The Good Ancestors Project

contact@goodancestors.org.au
ABN: 94 660 287 963

The implications of global catastrophic risk for Australia's strategic environment

The Defence Strategic Review calls for an outline of the "future strategic challenges facing Australia, which may require an Australian Defence Force operational response." Australia's national security and defence establishment is highly capable in understanding the strategic environment and traditional threats to Australia's national security interests. As past Defence doctrine clearly outlines, these threats include strategic competition, military capability and modernisation, terrorism and violent extremism, state fragility, coercive and grey-zone activities and emerging and disruptive technologies.

The Department of Defence must also play a central role in preparing for several major strategic challenges facing Australia that appear to receive little consideration in Defence strategic thinking, planning and investment priorities. These challenges belong in a special class of risk: global catastrophic risk (GCR).

Global catastrophic risks can be broadly defined as risks consequential enough to significantly harm human civilisation on a global scale. These risks - such as nuclear catastrophe, extreme climate change, threats induced by artificial intelligence (AI), engineering pathogens and space weather - represent the worst-case scenarios. They might be highly unlikely or uncertain. But they are not speculative or unrealistic. Indeed, it is these tail risks that require attention by the Australian national security community, and the Department of Defence specifically.

Our closest allies are already considering these risks. For example, the US National Intelligence Council highlighted these risks in their most recent Global Trends Report, the US Intelligence Community's flagship report for the incoming Presidential administration every four years:

> "Technological advances may increase the number of existential threats; threats that could damage life on a global scale challenge our ability to imagine and comprehend their potential scope and scale, and they require the development of resilient strategies to survive. Technology plays a role in both generating these existential risks and in mitigating them. [Human-induced] risks include runaway AI, engineered pandemics, nanotechnology weapons, or nuclear war."

The UK Government's upcoming National Resilience Strategy will prioritise the handling of complex and catastrophic risk:

> "Some risks are very unlikely to happen, but would have impacts or knock-on consequences that would be so widely felt that they require bespoke planning measures. Examples of this type of catastrophic risk might include: chemical, biological, radiological and nuclear (CBRN) risks; Artificial Intelligence risks; or widespread power outages. Learning the lessons from COVID-19, we need to build a more effective system for

> handling these complex risks. This should include assessing the whole range of potential impacts ahead of time, and ensuring we have sufficient oversight structures in place to assure adequate planning in place….Some other more existential risks (such as a large meteor strike on our planet) are statistically so unlikely that it may not be practicable for the Government to plan for them. There is nevertheless an important role for others to play in monitoring these risks and indicating any changes in their likelihood."

The Secretary General of the United Nations also recognised global catastrophic risks in his 2021 'Our Common Agenda' report:

> "These risks are now increasingly global and have greater potential impact. Some are even existential: with the dawn of the nuclear age, humanity acquired the power to bring about its own extinction. Continued technological advances, accelerating climate change and the rise in zoonotic diseases mean the likelihood of extreme, global catastrophic or even existential risks is present on multiple, interrelated fronts. Being prepared to prevent and respond to these risks is an essential counterpoint to better managing the global commons and global public goods."

Defence's primary focus is, justifiably, on conventional national security challenges, such as global conflict, regional security and national defence. And some of the risks that could become globally catastrophic are not unknown to Defence. Weapons of mass destruction, for example, is a long-standing issue for Australia and the Department of Defence. However, the globally catastrophic end of the risk spectrum is rarely, if ever, explored or factored into contingency planning. Intense and cascading global risks are likely to occur more frequently in the coming decades. And rising geopolitical tensions and a more contested world are likely to further exacerbate such risks.

The Defence Strategic Review should therefore give practical and urgent direction to the Department of Defence in several major areas of global catastrophic risk. The individual risks have implications for Australia's strategic environment and national security. Defence investments and capabilities could be devoted to understanding the risks. And Defence planning and preparedness may be required to build Australia's resilience.

Efforts towards understanding or reducing global catastrophic risks do not necessarily require significant resourcing, nor a change in remit. Defence assets and capabilities - particularly in the intelligence, science and technology domains - could relatively easily dedicate a minimal effort to global catastrophic risk with potentially very high pay-off for national and international security.

This submission does not cover all the global catastrophic risks. It highlights six key areas where Defence has a critical role to play in helping the Australian Government and the nation of Australia better understand, prevent and prepare for these risks. For each area, the submission provides practical recommendations that require very modest resource requirements. Specifically, this submission covers:

- Understanding and assessing global catastrophic risk

- Nuclear catastrophe and winter
- Artificial intelligence's impact on nuclear risk
- Catastrophic climate change
- Engineered pathogens
- Space weather and Near-Earth objects

Defence's mission and purpose is to "defend Australia and its national interests in order to advance Australia's security and prosperity." Defence must consider all threats and hazards, no matter how or from where they might arise, no matter how complex or unexpected. Australia and its citizens rely on Defence to think about and prepare for worst-case scenarios. Defence will have failed in that duty if it ignores global catastrophic risk.

Fundamentally, global catastrophic risk represents one of the greatest shared challenges of the coming decades. And Australia has an opportunity to lead globally on this issue. The Department of Defence can be one of Australia's greatest assets in leading that charge.

References and further reading

*United States National Intelligence Council. "*Global Trends 2040: A More Contested World." 2021. https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf, 65.

United Kingdom Cabinet Office. "The National Resilience Strategy: A Call for Evidence." 2021, 17.

United Nations."Our Common Agenda: Report of the Secretary-General." September 2021.

