INDO-PACIFIC
INSIGHT SERIES

Technopolitik: Technology, geostrategic competition and warfare

Alana Ford, Perth USAsia Centre

Volume 25, August 2025

Perth USAsia Centre
INDO-PACIFIC STRATEGY

KEY MESSAGES

1. Technology is reshaping strategic competition and warfare—transforming how, where, and by whom power is exerted.
2. Advanced technologies—such as AI, cyber tools, and autonomous systems—are not neutral; they are now critical instruments of geopolitical influence, disruption, and control.
3. Hybrid and irregular warfare increasingly blur the lines between peace and conflict, using low-cost, tech-enabled tactics, often below the threshold of conventional war.
4. China's grey zone pressure on Taiwan and North Korea's illicit crypto operations are examples of how the Indo-Pacific region has become a key theatre of high-tech competition, coercion and influence.
5. Australia must cut through bureaucratic inertia and accelerate long term capability development to adapt to this new era.

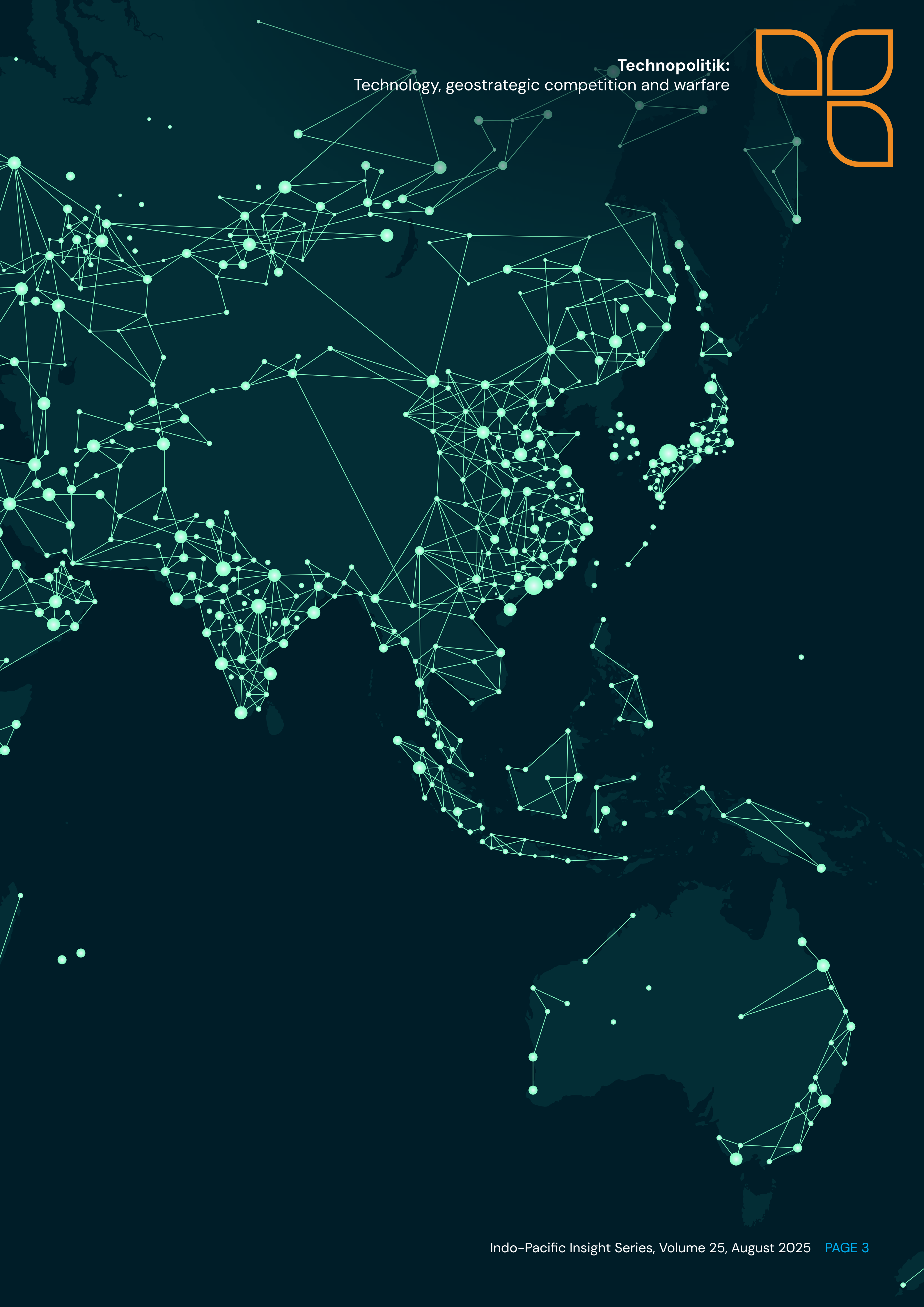
INTRODUCTION

The Indo-Pacific region is increasingly defined by strategic tension, where competition between major powers plays out not only through military posturing, but through influence campaigns, economic coercion, and technological edge. For governments, industries, and communities in the region, this matters deeply—because the contest for *power, influence, and legitimacy*[1] is no longer limited to distant battlefields or diplomatic backrooms. It is unfolding across our digital infrastructure, our supply chains, and even our public discourse. Understanding this evolving landscape is essential for anyone working to secure a stable, sovereign, and resilient Indo-Pacific future.

> “In an era defined by technological advancement, strategic competition and hybrid warfare, the battlefield isn't just in the sea, air, and land domains—it's also in the information domain.”

Advancements in cyber capabilities, artificial intelligence, autonomous systems, robotics, surveillance tools, and quantum computing are enabling actors to project power, shape narratives, disrupt adversaries, and conduct military operations in ways never seen before. As a result, technology has become both a domain of competition and a weapon within it, blurring the lines between war and peace, combatant and civilian, and influence and coercion.

