or advanced drones/robots."*

Conversely, **defence and future** evidenced in this comment: *"The integration of ICT and AI will enable more efficient and effective decision-making, improved situational awareness, and enhanced operational capabilities. This will ultimately contribute to the overall success and safety of defence forces in future conflicts."*

Defence and threats were also key to respondents' answers, for example: "*Defence forces should invest in cybersecurity, IoBT, autonomous system, and AI to enhance capabilities and address threats like cyberattacks, IoBT vulnerabilities, system risks, and concerns."*

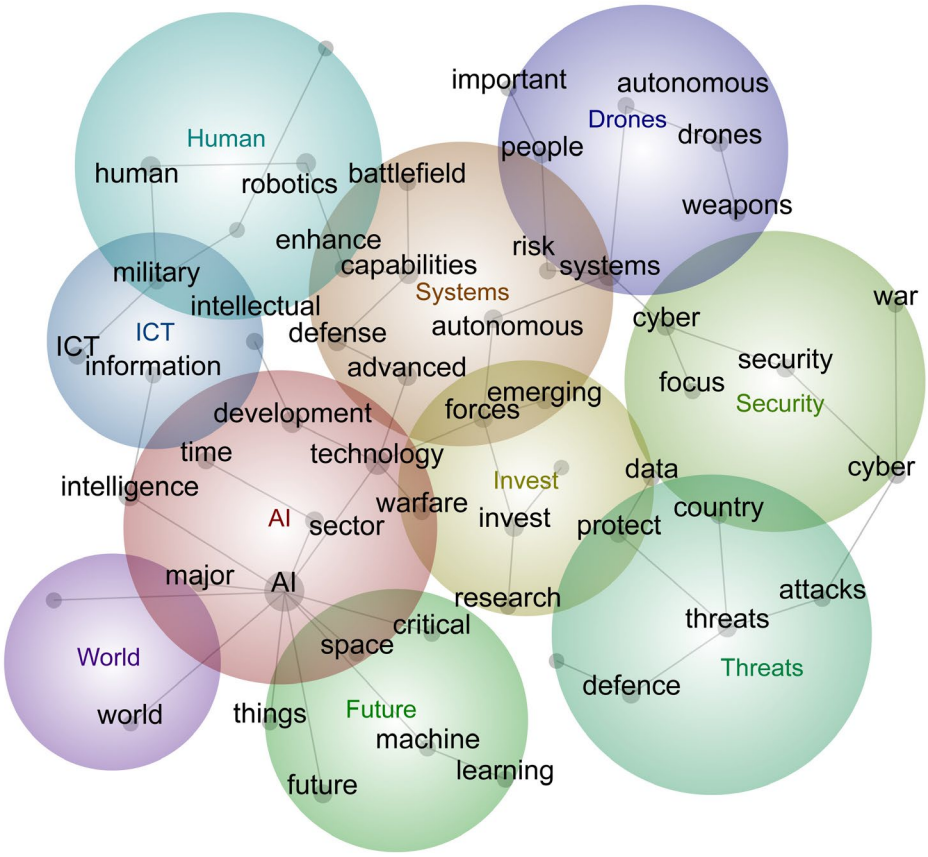
Notably, **defence and capabilities** evidenced in this comment: *"The defence force is moving into an emphasis on disruptive technology with high computing power, machine-learning capabilities and AI however, I'm sceptical of the ADF's capacity to deploy it."*

Additionally, **defence and invest** evidenced in this comment: *"Other countries will invest in technology, especially AI when it comes to defence. You don't want to be left behind".*

Lastly, **defence and security** were commented on as in this quote: *"Additionally, exploring AI applications can help improve decision-making processes, enabling faster and more accurate responses in various defence*

scenarios. These investments can ultimately enhance defence capabilities and contribute to the safety and security of nations."

Figure 2.5: Study 2 Leximancer Concept Map



The Leximancer concept map for Study 2 (Figure 2.5) revealed that the most important themes in the open-ended responses of the survey data were: AI, Systems, Invest, Future, Threats, Security, Drones, Human, ICT, and World.

The AI theme was the most prominent topic which appeared in the open-ended responses to the survey, and included mentions of the "sector", "technology", "development", "time", "intelligence", and "warfare".

For example: *"Cyberattacks, major tool of subversion, that crosses into industry and democracy. AI will affect most threats and capabilities in the future."*

Closely related to AI were themes of "Systems", and "Investment", which included a focus on "defence", "capabilities", "battlefield", "forces", "autonomous" and "emerging", as well as "research".

For example: *"Cyber, AI, Smart Sensors, Critical Artificial Intelligent Technology with and without Human interface. The future of space technology is worth investment now."*

Other prominent themes in the open-ended responses to the survey included "Future", "Threats", "Security" and "Human". Evident prominent concepts which highlighted the association between concepts and these themes included: "space", "machine learning", "defence threats", "protect data", "country threats", "cyber-attacks", "cyber security", "cyber war", "robotics", "human" and "military".

For example: *"Cyber-attacks are happening more frequently currently and probably should be looked into, and the rapid development of AI could potentially pose higher threats in the future."*

Less prominent, although also important emergent themes, included: “ICT”, “Drones” and “World”. These were characterised by discussion of “military”, “intellectual”, “information”, “ICT”, “risk”, “systems”, “autonomous drones” and “weapons”.

For example: *“The rapid dispersion and advancement of ICT, along with AI in the realm of robotics, is poised to significantly amplify human cognitive capabilities within the theatre of military operations.”*

Qualitative analysis: responses from experts

Given that there were only six experts, we focussed on the differences in responses in their open-ended questions as compared to the panel’s responses. In general, we identified six topics that the experts emphasised or perceived differently.