Understanding and assessing global catastrophic risk

Future strategic challenge: Global catastrophic risk (GCR) refers to the potential for certain threats or hazards to inflict significant damage to human wellbeing on a global scale. Global catastrophic risks are a particularly difficult national security challenge because they are highly uncertain, novel and with global implications. Navigating the complexity of such threats requires urgent and substantive support from Defence's intelligence, scientific and technology community.

Recommendation: Defence should devote a small but specific intelligence resourcing towards GCR. Defence could also better leverage the expertise of the Defence Science and Technology Group (DSTG) to model risks and produce robust and regular strategic assessments on relevant worst-case scenarios. Greater inter-agency coordination between DIO, DSTG and other agencies on these risks is also critical.

Global catastrophic risk (GCR) refers to the potential for certain threats or hazards to inflict significant damage to human wellbeing on a global scale. The community of academics, researchers and practitioners that study these risks continue to debate, assess and analyse the specific global catastrophic risks. There is strong consensus that certain risks could cause up to billions of deaths or put humanity so far back in its development it might never recover.

The study of these risks is based on scientific and empirical approaches. It is not a speculative or unsophisticated endeavour. In the past two decades, an integrated field of highly acclaimed institutions have formed specifically to study this tail risk to humanity. The Centre for the Study of Existential Risk at the University of Cambridge and the Future of Humanity Institute at the University of Oxford, for example, are pioneers in the field. The academic and scientific research mostly revolves around the set of risks, their potential likelihood and impact, the pathways and scenarios, possible solutions to reduce the risk, ways to build resilience, and the broader human, societal, political, economic and security implications.

Global catastrophic risk is particularly challenging from a national security and defence perspective. First, the magnitude of these low-level, high-impact risks warrants serious cause for concern and consideration. The scale of death and suffering of a global catastrophe would be incredibly high. The individual risks might be highly unlikely. But by virtue of their catastrophic impact, they present a major challenge to national security and prosperity.

Second, there remains a high degree of uncertainty and complexity surrounding these risks. Analysis, tracking and warning of the risks is an important function. How these risks could unfold, when they could occur and how likely the scenarios are renders them difficult problems to analyse and devote policy resources towards. Australia's defence intelligence community can help the Government navigate this difficulty. As the National Intelligence Council emphasises in their Global Trends 2040 report, "such low-probability, high-impact events are difficult to

forecast and expensive to prepare for but identifying potential risks and developing mitigation strategies in advance can provide some resilience to exogenous shocks."

Finally, many of the risks are novel or emerging. This requires strong foresight and horizon-scanning. Numerous catastrophic technology-based threats, such as artificial intelligence and bioengineering, are yet to be fully realised. The need to get ahead of the threat should animate proactive action by Defence.

Implications and recommendations for Defence

GCR could fundamentally alter Australia's strategic environment. It would be accentuated by today's uncertain geostrategic landscape. These risks have implications for Australia's national security and can even emerge from the defence and security domain itself.

Defence, notably its intelligence agencies, already plays a critical role in detecting, analysing and understanding global risk. Informing the Government on emerging, uncertain and extreme risks is a key activity in Defence's remit. Importantly, Australia's intelligence agencies have potential to focus on long-term and uncertain events, even if those events are not the highest priority over day-to-day intelligence requirements. Defence must consider GCR within this existing remit. The likelihood, pathways and implications of GCRs require detailed investigation by the Department of Defence to properly inform government policymaking.

At a minimum, Defence should devote small but specific intelligence resourcing towards global catastrophic risk. For example, an extreme global threats warning team sitting within the Defence Intelligence Organisation (DIO) could work across the intelligence community to identify and track these risks. This team could assess or back-cast potential extreme pathways and worst-case scenarios, and advise the Government on their national security implications. This team or mission would present a central point of responsibility for policymakers. DIO could also lead a Five Eyes effort to share insights across Allied intelligence partners.

Defence could also better leverage and equip the Defence Science and Technology Group (DSTG) to analyse, monitor and model risk. DSTG has world-leading scientific and technical expertise. And its recently developed horizon scanning function analyses trends in emerging science and technology areas over a 10-20 year timeframe. GCR should receive dedicated attention in DSTG's work. DSTG could work more systematically with DIO to produce strategic assessments on potential global catastrophic risks associated with biotechnology or emerging disruptive technology.

References and further reading

Leigh, Andrew. *What's the Worst That Could Happen? Existential Risk and Extreme Politics.* MIT Press, 2021.

Ord, Toby. T*he precipice: existential risk and the future of humanity.* Hachette Books, *2*020.

Letwin, Oliver. *Apocalypse How? Technology and the Threat of Disaster.* Atlantic, 2020.

Walsh, Bryan. *End Times: A Brief Guide to the End of the World*. Hachette Books, 2019

McKibben, Bill. *Falter: Has the Human Game Begun to Play Itself Out?*. Black Inc, 2019.

Richard A. Clarke, R.P. Eddy. *Warnings: Finding Cassandras to Stop Catastrophes.* Ecco, 2017.

Rees, Martin. *On the future: Prospects for humanity,* Pitchstone Publishing, 2018.

Nuclear catastrophe and winter

Future strategic challenge: The global catastrophic risk of nuclear war has not been higher since the Cuban Missile Crisis. The likelihood of a global catastrophic nuclear event is 0.5 percent risk per year, according to a 2021 assessment by the president of the Nuclear Threat Initiative. Assuming no change to this 0.5 percent estimate given current strategic dynamics, there would be a 40 percent chance of a major nuclear event in the remaining years of the century. Meanwhile, a full-scale nuclear war between the US and Russia would kill an estimated 5 billion people worldwide within two years, according to a recent landmark report, 'Nuclear Famine'. A very 'limited' nuclear war, involving less than three percent of the world's nuclear weapons, would cause catastrophic climate disruption and worldwide famine, putting 2 billion people at risk.