For Australia, this is not a distant concern, but a national imperative demanding action from across government, industry, and society more broadly.



1 KEY CONCEPTS

Strategic competition	A systemic rivalry between major powers (such as US-China) playing out across military, economic and normative domains.[2] In the Indo-Pacific, strategic competition is now shaped by technological dominance, alliance-building, and influence operations.[3]
Technopolitik	*Technopolitik*, for the purposes of this paper, is a nod to the term *Realpolitik*,[4] and refers to the strategic use of technology to influence geopolitical dynamics and assert national interests. Technology is not neutral – it's a geostrategic asset used by states to project power, influence narratives, disrupt economies and create dependencies.
Hybrid warfare	Hybrid warfare blends conventional military operations with unconventional tools such as cyber-attacks, information operations, and economic coercion to achieve strategic goals. These can be both covert and overt.[5,6] Hybrid tactics can be used across the full spectrum of conflict, from peacetime to full-scale war.
Irregular warfare	Irregular warfare is similar to hybrid warfare, but is typically conducted by non-state, proxy or state-backed actors below the threshold for conventional war. It is generally more asymmetric in nature, and involves the use of unconventional tactics like insurgency, guerrilla warfare, sabotage, subversion, and influence operations.[7]
Advanced technology	In the context of strategic competition, advanced technology refers to cutting-edge innovations, such as artificial intelligence, quantum computing, autonomous systems, biotechnology, and cyber capabilities, that are reshaping the global balance of power. Advanced technologies are not merely tools of progress but instruments of influence, control, and disruption. They are increasingly seen as critical national assets that underpin military advantage, economic competitiveness, and geopolitical leverage.

2 STRATEGIC COMPETITION IN THE ADVANCED TECH ERA

Strategic competition is not new, indeed it defined the 20th century from World War I, the Cold War standoff between the US and the Soviet Union, through to the current era of rivalry between the US and China.