1. The risk associated with the legacy infrastructure and systems which were vulnerable to cyber-attacks, *“Aging systems used by critical infrastructure operators is concerning considering that most of their operating system are legacy technologies, yet businesses are driving innovations with emerging technologies without considering the vulnerabilities associated with their environments”.*
2. The expert panel also highlighted the threats associated with autonomous remotely controlled systems that were vulnerable to hacking or cyber-attack, *“Cyber hacking, cyber snooping, cyber protection Digital twin of battlefield Man-unmanned system pairing AI in decision making.” “Cybersecurity of military platforms is a common gap that is difficult to plug.”*
3. The role and sophistication of the private sector in the defence industry and the competition it poses to the government lead defence sector, *“the Defence sector will struggle to keep up with advancements in the private sector in areas of high technology and retention of HR; dual-use technologies will become commonplace.”*
4. The development and deployment of early warning systems and protective capabilities to counter attacks, *“Active protection systems, counter drone, counter air, directed energy weapons. This survey lacks focus on what matters, being more lethal and protecting ourselves from their lethal effects.”*
5. Current conflict such as the war in Ukraine are providing indicators of what is to come, *“We are getting cues now as to what matters via Ukraine. Autonomous and smart sensor are priorities. Cyber defence and networks are important but not as damaging.”*
6. The rise of AI which allows for this information will provide a greater cognitive challenge for those involved in future warfare, *“War will be Multi-dimensional …. Real Information and Misinformation will be hard to differentiate. Resulting in overwhelming cognition demand for sense making, rapid decision cycle on wide range of technical expertise, and requiring large and diversified coordinated actions”.*

Chapter 4 – Summary of Findings, Implications and Conclusion

Introduction

The purpose of this research was to conduct a horizon scan[155] of disruptive and converging technologies of:

1. Cyber;
2. IoT/ IoBT;
3. AI; and
4. Autonomous systems.

The research conducted would help examine the opportunities and challenges of these four digital technology fields that have been identified as force multipliers in Australia's defence strategy.

This section summarises the two studies and discusses the key findings in extant published research and identifies implications for Australia's defence strategy and policy to better prepare itself.

Findings of Study 1 – Scientometric Study

The scientometric study provided the following key insights:

1. **Cyber technologies.** The review emphasised the increasing importance of cyber technologies across all domains, especially in warfare tactics and strategic competition. It further highlights rapid advancements and secure solutions for cyber warfare, leveraging algorithms and machine learning for defence. Furthermore, the analysis highlights the significance of human capital investment and education in achieving cyber superiority and security, underlining the role of training programs and cognitive agility in resilient cyber environments.
2. **IoT/ IoBT technologies.** When carrying out an analysis of IoT/IoBT technologies, we found emerging literature on the growth of automation driven by IoT/IoBT technologies, particularly in autonomous systems like drones, wearables, satellite communication, and radar technologies. The importance of securing IoT/IoBT systems against threats, emphasising defence mechanisms such as blockchain, AI, and machine learning to counter cyberattacks and maintain robustness, is also highlighted in research. The core IoT technologies and research interests include sensor networks, wireless communication, energy efficiency, and the emerging field of IoT technologies including nano technologies, all aimed at advancing the foundational technologies underpinning the IoT/IoBT paradigm.
3. **AI technologies.** The study finds that for AI in defence, a large emphasis is placed on AI's role in operational efficiencies, such as using deep learning techniques in additive manufacturing and employing recurrent neural networks for IoT malware detection. We found that AI is of central importance in future decision-making, including its potential impact on international relations and political states, as well as the risks associated with AI adoption in the defence sector. The research further highlights AI's pervasiveness in the development of other technologies, such as utilising deep reinforcement learning in UAV technologies and coordinating UAVs using animal colony perception techniques. Finally, the review identifies the increasing use of AI in medicine and health, including insomnia treatment, acute kidney injury detection, suicide prediction, and PTSD prevention among military personnel.

[155] Connery, D 2013, 'Horizon Scanning: Enhancing Strategic Insight for National Security Policymaking', *Security Challenges*, vol. 9, no. 3, pp. 11-30, Johnston, R & Cagnin, C 2011, 'The influence of future-oriented technology analysis: Addressing the Cassandra challenge', *Futures*, vol. 43, no. 3, pp. 313-6, Ramalingam, B & Jones, H 2007, *Strategic futures planning: a guide for public sector organisations*, Ark Group.

4. **Autonomous systems**. The research demonstrates the growing research and development of operationalisation of autonomous systems, including advancements in UAV manoeuvrability, underwater vehicle designs, and military robot control algorithms. There is also an emphasis on the ethics of autonomous systems including human-machine teaming, accountability for autonomous weapon systems, and the implications of lethal autonomous weapons on international relations. Finally, there is a large body of research in systems and networks supporting autonomous systems, including advancements in wireless sensor networks, energy-efficient routing algorithms for mobile sensor networks, and cooperative control strategies for autonomous vehicles.

The scientometric research (Study 1) also found eleven specific emerging and disruptive technologies or technological trends as follows:

1. Cyber Security of critical infrastructure;
2. Network Communications and Information technologies;
3. Swarm intelligence-related technologies and systems;
4. Industry 4.0 technologies where the cyber-physical domains merge;
5. Unmanned and autonomous systems;
6. Optimisation and other algorithms;
7. Neural Networks;
8. Smart Sensors;
9. Deep/Machine Learning;
10. Civil and military R&D and uses of these technologies; and
11. Convergence of technologies in strategic industries that support any phases of military operation.

Findings of Study 2 – Survey Research Study

Based on IFSH research survey methodology, the survey study followed up by evaluating the cyber, IoT/ IoBT, AI and autonomous systems technologies based on four dimensions: potential impact, likelihood of deployment / utilisation, extensiveness of use, and novelty. It also elicited responses from industry professionals on the timeliness of these technologies (near term <5 years; medium term 5-10 years; long term >10 years).

In the main technology areas, the research found that panel respondents ranked cyber and AI technologies more highly and more urgently as compared to IoT/ IoBT and autonomous systems technologies. This was similar among panel respondents and experts. However, experts saw greater timeliness for IoT/ IoBT and autonomous systems technologies i.e. instead of taking up to 10 years to develop, there was a more urgent need for these to be implemented in future conflicts.

In the specific technology areas, there was a similar high and near-term rating between panel and experts for cyber security technologies to protect critical infrastructure. However, there were differences between the panel and the experts in that experts generally saw shorter timelines for most of the other specialised technologies and technological trends.