Recommendation: Defence should model the impact of nuclear winter scenarios on Australia, with a particular focus on supply chains, food and the indirect security implications. Defence should also sponsor resource supply preparations for nuclear winter, including medical, fuel and basic food resource stockpiles.

The global catastrophic risk of nuclear war has not been higher since the Cuban Missile Crisis. Technological advances are expanding the range of dangerous pathways that could lead to nuclear war, while heightened geopolitical tensions and flailing arms control and crisis stability mechanisms raise the possibility of going down those pathways.

Russia's invasion of Ukraine, heightened nuclear tensions and the hair-trigger alert status of its strategic nuclear forces illuminate this danger. The risk of nuclear weapons use in the Indo-Pacific is growing, too. A confluence of factors are increasing the likelihood of accidental or intentional nuclear use: geopolitical tensions between China and the US and between India and Pakistan; weak nuclear command and control systems; emerging disruptive technologies; 'doctrinal dissonance'[1]; and non-existent nuclear 'hotlines' or communication channels in the region. There are at least sixty historical incidents that may have threatened to become a nuclear war, including as a result of technical glitches, false alarms, and intentional or inadvertent escalations.

The impact of a nuclear conflict would be globally catastrophic. Recent landmark scientific studies that simulate nuclear war scenarios between India and Pakistan show that even a so-called "limited" or "regional" nuclear war would be a planetary-scale event. For example, a war between India and Pakistan using less than 3 percent of the global nuclear arsenal could "crash the climate, the global food supply chains, and likely public order." Nuclear winter - that is, the long-term cooling and environmental effects caused by catastrophic sun-blocking soot - would

[1] Doctrinal dissonance refers to a mismatch in nuclear doctrines: ambiguities and competing ideas about nuclear deterrence among nuclear weapon states make it more likely that a limited, conventional conflict would escalate into a nuclear exchange.

produce crop failures that lead 2 billion people to die of starvation. In almost all countries, livestock and aquatic food production would be insufficient in substituting for reduced crop output. Despite recent advances in modelling nuclear winter scenarios, understanding in government is almost certainly lagging. In the 1980s, the United States Defence Nuclear Agency (now Defense Threat Reduction Agency) actively investigated nuclear winter. It concluded that a large-scale nuclear exchange could cause "atmospheric trauma" with "serious potential for severe consequences" for the weather and climate. This work sets a precedent for ongoing government efforts around the world, including in Australia.

Based on the very minimal recent study into nuclear winter, Australia, with its major agricultural products and southern location, appears to be one of the most resilient countries. However, there remains significant uncertainty in this assessment. The effects of ozone depletion and radiation on Australia and the region are unaccounted for. And world-wide starvation-induced unrest and mass migration could have severe effects on Australia's economic and security order.

Implications and recommendations for Defence

Defence should improve its understanding of nuclear weapons use scenarios, particularly nuclear winter scenarios. Important focus areas for a Defence assessment include resolving uncertainties in nuclear winter modelling research, canvassing a wider range of potential nuclear war scenarios, and predicting climate consequences of such scenarios and the flow-on effects for Australia's security environment. The modelling could build on existing work by academics and think tanks. This work is also useful for other sun-blocking catastrophes, such as super-volcanoes.

Defence could also lead preparations to improve Australia's resilience to nuclear winter. Defence could sponsor resource supply preparations for nuclear winter, including medical or fuel stockpiles. Producing even basic food resource stockpiles would help mitigate the agricultural decline and major supply chain disruption caused by nuclear winter, and could simultaneously be reserved for additional purposes. DSTG could conduct research into alternative foods that would be resilient to, or produce after, a nuclear catastrophe.

References and further reading

Nuclear Threat Initiative. "Remarks by Joan Rohlfind at Effective Altruism Global: London 2021." 30 October 2021.

Baum, Seth D.; De Neufville, Robert; and Barrett, Anthony M. "A Model For The Probability Of Nuclear War." Global Catastrophic Risk Institute Working Paper 18-1, 2018.

"Close Calls with Nuclear Weapons." *Union of Concerned Scientists*, April 2015.

Xia L, Robock A, Scherrer K, et al. "Global food insecurity and famine from reduced crop, marine fishery and livestock production due to climate disruption from nuclear war soot injection." *Nat Food* 3, (2022): 586 - 596. https://doi.org/10.1038/s43016-022-00573-0

Toon OB, Bardeen CG, Robock A, et al. "Rapidly expanding nuclear arsenals in Pakistan and India portend regional and global catastrophe." *Sci Adv.* 5, no. 10 (2019).

Reisner, J., D'Angelo, G., Koo, E., Even,W., Hecht, M., Hunke, E., et al., "Climate impact of a regional nuclear weapons exchange: An improved assessment based on detailed source calculations." *Journal of Geophysical Research,* 23 (2018): 2752–2772.

Bivens, Matt . "Nuclear Famine." International Physicians for the Prevention of Nuclear War, August 2022, 15.

Mills, M.J., Toon, O.B., Lee-Taylor, J., Robock, A. "Multi-decadal global cooling and unprecedented ozone loss following a regional nuclear conflict." *Earth's Future* 2 no. 4 (2014): 161-176.

Helfand, I. "Nuclear famine: Two billion people at risk." *International Physicians for the Prevention of Nuclear War,* 2013.