> “ In earlier eras, great power rivalry centred on conventional military strength, territorial control and industrial capacity. Today, competition blends military, economic, political and informational tools, each enabled by digital technologies. ”

The increasing ubiquity of advanced technology has not changed why strategic competition occurs. The overarching goals of power, influence and legitimacy remain the same. What **has** fundamentally changed, however, is how, where and who takes part.

SOME OF THE KEY CHANGES INCLUDE:

Change	**Example**
More than ever, the means and methods of strategic competition are rapid, low cost, and often covert.	Russia's use of "little green men" and unmarked cyber incursions during the 2014 Crimea annexation demonstrated how plausible-deniable state action—using covert forces and cyber tools—could rapidly shift facts on the ground without conventional warfare.[8]
The relatively low barrier to entry and cost of more ubiquitous technologies mean that competition is increasingly asymmetric, opening the door to non-traditional and small state actors.	During the Russia-Ukraine war, Ukrainian hacktivist collectives infiltrated a Russian drone manufacturer's network—deleting 47 terabytes of data and disrupting its production capabilities—demonstrating how relatively small, tech-savvy non-state actors can deliver high-impact results on a strategic scale.[9]
Offensive cyber operations and cyber espionage have emerged as central elements of strategic competition, giving new means to attack, sabotage, undermine, spy, and influence.[10]	Multiple China-linked hacker groups exploited a vulnerability in Microsoft SharePoint servers in July 2025, compromising as many as 100 government, industrial, and healthcare organisations across the US and Germany.[11]
AI, big data, and digital surveillance now have a significant impact on intelligence and military decision-making.[12]	During Exercise Talisman Sabre 2025, Australian and allied forces tested AI-driven systems like the SAF-Foresight 3D tool and BigBear.ai's ConductorOS to fuse real-time sensor data and improve soldier safety and command decisions.[13]
Modern technology can be used for economic coercion or to target critical infrastructure.	In November 2020, India's Maharashtra state power grid was knocked offline in a highly sophisticated cyberattack—widely attributed to China-backed actors—highlighting how adversaries now weaponise digital tools to create economic disruption and threaten critical infrastructure.[14]
Digital communications and cyber capabilities can be used to erode public support, damage trust in institutions, and create societal divisions.	Ahead of Australia's Indigenous Voice to Parliament referendum, China-linked accounts amplified far-right narratives online, demonstrating how foreign digital influence campaigns can damage institutional trust and polarize domestic discourse.[15]
Digital communications and real-time information sharing have profoundly changed Command, Control and Communication (C3) structures.	Modern communications systems allow for real-time battlefield decision-making, provide tactical advantages that would not be possible with analogue systems, and allow for communications from remote and hostile locations for more extended periods of time.[16]

Innovation and supply chains, particularly in relation to AI or critical minerals, have also emerged as key points of tension in today's era of great power rivalry. In a competition now facilitated by digital tools, actors have a vested interest in monopolising both the innovation and supply of these critical assets.

3 TECHNOLOGY IS RESHAPING CONFLICT AND WARFARE

Like strategic competition, the impact of technology on conflict and warfare has been profound.

For example, on 1 June 2025, Ukraine conducted ‘Operation Spiderweb’, a drone attack that targeted Russia’s long-range bomber fleet.[17] The operation used 116 small-strike drones, smuggled into Russia disguised as cargo in trucks, to simultaneously attack four Russian airbases. Control was maintained using Russian communications networks and AI-driven course-correction capabilities.[18] The tactical ingenuity, low cost, and technological aspects of this attack make it a compelling example of how the asymmetric warfare playbook is being rewritten, and how tech-enabled tactics can cripple a larger adversary’s strategic assets. The attack was coordinated, multi-theatre, and long-range using low-cost technologies, paired with non-kinetic means of warfare, like deception and strategic surprise.