In the open-ended responses, AI is seen to be a key linking technology. “AI” emerged as the theme that had the most overlap with other themes (five in total: Invest, Systems, ICT, World, and Future). The need for a systems approach was also emphasised. “Systems” emerged as a theme that had many overlapping aspects with other themes (four in total: Invest, AI, Human, Drones). And the respondents also reiterated the need for Investment in these emerging technologies where “invest” was a theme that connected with other themes (four in total: Systems, AI, Security, Threats).

The qualitative responses among respondents included concerns around the increasing complexity of technologies through combining platforms. This is reinforced by issues surrounding aging technologies and legacy systems that may make backward integration difficult with the exponential speed of technology

development. The reliance on AI, sensors and autonomous systems can also create vulnerability when human insights are removed and data can be corrupted, falsified, biased or remotely manipulated. And there were challenges in terms of human capital to maximise the development and effectiveness of these disruptive technologies i.e. the expertise, skills and knowledge required for future warfare are not part of the current defence force which results in an over-dependence on private contractors that are not country-specific.

Overall, the survey study provided a means to prioritise investments in defence technology which is discussed below.

Opportunities and Challenges and Implications for the Australian Department of Defence and the ADF

In terms of implications for the Australian Department of Defence, the 2023 Defence Strategic Review (DSR) and the recent February 2024 Defence Industry Development Strategy (DIDS) does have some highly relevant steps needed to seize opportunities and tackle the challenges that these disruptive technologies present.

To reinforce this, there are a number of recommendations based on our research:

1. **Urgent investment needed to develop and capitalise on these technologies**. Almost all of the disruptive technologies identified as having potential impact, likelihood of deployment / utilisation, extensiveness of use, and novelty for defence purposes were shown to be needed in the near-term (<5 years) or medium-term (<10 years). More concerningly, the expert respondents indicated that most of these were actually critical in the near-term (<5 years). In the 2024 DIDS, there were two timeframes identified as part of the Sovereign Defence Industrial Priorities - Epoch 1: 2023-2025 and Epoch 2: 2026 - 2030. Based on our research, it is likely that some of these priorities may need to be brought forward from the Epoch 2 timeframe for them to make a difference to Defence.

2. **Prioritise the investment in technology.** Given that there are limited resources, our research also points to ways to prioritise these technological investments in the context of Australia.

    a. **Main technology areas**. Like other researchers, we find that investments in cyber/AI will have higher impact and can be more rapidly implemented.[156] This differs from the more hardware-heavy focus of the DIDS. For the four areas that we examined, the following are the priorities:

        (1) **Priority 1.** Cyber technologies, AI technologies;

        (2) **Priority 2.** IoT/ IoBT technologies; and

        (3) **Priority 3.** Autonomous systems technologies.

    b. **Specific technologies**. For the 11 specific technologies or technology trends, the following are the priorities:

        (1) **Priority 1**. Cyber Security of critical infrastructure, network communications and IT, smart sensors;

        (2) **Priority 2.** Deep/ machine Learning technologies, unmanned and autonomous systems, optimisation and other algorithms, neural networks, industry 4.0 technologies, capitalising on the convergence of technologies in strategic industries, exploiting both civil and military R&D and uses of these technologies; and

        (3) **Priority 3.** Swarm intelligence-related technologies and systems.

3. **More explicit commitment of resources (e.g. financial, human) to invest in these technologies from both government and private sector**. These technologies are complex and do not come cheap. While there are timelines in the 2023 DSR and 2024 DIDS, the resourcing for these technological investments is unclear. And as the open-ended responses show, respondents are

156

aware that if there is insufficient investment in these technologies, Australia will be left behind and not be able to maintain its technological edge in the battlespace.

4. **Higher flexibility needed to exploit non-linear opportunities in technology innovation**. The respondents also recognised that the culture and nature of decision-making in the defence department and the sector in general means that it will increasingly struggle to keep up with advancements in the private sector in areas of high technology and retention of skilled personnel. There is a need to address this human aspect of technology innovation and management to fully realise the technological investments that will be made.

Conclusion

With rising environmental uncertainty, combined with even more rapid technological change, stakeholders in the strategic planning and policy communities are increasingly confronted by new challenges and opportunities in public decision-making and science, technology and innovation (STI) strategy-making (Linstone 2002). Technology foresight research such as the horizon scan conducted here are challenging because they involve an overwhelming number of technologies that impact citizen security, geopolitics, as well as industrial and international policy. However, it is hoped that this research has provided invaluable insights into the ever-evolving landscape of strategic policy decision-making in the context of ongoing technological disruption.

About the authors

Professor Pi-Shen Seet. Pi-Shen is a Professor of Entrepreneurship and Innovation at Edith Cowan University's (ECU) School of Business and Law. He has a PhD (University of Cambridge), M Defence Studies (University of Canberra) and is also a graduate Australian Army Command and Staff College, Singapore Armed Forces (SAF) Command and Staff College and the New Zealand Grade II Staff Course. He has served in command and staff officer positions in the SAF with particular experience working with the Australian and New Zealand Defence Forces. His research focuses on the interfaces between innovation and its impact on society. He has been chief investigator or partner investigator on competitive research projects securing about AUD$400,000 in Australian category 1, 2, 3 and 4 grants, and major international grants over the last 5 years. This includes 2 Department of Defence Strategic Policy Grants Program projects. Aside from publications in high-impact journals like *Technological Forecasting and Social Change, Journal of Technology Transfer,* and *Business and Society.* He has also been a multiple award winner for the SAF's Chief of Defence Force Paper Competition. His Australian research projects have led to major submissions to the Commonwealth Government and publications in high impact journals and media outlets such as *The Conversation* and *ABC News*. He has extensive experience in collaborating with both public and private sector organisations at national and State level, as well as with peak bodies and non-government organisations.