Artificial intelligence's impact on nuclear risk

Future strategic challenge: Ongoing rapid advances in artificial intelligence (AI) and its military application increase the catastrophic risk of nuclear use. Integrating AI into defence capabilities and nuclear weapons systems could greatly disrupt nuclear stability arrangements. For example, the use of AI-enabled intelligence, surveillance and reconnaissance (ISR) or weapon systems could enable the locating, tracking and targeting of an adversary's nuclear weapons and their facilities. This capability would erode the ability or perceived ability of a state to assure its retaliatory nuclear capability. Experts assess that AI, even with only modest rates of technical progress, has significant potential to exacerbate emerging challenges to nuclear stability by the year 2040. AI compounds the risks associated with rising geopolitical tensions and inadequate crisis stability mechanisms between hegemonic powers in the Indo-Pacific.

Recommendation: Defence should enhance its intelligence capabilities for assessing AI risks in the Indo-Pacific, including systematic monitoring of AI progress. It should also strengthen its analytical capabilities about AI's impact on nuclear stability in the region by increasing intelligence cooperation and policy engagement with Allied partners on the issue.

AI will have transformational and potentially highly disruptive impacts on security and defence issues. As the UK Department of Defence warns, AI will be a key area for geostrategic military competition, "not only as a means for technological commercial advantage but also as a battleground for competing ideologies."

AI systems are also vulnerable to both attack from adversaries (such as by 'poisoning' data) and to error as a result of automation bias and increased complexity. Defence is almost certainly grappling with challenges relating to AI's impact on Defence capabilities. However, one particularly concerning and neglected area of AI's impact on global security is its impact on nuclear risk. Specifically, recent and ongoing advances in AI could significantly impact strategic stability and increase the catastrophic risk of nuclear use by eroding the ability - or perceived ability - of a state to assure the survivability of its nuclear forces.

World-leading Defence research institutes such as the RAND Corporation and Stockholm International Peace Research Institute (SIPRI) have recently undertaken extensive research on the AI-nuclear risk nexus. According to the RAND study, the use of AI-enabled intelligence, surveillance and reconnaissance (ISR) or weapon systems could substantially enable the locating, tracking and targeting of an adversary's nuclear weapons and their facilities. AI-enabled ISR could therefore increase the vulnerability of a country's second-strike capability, compromising its deterrence capability. Moreover, if leaders believe they can disarm their opponents, they may be motivated to use nuclear weapons first in a crisis.

The *perception* of a state's AI capability and intention is also dangerous. For example, a state may perceive an adversary's investment in AI as rendering it more capable than it is. Perceiving a threat to its nuclear retaliatory capability, the state may therefore choose to adopt measures that decrease strategic stability or, in the worst case, use its nuclear weapons before it loses them. Both Russia and China appear to believe that the US is seeking to leverage AI to threaten the survivability of their strategic nuclear forces. This perception could have destabilising and potentially catastrophic consequences in a crisis situation.

AI-enhanced capabilities are also likely to further complicate the conditions that underpin nuclear stability through greater automation of nuclear command, control, and communications (NC3) systems. By 2040, experts consider it plausible that an AI system might be able to play aspects of military war games or exercises at superhuman levels, and thus be used to support nuclear decisions. The future incorporation of AI into decision support systems informing choices about the use of nuclear weapons would carry a host of new risks, particularly given AI's susceptibility to adversarial manipulation and subversion.

Although AI risk is still emerging, the technology is making rapid progress. It is already demonstrating superhuman performance at increasingly complex offensive and defensive tasks. RAND Corporation assesses that "AI has significant potential to exacerbate emerging challenges to nuclear strategic stability by the year 2040 even with only modest rates of technical progress."

The potential destabilising impact of AI advances on strategic stability are exacerbated by the prevailing geopolitical tensions in the Indo-Pacific. Ongoing great power competition means that China might, for example, assess that AI provides it with a usable military advantage over vulnerable US Allies and partners. The well-developed bilateral nuclear arrangements between Russia and the US will be complicated in a tripolar nuclear power system. Along with an absence of strategic communication channels between the two hegemons, these factors will increase the likelihood that regional conflict escalates into a nuclear conflict.

Implications and recommendations for Defence

Before these strategic challenges become acute, Australia needs to realistically understand AI's potential impact on global security, and especially nuclear stability. The development of global norms, rules or standards around AI integration into military capabilities is, for now, a dim prospect. There are numerous hurdles to the regulation of AI and other emerging disruptive technologies, including the difficulty in their verification and the reluctance of some states to give up a new capability whose military value is not fully known. Today, relevant technical expertise and understanding of the threat is in short supply, both within and outside of government. There also appears to be no active Defence planning, nor wider government planning, to mitigate the risk.

As an initial step, the Government should allocate the national intelligence community increased resources for assessing AI risks in the Indo-Pacific, including through threat-casting and systematic monitoring of AI progress. A recent report by the US Military Academy outlines several indicators of such progress that are worthy of monitoring, including "demonstration of human-out-of-the-loop decision-making for nuclear command and control systems," and "AI education

and career opportunities that reach a tipping point [which] push China into a position of global dominance within the field of AI."

Strengthening intelligence and policy engagement with Allied partners on the AI-nuclear risk nexus is also critical. At the 2021 Australia-US Ministerial Consultations, AI was discussed as an area that would benefit from developing a joint horizon scanning mechanism. This is a welcome development. Australia should look to deepen its own analytical capabilities about AI's impact on nuclear stability, including in the Indo-Pacific, through increased intelligence sharing with countries that have high-quality analytical assessment capabilities on these issues.