Some of the most significant changes to conflict and warfare include:

- The battlefield is no longer just in the sea, air or land. It has expanded to new domains, with cyberspace, outer space, and the electromagnetic spectrum now critical arenas for military operations.[19]
- Warfare is increasingly conducted through remote and autonomous systems (such as drones and robotics), reducing risk to personnel and changing the rules of engagement.[20]
- Digital communications, AI and automation are accelerating the speed of warfare, enabling faster targeting, decision-making, and situational awareness.[21]
- Cyberattacks can now disable or degrade enemy capabilities without a single shot being fired—crippling command systems, jamming communications, or disrupting logistics and infrastructure.[22]
- Information warfare and psychological operations have become central to military campaigns, using digital tools to manipulate perception and morale.[23]
- Precision-guided munitions and networked weapons systems have increased the lethality and accuracy of strikes.[24]
- Commercial and dual-use technologies have blurred the line between civilian and military assets, making critical systems more vulnerable and conflict more legally and ethically complex.[25]

4 STRATEGIC FORESIGHT: WHAT COMES NEXT?

Predicting the future impact of technology on strategic competition and warfare is challenging. Innovation and tech adoption cycles move at a pace that far outstrips policymaking, which often only accelerates in times of crisis. However, there are some themes that are widely discussed among technologists, policy commentators and thought leaders.

1. **AI-Powered cognitive warfare**
AI will increasingly supercharge information and psychological operations.[26] Adversaries will deploy personalised influence campaigns at scale, blending real and synthetic content to manipulate public opinion and erode societal trust.

2. **Quantum disruption of cyber norms**
Quantum computing may have the future potential to render current encryption obsolete.[27,28] States with early adoption of quantum capabilities could gain near-total access to sensitive data, triggering a paradigm shift in cyber defence, espionage, and secure communications.

3. **Autonomous conflict at machine speed**
While controversial and debated amongst military experts, decision loops may shrink as autonomous systems and AI begin to conduct parts of the OODA (Observe-Orient-Decide-Act) loop without human input.[29] The risks of accidental escalation or algorithmic error would rise, potentially leading to conflict or harm.

4. **Fragmentation of tech ecosystems**
Decoupling between US-led and China-led technology ecosystems will intensify. This technological bifurcation will redefine everything from internet standards to supply chains, placing increased pressure on middle powers to choose or hedge.[30]

5. **Weaponisation of everyday tech**
Commercial platforms, personal devices, and IoT systems will increasingly be exploited for strategic ends—from smart appliances used in botnets (a network of hijacked devices controlled remotely), to social media exploited for influence operations.[31]

6. **Grey zone expansion**
Hybrid operations will intensify in areas like infrastructure sabotage, election interference, subsea cable interference, and space-based disruption—all falling below the threshold of war but eroding sovereignty.

Technopolitik in Action:
Case Studies from the Indo-Pacific

CHINA'S GREY ZONE TACTICS AGAINST TAIWAN

China continues to apply pressure on Taiwan through a combination of grey zone tactics that stop short of full-scale military conflict.[32] These include frequent routine incursions by drones and surveillance aircraft, disinformation campaigns, and coordinated cyber operations designed to erode public confidence and test Taiwan's defences. This strategy reflects a broader trend of using low-cost, high-deniability, tech-enabled tools to reshape strategic environments without triggering armed conflict.

NORTH KOREA'S ILLICIT FINANCING OF WEAPONS PROGRAM

North Korea has significantly escalated its use of cyber-enabled financial crimes to circumvent sanctions and fund its weapons programs. State-backed hacking groups have engaged in extensive cryptocurrency theft, ransomware attacks, and blockchain manipulation to secure illicit revenue streams. These activities have helped fund its weapons programs despite heavy global restrictions. In 2022 alone, North Korea is estimated to have stolen over US$1 billion in cryptocurrency.[33]

5 FROM INSIGHT TO ACTION: AUSTRALIA'S NATIONAL IMPERATIVE

Technology is not just reshaping the character of strategic competition and conflict—it is accelerating it. The pursuit of power, influence, and legitimacy endures, but the means of contest have fundamentally shifted.