Associate Professor Mike Johnstone. Mike is an A/Prof at the School of Science at ECU, where he teaches network security and mobile application development. He has publications in high-impact journals like IEEE Transactions on Information Forensics and Security, Sensors and Computer Networks as well as features in The Conversation and ABC Radio. As a member of the Centre for Securing Digital Futures at ECU, his work on resilient systems covers secure development methodologies, wireless sensor networks and the security of IoT devices, with a focus on critical infrastructure. With over 30 years of experience in ICT, he provides consultancy services in cyber security for private industry, government and research organisations. He has held various IT roles including programmer, systems analyst, project manager and network manager before moving to academia. A/Prof Johnstone serves on various cyber-related A-ranked conference committees. He was the theme lead for Network Forensics-Response to Emerging Threats in the Industry-driven, federally funded Cyber Security Cooperative Research Centre (CSCRC).

Associate Professor Janice Jones. Janice (Jane) is an A/Prof of Human Resource Management (HRM) at Flinders University's College of Business, Government & Law. She has a PhD (Flinders University) and M. Commerce (University of NSW). Her research focuses on the interfaces between innovation, technology and HRM. She has been chief investigator or partner investigator on competitive research projects in Australian category 1, 2, 3 and 4 grants over the last 5 years. This includes 2 Department of Defence Strategic Policy Grants Program projects. She has publications in high-impact journals like *Technological Forecasting and Social Change, Journal of Technology Transfer* and *Industrial Marketing Management*. Her research projects have led to major submissions to the Commonwealth Government and publications in high impact journals and media outlets such as *The Conversation*. She has extensive experience in collaborating with both public and private sector organisations across levels of government, as well as with peak bodies and non-government organisations.

Dr Anton Klarin. Anton is a Senior Lecturer in Management, at Curtin University's School of Management and Marketing. His research encompasses and has been published on the topics of strategic choices of emerging market firms (for example, in *Journal of Management Inquiry*), institutional environments in emerging markets, and interdisciplinary research using scientometric methods (publications in *Technological Forecasting and Social Change*, *Systems Research and Behavioral Science*, *Journal of Business Research, International Business Review,* and other high impact outlets). He has also published a policy document on the Internet of Things and received an Emerald Literati Award for Excellence.

***Dr Helen Cripps*.** Helen is honorary Senior Lecturer at ECU's School of Business and Law (SBL). She conducts industry-based research across multiple sectors including maritime, electronic health, tourism and text mining. Helen's research sits at the nexus of online media, technology adoption and innovation as it draws on her national and international network. Her research projects have covered industries in Australia, Slovenia, Croatia, Finland, Norway, Sweden, UK and USA. She has received numerous awards for innovative delivery of the new product development unit at SBL which involves the collaborative development of new technologies between

teams from different countries. She has also won awards from Women in Technology Western Australia (WiTWA) for innovative technology projects in education.

***Dr Jalleh Sharafizad*.** Jalleh is a Senior Lecturer in Entrepreneurship and Innovation at ECU's SBL. Jalleh has achieved notable success in the fields of entrepreneurship, small business, and regional entrepreneurship development. Her extensive publications include contributions to prestigious international journals such as the *Entrepreneurship and Regional Development, Journal of Business and Industrial Marketing, International Journal of Hospitality Management, Journal of Hospitality and Tourism Management, Human Resource Management, Studies in Higher Education Journal,* and *Education + Training.* Jalleh has been awarded the University of Antwerp's Staff Exchange Erasmus program award and Edith Cowan University's Athena SWAN Advancement Scheme award. She has also effectively and successfully led multiple research projects funded by both Edith Cowan University and the Western Australian Government.

Dr Violetta Wilk. Violetta is a Senior Lecturer in Digital Marketing in the School of Business and Law, at Edith Cowan University. Violetta has over 15 years of corporate marketing experience. Her areas of research expertise include big data analytics, data visualisation, user-generated content (UGC), interactive internet-based consumer behaviour, and the persuasive contextual attributes of online communication. She researches, teaches and consults on these topics. She was a Chief Investigator on the ECU team for the 2021 DSP Multi-Party Collaborative Project on "Three case studies of Mass Influence Organisations" which studied Cambridge Analytica (CA), The Russian Internet Research Agency (IRA), and Mainstream Social Media, especially Facebook (FB). Violetta is currently Chief Investigator on several studies involving big data analysis using data visualisation of social media user generated content from platforms including Twitter, Facebook, Instagram, YouTube and other online and social media communities. She specialises in data visualisation of large qualitative datasets. Her research has recently been published in such journals as *The International Entrepreneurship and Management Journal, Asia Pacific Journal of Marketing and Logistics,* and *Public Relations Review.* Dr Wilk is currently involved in a research project investigating truth decay in social media user-generated content. She is a Fellow and Mentor with the Australian Marketing Institute and a Certified Practicing Marketer.

***Professor David Suter*.** David is a Professor of Computer Science in the ECU School of Science (Computing and Security). He leads a team carrying out leading research in computer vision and big-data analysis. His special expertise includes robust statistical fitting, computational geometry and machine learning. He has been a member of the Australian Research Council (ARC) College of Experts and has secured competitive ARC and NHMRC grants as Chief Investigator. He is also a current and past member of editorial boards of the *International Journal of Computer Vision*, *Pattern Recognition*, *IPSJ Transactions on Computer Vision and Applications*, *Journal of Mathematical Imaging and Vision*, and *Machine Vision and Applications*.