The UK could be another partner. The UK Ministry of Defence outlined in its recently published Artificial Intelligence Strategy that it will study "the effects of AI on the inter-linked domains of cyber, space and nuclear, examining AI's potential to accelerate or amplify developments linked to other emerging and strategic technologies."

References and further reading

Geist, Edward and Andrew J. Lohn. *How Might Artificial Intelligence Affect the Risk of Nuclear War?* Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/perspectives/PE296.html, 11.

Boulanin, Vincent; Saalman, Lora; Topychkanov, Petr; su, Fei; and Carlsson, Moa peldán. "Artificial Intelligence, Strategic stability and Nuclear Risk." *SIPRI,* June 2020.

Lieber, Keir A., Press, Daryl G. "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence." *International Security* 41, no. 4 (2017): 9–49.

Kroenig, Matthew. "Will Emerging Technology Cause Nuclear War?" *Strategic Studies Quarterly* 15, No. 4 (2021): 59-73.

Johnson, James. "'Catalytic nuclear war' in the age of artificial intelligence & autonomy: Emerging military technology and escalation risk between nuclear-armed states." *Journal of Strategic Studies*, (2021), DOI: 10.1080/01402390.2020.1867541.

Hitchens, Theresa. "The nuclear 3 body problem: STRATCOM 'furiously' rewriting deterrence theory in tripolar world." *Breaking Defence,* 11 August 2022.

Vanatta, Natalie; Johnson, Brian David; Brown, Jason C.; Lindsay, Greg; and Carrott, James. "Future Implications of Emerging Disruptive Technologies on Weapons of Mass Destruction." *ACI Technical Reports*, 49 (2022). https://digitalcommons.usmalibrary.org/aci_rp/49, 62.

Catastrophic climate change

Future strategic challenge: A catastrophic climate change scenario refers to an abrupt, non-linear, and irreversible environmental change triggered when planetary "tipping points" are crossed. Study of this tail risk remains very limited. But the few scientific studies with estimates conclude that the probability of catastrophic climate change is between 5-20 percent, depending on different emissions pathways. Catastrophic climate scenarios could cause significant disruptions to ecosystems, society and economies. It could potentially make large areas of Earth uninhabitable. The factors leading to these tipping points remain unclear. But catastrophic climate change is much more likely if warming is above 6°C this century. Even if significant headway is made towards achieving the UN Paris Agreement target of 1.5-2 degrees Celsius level of global warming, catastrophic climate scenarios cannot be ruled out.

Recommendation: Defence should pre-empt worst-case climate scenarios by increasing investment in climate intelligence capabilities, undertaking new war-gaming exercises, and enhancing intelligence cooperation with regional partners. Defence should also factor worst-case climate scenarios into contingency planning, including by considering how they would affect ADF capability and force structure.

The impact of climate change on Australian and regional security has been a theme of previous defence reviews. It is also currently receiving attention under the climate security assessment led by the Office of National Intelligence. This work and consideration is important because climate change will almost certainly cause disruptions to food, water and energy in our region. However, catastrophic climate change scenarios receive very little attention. The public and the media commonly label climate change as 'catastrophic' or 'existential'. But, truly catastrophic climate scenarios are poorly understood and overlooked in both academic literature and Australian policy making circles.

These scenarios refer to the abrupt, non-linear, and irreversible environmental changes triggered when planetary 'tipping points' are crossed. It is unclear what could trigger these tipping points. But catastrophic climate change is much more likely if warming is above 6°C this century. It could trigger feedback loops and cascade effects in our climate. Some tipping points - such as melting arctic permafrost leading to catastrophic amounts of emissions being released - are already looming. Others, such as cloud feedback loops, remain underexplored and highly uncertain dangers. Such scenarios warrant more serious consideration by the Government, including Defence.

Despite increasing global efforts to control emissions, catastrophic climate change remains a possibility worth preparing for. A recent scientific study found that five major planetary tipping points could be crossed even at the level of global warming already reached, while six others would become "likely" at 1.5°C global warming - the target identified by the UN Paris Agreement.

Three separate studies conclude that the probability of catastrophic climate change is between 5 and 20 per cent, depending on different emissions pathways. The 2015 book, *Climate Shock*, assessed an 11 percent chance of a greater than 6°C temperature under a realistic medium-high emissions pathway. A 2015 study notes that the possibility of a rise of 6°C out to 2100 at 20 percent if the world continued its focus on fossil fuels and significantly increased its greenhouse gas use. A 2017 study finds that exceeding 5°C of warming by the end of the century - defined as 'beyond catastrophic, including existential threats' - is a 5 percent probability without climate policies.

We are equally uncertain about what the world looks like with temperatures increasing at these levels. It is extremely difficult to assess humanity's resilience to climate disruption, dynamics of global ecological and social systems, and when and how feedback loops kick in. With global temperatures currently predicted to increase by 2.3 - 3.5°C by 2100, according to data from the UN's Intergovernmental Panel on Climate Change (IPCC), the world is on course to cross multiple disastrous tipping points. More alarmingly, scientists assess that tipping elements are interlinked; crossing one boundary may cause others to be crossed, creating a 'cascading collapse'. Higher temperature pathways could also trigger other systemic risks by causing famine and malnutrition, extreme weather, increased violence and conflict and vector-borne diseases.