Australia is not immune to these shifts. In fact, we are at a pivotal juncture. Our ability to navigate this new era of *technopolitik*—to be relevant, secure, and influential—will depend on how quickly and decisively we adapt.

This demands a sizable cultural and institutional shift. Australia cannot afford to let ambition be stifled by bureaucracy and election-cycles. We need to cut through the red tape, fast-track capability development, and empower those at the coalface of innovation—whether in defence industry, academia, or the otherwise. Every delay is a liability, and every missed opportunity is space ceded to adversaries who are already moving at speed.

AUKUS Pillar II is one powerful lever for signalling ambition and accelerating capability. It represents a tangible mechanism for trilateral cooperation on advanced technologies, and a vehicle to build deeper trust and interoperability with key allies. But it is not the only mechanism. AUKUS alone cannot transform Australia into a technology-capable strategic actor. We must pursue parallel efforts, including through regional partnerships with likeminded middle powers like Japan, through domestic reform, and through whole-of-nation investment in innovation, skills, and resilience.

Australia needs to:

- Ramp up investment and support for building sovereign dual-use technology capabilities,
- Create a national fast lane for defence and critical technology that removes the burden of slow procurement and capability development cycles,
- Mobilise state and local governments as security actors, which are currently underutilised but can often be the first hit by hybrid threats (e.g. a cyberattack on a hospital or port), and
- Make national resilience and preparedness everyone's business.

If Australia gets this right, we can help shape a more stable, secure and sovereign future in a region being rapidly redefined by technology. If we get it wrong, others will continue to shape it for us.

ENDNOTES

[1] Rebecca Patterson et al. (2024), *Winning Without Fighting: Irregular Warfare and Strategic Competition in the 21st Century*, Cambria Press, https://www.cambriapress.com/pub.cfm?bid=1165

[2] RAND Project AIR FORCE (2020), *U.S.-China Competition in the Indo-Pacific*, https://www.rand.org/paf/projects/us-china-competition.html

[3] James Van de Valde (2024), *What is 'strategic competition' and are we still in it?*, The SAIS Review of International Affairs, https://saisreview.sais.jhu.edu/what-is-strategic-competition-and-are-we-still-in-it/

[4] John Bew (2017), *RealPolitik: A History*, Foreign Affairs, https://www.foreignaffairs.com/reviews/capsule-review/2017-04-14/realpolitik-history

[5] North Atlantic Treaty Organisation (2024), *Countering hybrid threats*, https://www.nato.int/cps/en/natohq/topics_156338.htm

[6] Alana Ford (2025), *Disinformation and cognitive warfare*, Perth USAsia Centre, https://perthusasia.edu.au/research-and-insights/publications/disinformation-and-cognitive-warfare/

[7] Rebecca Patterson et al. (2024), *Winning Without Fighting: Irregular Warfare and Strategic Competition in the 21st Century*, Cambria Press, https://www.cambriapress.com/pub.cfm?bid=1165

[8] Robert Muller (2024), *Russia's use of little green men in the conflict in Ukraine*, Medium, https://medium.com/@DrRobertMuller/russias-use-of-little-green-men-in-the-conflict-in-ukraine-95ece34741ad

[9] Daryna Antoniuk (2025), *Ukraine-aligned hackers claim cyberattack on major Russian drone supplier*, The Record, https://therecord.media/ukraine-hackers-claim-attack-russia-gaskar-group-drone-maker

[10] Tom Uren et al. (2018), *Defining offensive cyber capabilities*, Australian Strategic Policy Institute, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities/

[11] James Pearson and Raphael Satter (2025), *Microsoft server hack hit about 100 organisations, researchers say*, Reuters, https://www.reuters.com/sustainability/boards-policy-regulation/microsoft-server-hack-hit-about-100-organizations-researchers-say-2025-07-21/