Mr Tony Marceddo. Tony leads the strategy, growth and development for the ECU research theme called Securing Digital Futures (SDF). SDF is a new interdisciplinary research approach that builds on ECU's existing strengths in Cyber-Security, Artificial Intelligence, Autonomous Systems, Information warfare, Digital Citizenship and Human Behaviours. Tony also leads Defence Research and Engagement for the university. Previously, Tony was the General Manager of Vault Cloud, the first Australian cloud company to have their cloud service certified by the Australian Government (Australian Signals Directorate) to handle information up to Protected. Tony has also had over 30-years of leadership experience spanning numerous industries including the Defence, Intelligence, Space, Cyber and Communication sectors. These include General Manager of Australian Intelligence and Cyber Security at Northrop Grumman. Where he was responsible for the incorporation of M5 Network Security into Northrop Grumman operations. The integration included the delivery of key projects to the Defence industry, such as next-generation secure mobile ICT, secure communications for the Australian Army, and computer network defence. Tony also worked for Raytheon for some years in a range of management and project roles, which included Deputy General Manager for the Intelligence and Cyber business. This included the integration of COMPUCAT into Raytheon operations and managing the Intelligence and Security programs. Tony further demonstrated his management skills in this position, overseeing more than 400 direct staff when managing the Joint Defence Facility Pine Gap (JDFPG) contract for Raytheon at Alice Springs and 160 staff as the manager for the Canberra Deep Space Communication Complex (CDSCC) contract at Tidbinbilla. Tony also possesses extensive experience working in the Australian Federal Government, primarily within the Intelligence Sector where he was a senior manager with the Australian Defence Intelligence for over 25 years. Tony's achievements in the Defence and Intelligence sectors have been recognised by the Australian and United States Intelligence communities with a US Intelligence Medallion and an Australian Intelligence Community Medallion.

Appendix 1: Survey Research Study detailed tables

Cyber technologies

Tables A1.1, A1.2, A1.3 and A1.4 present the results with respect to cyber technologies. Similar to IFSH's research[157], heatmaps were derived from the tables, but instead of using one colour, we have used a traffic-light based system whereby green illustrates the higher frequency of responses and pink lower frequency of responses with orange highlighting the in-between range. The responses that were red-bolded highlighted the highest responses from the panel.

Table A1.1 – Impact of Cyber Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Impact	Very High	55.00	13.25	29.00	6.99	21.00	5.06	105.00
	High	**67.00**	**16.14**	65.00	15.66	24.00	5.78	156.00
	Moderate	50.00	12.05	61.00	14.70	9.00	2.17	120.00
	Low	12.00	2.89	12.00	2.89	2.00	0.48	26.00
	Very Low	2.00	0.48	5.00	1.20	1.00	0.24	8.00
	Total	186.00		172.00		57.00		415.00

Table A1.2 – Likelihood of Deployment/ Utilisation of Cyber Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Likelihood of Deployment/ Utilisation	Very High	**81.00**	**19.52**	22.00	5.30	26.00	6.27	129.00
	High	59.00	14.22	49.00	11.81	12.00	2.89	120.00
	Moderate	38.00	9.16	76.00	18.31	6.00	1.45	120.00
	Low	18.00	4.34	13.00	3.13	1.00	0.24	32.00
	Very Low	9.00	2.17	3.00	0.72	2.00	0.48	14.00
	Total	205.00		163.00		47.00		415.00

[157] Favaro, M, Renic, N & Kühn, U 2022, *Negative multiplicity: Forecasting the future impact of emerging technologies on international stability and human security*, Institute of Peace Research and Security Policy at the University of Hamburg, Hamburg.

Table A1.3 – Extensiveness of Cyber Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Extensiveness	Very High	**74.00**	**17.83**	17.00	4.10	27.00	6.51	118.00
	High	65.00	15.66	60.00	14.46	18.00	4.34	143.00
	Moderate	49.00	11.81	62.00	14.94	3.00	0.72	114.00
	Low	20.00	4.82	11.00	2.65	0.00	0.00	31.00
	Very Low	7.00	1.69	2.00	0.48	0.00	0.00	9.00
	Total	215.00		152.00		48.00		415.00

Table A1.4 – Novelty of Cyber Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Novelty	Very High	34.00	8.19	17.00	4.10	28.00	6.75	79.00
	High	53.00	12.77	44.00	10.60	9.00	2.17	106.00
	Moderate	58.00	13.98	**79.00**	**19.04**	7.00	1.69	144.00
	Low	41.00	9.88	21.00	5.06	3.00	0.72	65.00
	Very Low	16.00	3.86	2.00	0.48	3.00	0.72	21.00
	Total	202.00		163.00		50.00		415.00

IoT/ IoBT

Tables A1.5, A1.6, A1.7 and A1.8 present the results with respect to IoT/ IoBT technologies.

Table A1.5 – Impact of IoT/ IoBT Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Impact	Very High	19.00	4.58	17.00	4.10	16.00	3.86	52.00
	High	56.00	13.49	53.00	12.77	18.00	4.34	127.00
	Moderate	55.00	13.25	**96.00**	**23.13**	16.00	3.86	167.00
	Low	27.00	6.51	25.00	6.02	2.00	0.48	54.00
	Very Low	8.00	1.93	5.00	1.20	2.00	0.48	15.00
	Total	165.00		196.00		54.00		415.00

Table A1.6 – Likelihood of Deployment/ Utilisation of IoT/ IoBT Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Likelihood of Deployment/ Utilisation	Very High	44.00	10.60	13.00	3.13	18.00	4.34	75.00
	High	55.00	13.25	58.00	13.98	13.00	3.13	126.00
	Moderate	41.00	9.88	86.00	20.72	14.00	3.37	141.00
	Low	24.00	5.78	26.00	6.27	3.00	0.72	53.00
	Very Low	12.00	2.89	3.00	0.72	5.00	1.20	20.00
	Total	176.00		186.00		53.00		415.00

Table A1.7 – Extensiveness of IoT/ IoBT Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Extensiveness	Very High	44.00	10.60	12.00	2.89	16.00	3.86	72.00
	High	51.00	12.29	44.00	10.60	20.00	4.82	115.00
	Moderate	49.00	11.81	86.00	20.72	21.00	5.06	156.00
	Low	26.00	6.27	20.00	4.82	7.00	1.69	53.00
	Very Low	12.00	2.89	6.00	1.45	1.00	0.24	19.00
	Total	182.00		168.00		65.00		415.00

Table A1.8 – Novelty of IoT/ IoBT and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Novelty	Very High	31.00	7.47	14.00	3.37	20.00	4.82	65.00
	High	45.00	10.84	46.00	11.08	11.00	2.65	102.00
	Moderate	53.00	12.77	90.00	21.69	14.00	3.37	157.00
	Low	38.00	9.16	23.00	5.54	4.00	0.96	65.00
	Very Low	20.00	4.82	3.00	0.72	3.00	0.72	26.00
	Total	187	45.06	176.00	42.41	52.00	12.53	415.00

Artificial Intelligence (AI)

Tables A1.9, A1.10, A1.11 and A1.12 present the results with respect to AI technologies.