Implications and recommendations for Defence

As President Biden's administration highlighted in the October 2022 National Security Strategy, "climate change is the greatest [of all of the shared problems we face] and potentially existential for all nations." Given the stakes, the Defence Strategic Review should pre-empt worst-case climate scenarios and factor them into contingency planning for the next decade. Currently, there appears to be limited information-gathering or assessment of these worst-case scenarios for Department of Defence activities, including the potential for climate change to contribute to systemic risk.

Defence should take measures that inform the Government of these worst-case scenarios and potential government responses. For example, it could increase its investment in climate intelligence capabilities. These efforts would help identify and develop a meaningful understanding of the plausible yet complex worst-case scenarios. Enhanced intelligence cooperation with regional partners in this area would also be advantageous. Defence could also undertake new simulation and war-gaming exercises to prepare for catastrophic climate impacts.

Defence is already assessing the climate resilience of its infrastructure. However, the Defence Strategic Review should direct a more comprehensive consideration of the implications of extreme climate scenarios on ADF capability preparedness, operational readiness and sustainment, including the possible need for new skills, equipment and supplies.

Defence must also consider how to shape ADF force structure, and build Defence's resilience, to meet the threat of natural disasters occurring at "unimagined scales, in unprecedented combinations and in unexpected locations," which was a dangerous potential highlighted in Australia's National Disaster Risk Reduction Framework. Physical and social impacts of extreme climate change would transcend political boundaries, increasing the risk that crises cascade

beyond any one region. This could require Defence to shift its high priority focus on Australia's immediate region to contribute to military stabilisation operations in regions further afield, stretching ADF human capability and logistical resources.

References and further reading

Kempa, Luke et al. "Climate Endgame: Exploring catastrophic climate change scenarios." *PNAS* 119, no. 34 (2022), 1.

Rockström, J., Steffen, W., Noone, K., Persson, A., Chapin, F. S., Lambin, E. F., et al. "A safe operating space for humanity." *Nature* 461, no 7263 (2009):, 472–475. https://doi.org/10.1038/ 461472a.

Popp, M; Schmidt, H; Marotzke, J. "Transition to a moist greenhouse with CO2 and solar forcing." *Nat, Commun* 7, (2016), 10627.

McKay, David I. Armstrong et. al. "Exceeding 1.5°C global warming could trigger multiple climate tipping points." *Science* (2022).

King, David; Schrag, Daniel; Dadi, Zhou; Ye, Qi; and Ghosh, Arunabha. "Climate Change Risk Assessment." *Centre for Science and Policy,* 2015.

Xua, Yangyang and Ramanathanb, Veerabhadran. "Well below 2 °C: Mitigation strategies for avoiding dangerous to catastrophic climate changes." *PNAS* 114, no. 39 (2017): 10315–10323.

Wagner, Gernot and Weitzman, Martin L. *Climate Shock: The Economic Consequences of a Hotter Planet Hardcover*. Princeton University Press, February 2015.

Beard, S.J; Holt, Lauren; Tzachor, Asaf; Kemp, Luke; Avin, Shahar; Torres, Phil; Belfield, Haydn. "Assessing climate change's contribution to global catastrophic risk." *Futures* 127 (March 2021).

Cox, Kate et al. "A Changing Climate: Exploring the Implications of climate change for UK Defence and Security." *RAND Corporation,* 2020

Steffen, W et al. "Planetary boundaries: Guiding human development on a changing planet." *Science* 347, no 6223, (2015). DOI: 10.1126/science.1259855.

Engineered pathogens

Future strategic challenge: Bioengineered pathogens are a huge risk over the coming decades. This emerging risk is driven by technological advances in synthetic biology and artificial intelligence, widespread availability of genetic data, and the explosion of high-containment laboratories for working with very high-risk pathogens.

Recommendation: Defence should clearly establish in Defence doctrine that pandemic preparedness is a matter of Australian national security. Defence should enhance its scientific, technology and intelligence capabilities to better identify emerging extreme biological threats. It should also allocate additional resources to Defence Science Technology Group's 'disease modelling' research program, including to enhance preparedness for engineered pandemics. Defence should also review its operational plans for different levels of pandemic risk, including both natural and engineered.

Catastrophic biological risks, such as engineered pathogens, are another major strategic challenge that requires more serious attention in Defence planning. COVID-19 highlighted the profound societal impact caused by the spread of a novel biological agent – even a naturally occurring one. But engineered pathogens could pose a more extreme threat to human health and economies by enabling a nefarious actor to strike a careful balance between lethality and infectivity across a particular population. Factors outlined below demonstrate the increasing plausibility of bioengineered agents being released within the century.

Firstly, the biosecurity threat paradigm is expanding primarily due to rapid improvements in dual-use technology – notably synthetic biology. These advances in molecular engineering, as well as the wide availability of genetic data, synthesis tools, techniques and methods, mean that researchers are now able to engineer biological agents with greater ease and precision. The continued advance and spread of biotechnology will likely further reduce the level of technical proficiency, cost and equipment thresholds required for an unsophisticated adversary to engineer pathogens that are deadlier, more contagious and more difficult to treat than natural ones.

The fact that such technology is not currently accessible or has not yet been misused is a poor predictor of its potential future misuse. For example, the society-wide impacts of COVID-19 could serve as a catalyst for "the most creative and dangerous groups and individuals to reconsider bio-terrorist attacks" against Australia or its allies, including through engineered pathogens. Additionally, the global shortcomings in preparedness for COVID-19 and questions surrounding its origins may further motivate actors with nefarious intent to misuse such technology. This issue might extend beyond a counter-terrorism lens. As technology is democratised, students, insiders or other malicious actors could produce and release a virus more consequential than COVID-19. Although this would typically be seen as a policing problem, the global reach and catastrophic impact of such an event should make it a Defence priority as well.