[12] Sarah Grand Clément (2023), *Artificial Intelligence Beyond Weapons: Application and Impact of AI in the Military Domain*, UNIDIR, https://unidir.org/wp-content/uploads/2023/10/UNIDIR_AI_Beyond_Weapons_Application_Impact_AI_in_the_Military_Domain.pdf

[13] Robert Dougherty (2025), *ConductorOS AI system locks in Exercise Talisman Sabre 2025 appearance*, Defence Connect, https://www.defenceconnect.com.au/industry/15682-conductoros-artificial-intelligence-system-locks-in-exercise-talisman-sabre-2025-appearance

[14] Reuters (2021), *Mumbai power outage could have been cyber sabotage*, says minister, https://www.reuters.com/article/world/mumbai-power-outage-could-have-been-cyber-sabotage-says-minister-idUSKCN2AT31P/

[15] Tom McIlroy (2023), *Trolls, China spreading Voice disinformation*, Australian Financial Review, https://www.afr.com/politics/federal/trolls-china-spreading-voice-disinformation-20230828-p5dzvm

[16] Omnetics (2023), *The evolution of military comms: From radios to advanced digital systems*, Army Technology, https://www.army-technology.com/sponsored/the-evolution-of-military-comms-from-radios-to-advanced-digital-systems/

ENDNOTES *Continued*

17 Kateryna Bondar (2025), *How Ukraine's Operation "Spider's Web" redefines Asymmetric Warfare*, Center for Strategic & International Studies, https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare

18 Dylan Malyasov (2025), *Ukraine uses AI drones to target Russian bombers*, Defence Blog, https://defence-blog.com/ukraine-uses-ai-drones-to-target-russian-bombers/

19 Lieutenant Colonel Athanasios Sdrakas GR AF (2025), *Navigating the Digital Battlefield: Understanding Cyber Electromagnetic Activities in Warfare*, The Journal of the JAPCC, Joint Air Power Competence Centre, Edition 39, https://www.japcc.org/articles/navigating-the-digital-battlefield/

20 Brandon Schingh (2025), *The Future of Warfare: Autonomous Technologies in Modern Conflict*, Small Wars Journal, https://smallwarsjournal.com/2025/01/28/the-future-of-warfare-autonomous-technologies-in-modern-conflict/

21 Mohammad Atif Khan (2024), *AI-Driven Tactical Communication and Networking for Defense for Enhancing Situational Awareness, Security, and Autonomous Decision-Making in Modern Warfare*, International Journal of Engineering and Science Invention, Vol. 13 Issue. 12, https://www.ijesi.org/papers/Vol%2813%29i12/13127987.pdf

22 Jason Healey (2024), *Cyber Effects in Warfare: Categorising the Where, What, and Why*, Texas National Security Review, Vol. 7 Issue 4, https://tnsr.org/2024/08/cyber-effects-in-warfare-categorizing-the-where-what-and-why/

23 Alana Ford (2025), *Disinformation and cognitive warfare*, Perth USAsia Centre, https://perthusasia.edu.au/research-and-insights/publications/disinformation-and-cognitive-warfare/

24 Lieutenant Colonel Francesco Esposito IT AF (2019), *Precision-Guided Munitions of the Future: And the Related Challenges to NATO*, The Journal of the JAPCC, Joint Air Power Competence Centre, Edition 28, https://www.japcc.org/articles/precision-guided-munitions-of-the-future/

25 Ruben Stewert (2025), *The shifting battlefield: technology, tactics, and the risk of blurring lines in warfare*, International Committee of the Red Cross, https://blogs.icrc.org/law-and-policy/2025/05/22/the-shifting-battlefield-technology-tactics-and-the-risk-of-blurring-lines-of-warfare/

26 Alana Ford (2025), *Disinformation and cognitive warfare*, Perth USAsia Centre, https://perthusasia.edu.au/research-and-insights/publications/disinformation-and-cognitive-warfare/