Table A1.9 – Impact of AI Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Impact	Very High	67.00	16.14	38.00	9.16	38.00	9.16	143.00
	High	56.00	13.49	54.00	13.01	30.00	7.23	140.00
	Moderate	27.00	6.51	57.00	13.73	5.00	1.20	89.00
	Low	15.00	3.61	13.00	3.13	2.00	0.48	30.00
	Very Low	10.00	2.41	2.00	0.48	1.00	0.24	13.00
	Total	175.00		164.00		76.00		415.00

Table A1.10 – Likelihood of Deployment/ Utilisation of AI Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Likelihood of Deployment/ Utilisation	Very High	91.00	21.93	21.00	5.06	35.00	8.43	147.00
	High	51.00	12.29	55.00	13.25	19.00	4.58	125.00
	Moderate	31.00	7.47	56.00	13.49	7.00	1.69	94.00
	Low	19.00	4.58	17.00	4.10	2.00	0.48	38.00
	Very Low	8.00	1.93	3.00	0.72	0.00	0.00	11.00
	Total	200.00		152.00		63.00		415.00

Table A1.11 – Extensiveness of AI Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Extensiveness	Very High	72.00	17.35	16.00	3.86	35.00	8.43	123.00
	High	54.00	13.01	56.00	13.49	30.00	7.23	140.00
	Moderate	36.00	8.67	61.00	14.70	4.00	0.96	101.00
	Low	17.00	4.10	13.00	3.13	6.00	1.45	36.00
	Very Low	11.00	2.65	3.00	0.72	1.00	0.24	15.00
	Total	190.00		149.00		76.00		415.00

Table A1.12 – Novelty of AI Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Novelty	Very High	56.00	13.49	20.00	4.82	41.00	9.88	117.00
	High	58.00	13.98	43.00	10.36	16.00	3.86	117.00
	Moderate	46.00	11.08	**72.00**	**17.35**	9.00	2.17	127.00
	Low	18.00	4.34	16.00	3.86	6.00	1.45	40.00
	Very Low	12.00	2.89	1.00	0.24	1.00	0.24	14.00
	Total	190.00		152.00		73.00		415.00

Autonomous Systems

Tables A1.13, A1.14, A1.15 and A1.16 present the results with respect to AI technologies.

Table A1.13 – Impact of Autonomous Systems Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Impact	Very High	35.00	8.43	16.00	3.86	19.00	4.58	70.00
	High	42.00	10.12	78.00	18.80	29.00	6.99	149.00
	Moderate	44.00	10.60	**88.00**	**21.20**	11.00	2.65	143.00
	Low	19.00	4.58	12.00	2.89	6.00	1.45	37.00
	Very Low	12.00	2.89	2.00	0.48	2.00	0.48	16.00
	Total	152.00		196.00		67.00		415.00

Table A1.14 – Likelihood of Deployment/ Utilisation of Autonomous Systems Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Likelihood of Deployment/ Utilisation	Very High	53.00	12.77	17.00	4.10	29.00	6.99	99.00
	High	45.00	10.84	64.00	15.42	11.00	2.65	120.00
	Moderate	39.00	9.40	**86.00**	**20.72**	11.00	2.65	136.00
	Low	28.00	6.75	15.00	3.61	4.00	0.96	47.00
	Very Low	9.00	2.17	3.00	0.72	1.00	0.24	13.00
	Total	174.00		185.00		56.00		415.00

Table A1.15 – Extensiveness of Autonomous Systems Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Extensiveness	Very High	45.00	10.84	12.00	2.89	26.00	6.27	83.00
	High	52.00	12.53	57.00	13.73	23.00	5.54	132.00
	Moderate	35.00	8.43	100.00	24.10	11.00	2.65	146.00
	Low	20.00	4.82	12.00	2.89	6.00	1.45	38.00
	Very Low	14.00	3.37	2.00	0.48	0.00	0.00	16.00
	Total	166.00		183.00		66.00		415.00

Table A1.16 – Novelty of Autonomous Systems Technologies and Timeliness in Future Conflict

		Timeliness						
		Near Term		Medium Term		Long Term		Total
		Response	Percentage	Response	Percentage	Response	Percentage	
Novelty	Very High	27.00	6.51	18.00	4.34	23.00	5.54	68.00
	High	52.00	12.53	60.00	14.46	17.00	4.10	129.00
	Moderate	55.00	13.25	78.00	18.80	17.00	4.10	150.00
	Low	20.00	4.82	23.00	5.54	5.00	1.20	48.00
	Very Low	15.00	3.61	2.00	0.48	3.00	0.72	20.00
	Total	169.00		181.00		65.00		415.00

Appendix 2: Survey Questionnaire

Future Technology Threats and Capabilities: A Horizon Scan

Start of Block: Default Question Block

This research aims to understand the opportunities and challenges posed by the new disruptive technologies under investigation in this project including cyber, the Internet-of-(battlefield)-things (IoT/IoBT), artificial intelligence (AI), and autonomous systems. The technologies are cyber-physical in nature and hence overlap with other technologies as well as falling under both civil and military domains. We are seeking your insights as an industry and/or military professional. Your answers will be confidential and only used for this academic research and your participation in this research is voluntary. Your name or any other identifying information will not be included in any of the publications or presentations.

If you decide to take part and later change your mind, you are free to withdraw from the study at any time during the survey, all the information you provided will be destroyed. You will not incur any risks from withdrawing from this project. All data collected will be kept in accordance with Edith Cowan University (ECU) Data Management Policy. Electronic data will be stored on a secure Microsoft SharePoint site provisioned by ECU's IT Services. All records will be stored as required in ECU's Records Management Policy.