Increasingly advanced artificial intelligence will only exacerbate the risk: "AI could potentially lower some of the barriers for a malicious actor to design dangerous pathogens with custom features," according to a 2019 study seeking to understand the risks of AI intersecting with synthetic biology. AI could reduce design and testing time, help more easily find mutations of pathogens that could increase its virulence, transmission and lethality, and reduce the pathogen's ability to be screened or detected. As the study states, eventually, a bad actor could perform "complete hands-off, in silico [that is, computer simulated] design, building, and testing of a novel or recreated pathogen."

Implications and recommendations for Defence

In light of the potential consequences, the threat of bioengineered pathogens should be regularly assessed, anticipated and planned for at all levels of government, including Defence. Recent public-facing Defence documents such as the 2020 Defence Strategic Update and the 2016 Defence White Paper briefly allude to the threat. They state that non-state actors can "adapt new technologies and techniques requiring minimal preparation for their purposes." But this assessment falls short in conveying the scale of the bioterrorism threat, and completely neglects the potential existential risk posed by engineered pathogens.

Defence must clearly establish in Defence doctrine that pandemic (natural and engineered) preparedness and response are matters of Australian national security. The US National Security Strategy recognised the threat, stating that the US must "prepar[e] for catastrophic biological risks, including by improving early warning and disease surveillance, data sharing and forecasting; speeding development, domestic manufacturing, and delivery of medical countermeasures; advancing safe biotechnology development and manufacturing; and overcoming inequities in care quality and access." Indeed, on 18 October 2022, the US released its National Biodefense Strategy, which envisions a US that "creates a world free from catastrophic biological incidents."

Defence must also enhance its scientific, technological and intelligence capabilities to better identify and respond to emerging extreme biological threats. Enhanced understanding of the threat would require continually monitoring and reassessing bioengineering developments and their security implications, including their capacity to shift the geopolitical paradigm.

Defence could also lead a thorough assessment on the prospect of the deliberate misuse of novel pathogens with pandemic or epidemic potential, in coordination with other relevant government agencies. For example, the DIO and the DSTG should produce regular joint assessments on the threat posed by synthetic biology and engineered pathogens. DSTG's 'disease modelling' research program is worthy of additional resourcing, in order to strengthen and diversify understanding of ways to counter malicious use of biological agents. This could include investigation of potential medical countermeasures to engineered pandemic threats, as well as development of molecular identification techniques that would enable rapid identification of microbial pathogens in the event of an accidental or intentional release of a bioengineered pathogen.

Additionally, Defence should provide substantive input into whole-of-government efforts to reduce catastrophic biological risks associated with advancements in technologies and dual-use

research and development. This includes actively working with like-minded countries to establish, reinforce and strengthen international biosafety and biosecurity norms and practices. A priority remains updating regulations to reflect contemporary key principles for responsible stewardship of bioscience - specifically with respect to engineered pathogens - in light of the lowering of barriers to bioscience and likely democratisation of bioweapons.

As pandemics, both natural and engineered, become an ongoing and potentially increasing risk, Defence has a critical role to play. General pandemic monitoring, prevention and preparedness would assist even in tail risk scenarios. Defence should review its operations plans for different levels of pandemic risk.

References and further reading

Sandberg, A. & Bostrom, N. "Global Catastrophic Risks Survey: Technical Report #2008-1." *Future of Humanity Institute,* Oxford University, 2008, 1-5.

Wickiser, John K.; O'Donovan, Kevin; Washington, Michael; Hummel, Stephen; and Burpo, Fred J. "Engineered Pathogens and Unnatural Biological Weapons: The Future Threat of Synthetic Biology." West Point Research Papers. 628. 2020. https://digitalcommons.usmalibrary.org/usma_research_papers/628.

Lentzos, Filippa; Rybicki, Edward; Engelhard, Margret; Paterson, Pauline; Sandholtz, Wayne; Reeves, Guy. "Eroding norms over release of self-spreading viruses." *Science* 375, no. 6576 (2022): 31-33.

Cruickshank, Paul and Rassler, Don. "A View from the CT Foxhole: A Virtual Roundtable on COVID-19 and Counterterrorism with Audrey Kurth Cronin, Lieutenant General (Ret) Michael Nagata, Magnus Ranstorp, Ali Soufan, and Juan Zarate." *CTC Sentinel* 13, no. 6 (2020).

United States Office of the Director of National Intelligence. "Annual Threat Assessment of the US Intelligence Community." February 2022.

Carbonell, Pablo; Radivojevic, Tijana; and Martín, Héctor García. "Opportunities at the Intersection of Synthetic Biology, Machine Learning, and Automation." *ACS Synth. Biol* 8, no. 7 (2019): 1474–1477.

United States White House. National Biodefense Strategy and Implementation Plan for Countering Biological Threats, Enhancing Pandemic Preparedness, and Achieving Global Health Security. October 2022.

Space weather and Near-Earth Objects (NEOs)

Future strategic challenge: The frequency and scale of solar eruptions, known as Coronal Mass Ejections (CME), vary with the 11 year solar cycle. A major concern is the possibility of a severe-scale CME of a similar magnitude to the 'Carrington Event' - named after the space weather superstorm of 1859. A 2020 scientific study found a 28 percent chance of at least one severe storm per year and a 0.7 percent chance of a Carrington-class storm per year. Such an event could cause global power grid failure, collapse in GPS systems and wide scale communications outages. Near-Earth Objects, such as asteroids above 1m in diameter, impact Earth at about once per 100 years and could, in the worst case, be misidentified as a nuclear launch event. They frequently cause localised damage, but also occasionally cause global environmental damage.