27 Markus Pflitsch (2023), *Quantum Computers Could Make Today's Encryption Defenseless*, Forbes, https://www.forbes.com/councils/forbestechcouncil/2023/05/04/quantum-computers-could-make-todays-encryption-defenseless/

28 Sead Fadilpašić (2025), *Forget ransomware – most firms think quantum computing if the biggest security risk to come*, Tech Radar, https://www.techradar.com/pro/security/forget-ransomware-most-firms-think-quantum-computing-is-the-biggest-security-risk-to-come

29 Owen Daniels (2021), *Speeding Up the OODA Loop with AI: A Helpful or Limiting Framework?*, Joint Air & Space Power Conference 2021 Read Ahead, Joint Air Power Competence Centre, https://www.japcc.org/essays/speeding-up-the-ooda-loop-with-ai/

30 Jon Bateman (2022), *U.S.-China Technological 'Decoupling': A Strategy and Policy Framework*, Carnegie Endowment for International Peace, https://carnegieendowment.org/research/2022/04/us-china-technological-decoupling-a-strategy-and-policy-framework/?lang=en

31 Moemedi Lefoane et al. (2025), *Internet of Things botnets: A survey on Artificial Intelligence based detection techniques*, Journal of Network and Computer Applications, Vol. 236, https://www.sciencedirect.com/science/article/pii/S1084804525000074

32 Derek Grossman (2025), *The Chinese Communist Party's Gray Zone Tactics Against Taiwan*, RAND, https://www.rand.org/pubs/external_publications/EP70899.html

33 Michelle Nichols (2024), *Exclusive: North Korea laundered $147.5 mln in stolen crypto in March*, say UN experts, Reuters, https://www.reuters.com/technology/cybersecurity/north-korea-laundered-1475-mln-stolen-crypto-march-say-un-experts-2024-05-14/

ABOUT THE AUTHOR

Alana leads the Centre's work on critical and emerging issues, with a particular focus on cyber and tech policy. She brings to the role extensive experience working on these issues for the Commonwealth Government in Australia and internationally, as well as passion for driving social impact and policy change at the intersection of technology and society.

Prior to joining the Perth USAsia Centre, Alana served as the Attorney General Department's representative to the United States in Washington D.C. In this role, she led the Australian Government's efforts to address online harms and criminal exploitation of technology, as well as other high profile national security, law enforcement and criminal justice matters.

Previously, she served in the Department of Home Affairs, where she led work on a broad range of national security issues, including cyber and digital technology policy, law enforcement policy, countering online terrorism, child exploitation, and intelligence.

Alana's expertise extends beyond her public service, with a strong commitment to responsible tech advocacy and leadership through her position on the Board of Directors at the Data Federation Lab.

in https://www.linkedin.com/in/alana-ford1/

Perth USAsia Centre

ABOUT PERTH USASIA CENTRE

The Perth USAsia Centre is a leading think tank focused on Indo-Pacific strategy. Through our research and educational activities, we strengthen relationships and strategic thinking between Australia, the Indo-Pacific, and the United States. Based at the University of Western Australia, we are a non-partisan and not-for profit institution. We engage thought leaders across government, business, and academia to address challenges and opportunities in the Indo-Pacific region. Since the Centre's inception in 2013, we have hosted more than 750 events across 25 cities in 10 countries, and engaged a world-class community of over 27,000 strategic thinkers and policy leaders.

ACKNOWLEDGEMENTS

The Perth USAsia Centre would like to thank the wide range of individuals who have supported the production of this report. Many other individuals – across business, government and academia – kindly offered insights, information and feedback that have enriched the report. Nonetheless, the author is responsible for all content and arguments contained herein.

Perth USAsia Centre

INDO–PACIFIC
INSIGHT SERIES

Technopolitik: Technology, geostrategic competition and warfare

Alana Ford, Perth USAsia Centre

Volume 25, August 2025