The study has been approved by the ECU Human Research Ethics Committee (2020-01485-SEET). If you have any inquiries about the questionnaire, please contact the Chief Investigator: Prof. Pi-Shen Seet E: p.seet@ecu.edu.au P: 08 6304 2486 If you have any concerns or complaints and wish to contact an independent person about this research project, you may contact: Research Ethics Officer, Human Research Ethics Committee, Edith Cowan University 270 Joondalup Drive JOONDALUP WA 6027 Phone: (08) 6304 2170 Email: research.ethics@ecu.edu.au

By proceeding to the next section, completing, and submitting the survey means you have indicated your consent to participate in the research study. Please take your time to answer the following questions. There are no right or wrong answers. Please tick the box that most closely represents you or how you feel. Please complete the whole questionnaire.

1. What is your gender?

2. What is your current age?

3. Where do you live?

4. Which best describes the industry you work in?
   - Cyber/Information Technology
   - The Internet-of-(battlefield)-things (IoT/IoBT)
   - Artificial Intelligence (AI)
   - Autonomous Systems
   - Defence
   - Law enforcement or Emergency Services
   - Science
   - Engineering

5. In which of the following do you have the most experience in?
   - Cyber/Information Technology:
   - The Internet-of-(battlefield)-things (IoT/IoBT):
   - Artificial Intelligence (AI):
   - Autonomous Systems:
   - Defence:
   - Law enforcement or Emergency Services:
   - Science:
   - Engineering:

6. How many years have you worked in the industry you nominated above?

7. Please indicate your degree of knowledge of the following:
   - Cyber/Information Technology:
   - The Internet-of-(battlefield)-things (IoT/IoBT):
   - Artificial Intelligence (AI):
   - Autonomous Systems:
   - Defence:
   - Law enforcement or Emergency Services:
   - Science:
   - Engineering:

8. Potential Impact: How would you evaluate the Impact and the Timeliness/ Time Span of the following disruptive and converging technology categories in future conflicts?
   - Cyber/Information Technology:
   - The Internet-of-(battlefield)-things (IoT/IoBT):
   - Artificial Intelligence (AI):
   - Autonomous Systems:

	Impact					**Timeliness**		
Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)	**Technology Categories**	Near term <5 years (1)	Medium term (5-10 years (2)	Long term >10 years (3)
○	○	○	○	○	Cyber (1)			
○	○	○	○	○	Internet-of-Things (IoT) / Internet of Battlefield Things (IoBT) (2)			
○	○	○	○	○	Artificial Intelligence (AI) (3)			
○	○	○	○	○	Autonomous systems (4)			

9. Likelihood of Deployment or Utilization: How would you evaluate the likelihood of deployment or utilization and the Timeliness/ Time Span of the following disruptive and converging technology categories in future conflicts?
    - Cyber/Information Technology:
    - The Internet-of-(battlefield)-things (IoT/IoBT):
    - Artificial Intelligence (AI):
    - Autonomous Systems:

10. Extensiveness of Use: How would you evaluate the extensiveness of use and the Timeliness/ Time Span of the following disruptive and converging technology categories in future conflicts?
    - Cyber/Information Technology:
    - The Internet-of-(battlefield)-things (IoT/IoBT):
    - Artificial Intelligence (AI):
    - Autonomous Systems:

11. Novelty of Use: How would you evaluate the novelty of use and the Timeliness/ Time Span of the following disruptive and converging technology categories in future conflicts?
    - Cyber/Information Technology:
    - The Internet-of-(battlefield)-things (IoT/IoBT):
    - Artificial Intelligence (AI):
    - Autonomous Systems:

12. What are some specific Cyber technology, Internet of Things (IoT)/ Internet of Battlefield Things (IoBT), Autonomous systems, or Artificial Intelligence (AI) opportunities or threats that defence forces should be investing in or doing research and development (R&D)? Why?

13. Potential Impact: How would you evaluate the Impact and the Timeliness/ Time Span of the following disruptive and converging specific technologies in future conflicts?
    - Cyber Security of critical infrastructure:
    - Network Communications and Information technologies (e.g. for the mission design, structure, and operations
    - Deep/Machine Learning:
    - Swarm intelligence-related technologies and systems
    - Industry 4.0 technologies where the cyber-physical domains merge
    - Civil and military R&D and uses of these technologies
    - Convergence of technologies in strategic industries that support any phases of military operations
    - Optimization and other algorithms
    - Neural Networks:
    - Smart Sensors

	Impact				Specific technologies	timeliness		
○	○	○	○	○	Cyber Security of critical infrastructure (1)			
○	○	○	○	○	Network Communications and Information technologies (e.g. for the mission design, structure, and operations) (2)	○	○	○
○	○	○	○	○	Swarm intelligence-related technologies and systems (3)	○	○	○
○	○	○	○	○	Industry 4.0 technologies where the cyber-physical domains merge (4)	○	○	○
○	○	○	○	○	Civil and military R&D and uses of these technologies (5)	○	○	○
○	○	○	○	○	Convergence of technologies in strategic industries that support any phases of military operations (6)	○	○	○
○	○	○	○	○	Unmanned and autonomous systems (7)	○	○	○
○	○	○	○	○	Optimisation and other algorithms (8)	○	○	○
○	○	○	○	○	Neural Networks (9)	○	○	○
○	○	○	○	○	Smart Sensors (10)	○	○	○
○	○	○	○	○	Deep/Machine Learning (11)	○	○	○

14. Likelihood of Deployment or Utilization: How would you evaluate the likelihood of deployment or utilization and the Timeliness/ Time Span of the following disruptive and converging specific technologies in future conflicts?
    - Cyber Security of critical infrastructure
    - Network Communications and Information technologies (e.g. for the mission design, structure, and operations
    - Deep/Machine
    - Swarm intelligence-related technologies and systems
    - Civil and military R&D and uses of these technologies
    - Industry 4.0 technologies where the cyber-physical domains merge
    - Unmanned and autonomous systems
    - Optimization and other algorithms
    - Neural Networks
    - Smart Sensors:

15. Extensiveness of use in the deployment or utilization: How would you evaluate the Extensiveness of use in the deployment or utilization and the Timeliness/ Time Span of the following disruptive and converging specific technologies in future conflicts?
    - Cyber Security of critical infrastructure
    - Network Communications and Information technologies (e.g. for the mission design, structure, and operations
    - Deep/Machine
    - Swarm intelligence-related technologies and systems
    - Civil and military R&D and uses of these technologies
    - Industry 4.0 technologies where the cyber-physical domains merge
    - Unmanned and autonomous systems
    - Optimization and other algorithms
    - Neural Networks
    - Smart Sensors

16. Novelty of use: How would you evaluate the novelty of use and the Timeliness/ Time Span of the following disruptive and converging technology categories in future conflicts in the Short term (less than 5 years)?
    - Cyber Security of critical infrastructure
    - Network Communications and Information technologies (e.g. for the mission design, structure, and operations
    - Deep/Machine
    - Swarm intelligence-related technologies and systems
    - Civil and military R&D and uses of these technologies
    - Industry 4.0 technologies where the cyber-physical domains merge
    - Unmanned and autonomous systems
    - Optimization and other algorithms
    - Neural Networks

- Smart Sensors

17. Current ADF Capability Gap: Based on your knowledge of the Australian Defence Force (ADF), how would you evaluate the current capability gap in the ADF in the following disruptive and converging technology categories in future conflicts?
    - Cyber
    - Internet-of-Things (IoT) / Internet of Battlefield Things (IoBT Cyber
    - Artificial Intelligence (AI)
    - Autonomous systems:

	Current ADF Capability Gap				
Technology categories	Very behind (1)	Behind (2)	On Par (3)	Ahead (4)	Very ahead (5)
Cyber (1)	○	○	○	○	○
Internet-of-Things (IoT) / Internet of Battlefield Things (IoBT) (2)	○	○	○	○	○
Artificial Intelligence (AI) (3)	○	○	○	○	○
Autonomous systems (4)	○	○	○	○	○

18. Given your knowledge of the Australian Defence Force (ADF), how would you evaluate the current capability gap of the ADF in the following specific disruptive and converging technologies in future conflicts?
    - Cyber Security of critical infrastructure
    - Network Communications and Information technologies (e.g. for the mission design, structure, and operations)
    - Swarm intelligence-related technologies and systems
    - Industry 4.0 technologies where the cyber-physical domains merge:
    - Civil and military R&D and uses of these technologies
    - Convergence of technologies in strategic industries that support any phases of military operations
    - Unmanned and autonomous systems
    - Optimization and other algorithms
    - Neural Networks
    - Smart Sensors

- Deep/Machine Learning

Specific technologies	Very behind (1)	Behind (2)	On Par (3)	Ahead (4)	Very ahead (5)
Cyber Security of critical infrastructure (1)	○	○	○	○	○
Network Communications and Information technologies (e.g. for the mission design, structure, and operations) (2)	○	○	○	○	○
Swarm intelligence-related technologies and systems (3)	○	○	○	○	○
Industry 4.0 technologies where the cyber-physical domains merge (4)	○	○	○	○	○
Civil and military R&D and uses of these technologies (5)	○	○	○	○	○
Convergence of technologies in strategic industries that support any phases of military operations (6)	○	○	○	○	○
Unmanned and autonomous systems (7)	○	○	○	○	○
Optimisation and other algorithms (8)	○	○	○	○	○
Neural Networks (9)	○	○	○	○	○
Smart Sensors (10)	○	○	○	○	○
Deep/Machine Learning (11)	○	○	○	○	○

19. Urgency of investment priority: Given your knowledge of the current domestic and international environment, what urgency of investment priority should the government make in these technology categories for future conflicts ?

- Cyber
- Internet-of-Things (IoT) / Internet of Battlefield Things (IoBT)
- Artificial Intelligence (AI)
- Autonomous systems

	urgency of investment priority				
Technology categories	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Cyber (1)	○	○	○	○	○
Internet-of-Things (IoT) / Internet of Battlefield Things (IoBT) (2)	○	○	○	○	○
Artificial Intelligence (AI) (3)	○	○	○	○	○
Autonomous systems (4)	○	○	○	○	○

20. Urgency of investment priority: Given your knowledge of the current domestic and international environment, to what **urgency of investment priority** should the government make in these **specific technologies** categories for future conflicts
    - Cyber Security of critical infrastructure
    - Network Communications and Information technologies (e.g. for the mission design, structure, and operations)
    - Swarm intelligence-related technologies and systems
    - Industry 4.0 technologies where the cyber-physical domains merge
    - Civil and military R&D and uses of these technologies
    - Convergence of technologies in strategic industries that support any phases of military operations
    - Unmanned and autonomous systems
    - Optimization and other algorithms
    - Neural Networks
    - Smart Sensors
    - Deep/Machine Learning

	urgency of investment priority				
Specific technologies	Extremely Low (1)	Low (2)	Moderate (3)	High (4)	Extremely High (5)
Cyber Security of critical infrastructure (1)	○	○	○	○	○
Network Communications and Information technologies (e.g. for the mission design, structure, and operations) (2)	○	○	○	○	○
Swarm intelligence-related technologies and systems (3)	○	○	○	○	○
Industry 4.0 technologies where the cyber-physical domains merge (4)	○	○	○	○	○
Civil and military R&D and uses of these technologies (5)	○	○	○	○	○
Convergence of technologies in strategic industries that support any phases of military operations (6)	○	○	○	○	○
Unmanned and autonomous systems (7)	○	○	○	○	○
Optimisation and other algorithms (8)	○	○	○	○	○
Neural Networks (9)	○	○	○	○	○
Smart Sensors (10)	○	○	○	○	○
Deep/Machine Learning (11)	○	○	○	○	○

21. Write a future statement concerning the employment of future technology in the defence sector in 10 years' time.(e.g. Info-communication technology (ICT) and artificial intelligence (AI) will dissipate and develop quickly and widely in robotics which will enhance the development of human intellectual capacity in the battlespace)

22. Are there any other aspects regarding the sources and impact of Future Technology, Threats and Capabilities for defence forces that researchers and the government should be considering or considering? Why should it invest?

23. What is your place of birth?

24. Are you an Australian citizen?
    - No (please specify your nationality):Are you an Australian citizen?

25. What is the highest education level you achieved?