Recommendation: Defence should prepare for the space weather threat, including by exercising how it would respond to a Part IIIAAA (Defence Force call out) request in response to a catastrophic space weather forecast and by taking preparedness and resilience measures of Defence assets and capabilities. Defence, through Space Command, should also improve its own understanding of the potential direct and indirect security implications of space weather, NEOs and other uses of outer space by countries and companies. Finally, it should strengthen international systems of communication and coordination to limit the risk of unilateral misidentification of NEOs.

Outer space presents another vector of tail risk with global and national security implications. Space weather, particularly solar storms, and near-earth objects, particularly asteroids, could cause significant harm to human life and critical infrastructure. These events could directly or indirectly cause harm, and so are threats to national security that might require a Defence response.

According to NASA, "Space weather includes any and all conditions and events on the sun, in the solar wind, in near-Earth space and in our upper atmosphere that can affect space-borne and ground-based technological systems". Depending on the nature and magnitude of the event, space weather can interfere with electrical and communications infrastructures.

The frequency and scale of CMEs varies with the 11-year solar cycle. At a minimum, they are observed once per week, though almost all are too moderate to cause catastrophic damage. More concerning are 'great' super storms, such as that which affected parts of Scandinavia in 1921, or another which missed Earth by a week in 2012. Most concerning is the possibility of a Carrington-class CME, named after the space weather superstorm of 1859, which today would probably result in severe disruption. According to a 2020 scientific study, there is on average a 28 percent chance of at least one severe storm per year and a 0.7% chance of a Carrington class storm per year.

On very rare occasions, Earth is struck by an object capable of causing global environmental damage. These Near-Earth Objects, particularly asteroids, more frequently cause localised damage. For example, the Tunguska event, which occurred in 1908 in Eastern Siberia, involved a 50-60 metre asteroid striking the atmosphere. The resulting blast is thought to have been on par with the largest hydrogen bombs ever tested. It created a shock wave that flattened trees over hundreds of kilometres. If a similar-sized object struck a major city today, it would likely kill millions. A further example is when, in 2013, a 20 metre asteroid exploded above Chelyabinsk, Russia, causing around 1,500 injuries and damage to thousands of buildings. It reportedly carried 20 to 30 times the energy of the Hiroshima atomic bomb.

NASA's Planetary Defence Coordination Office (PDCO) provides early detection of some of the most hazardous NEOs, which are those greater than 30-50 metres. NASA estimates it has mapped over 99 percent of those objects in our solar system that would be extinction level events. However, NEOs the size of the Chelyabinsk object and somewhat larger are not mapped. That the world could be surprised by an object that causes a blast the size of several nuclear weapons is plausible.

Of potential greater concern is the indirect consequences of small asteroid impacts. There have been several instances in the decades since the development of nuclear weapons where launch decision procedures were initiated due to non-military events being misinterpreted as weapons launches. These include a moonrise, unusual reflection off clouds and the launch of a scientific weather rocket. Asteroids above 1m in diameter, which impact Earth at about once per year, could be misidentified as a nuclear launch event.

In 2014, the Comprehensive Nuclear Test Ban Treaty Organisation stated that its network of sensors had recorded 26 atom-bomb-scale asteroid impacts to Earth's atmosphere since 2000 Similarly, solar storms could also have devastating indirect impacts caused through false alarm, as exemplified by the 1967 CME-triggered geomagnetic storm, which almost triggered nuclear warfare between the US and USSR. Total disruption to polar surveillance radars during the Cold War led the US nuclear bomber squadrons to mobilise for a strike on the USSR, until it was identified that the Sun was the source of the radio interference.

Implications and recommendations for Defence

Defence must have the capability to monitor and prepare for the space weather threat. Currently, the monitoring function is largely fulfilled by the Bureau of Meteorology's Australian Space Weather Alert System, which produces warnings and real-time observations of severe space weather, with accompanying basic safety measures. The National Space Agency is responsible for coordinating the Government's civil space work, including facilitating international space engagement. The newly established Defence Space Command within Australia's Air force seeks to ensure space access and power in an increasingly "contested space," and to protect commercial and military assets against space debris, collisions and destructive acts.

The strategies adopted by the US and UK to respond to the threat of space weather and NEOs, alongside relevant academic research, provide examples of clear policy paths Defence could take towards managing the risk.

Defence, through Space Command, should improve its own understanding of the potential direct and indirect security impacts of extreme space weather, Near-Earth objects and other implications of use of outer space by countries and companies. For example, one recent study highlighted ten pathways for how space exploration and activity could increase global risk, including the nefarious use of asteroid deflection capability and potentially harmful extraterrestrial organisms transferred into Earth's biosphere.

War-gaming how other nations might respond in the aftermath of an extreme space weather or NEO event would also be constructive. Considerations include how countries might take advantage if a neighbour competitor was crippled for an extended period, how Defence capabilities would operate in such an environment, and how critical supply chain issues might impact security. For example, an extreme space weather event would likely damage grid-scale transformers made in China, and in optimal situations could take many months to be manufactured, shipped and delivered.

Defence should also play an active role in preparing mitigating actions for the event when the Bureau of Meteorology launches an extreme space weather observation or forecast, including a solar storm warning. This requires exercising how it would respond to a part IIIAAA Call Out order in response to an extreme space weather forecast. Defence should also take preparedness and resilience measures of Defence assets and capabilities. For example, it should enhance the protection of its communication systems in the event of Space Weather, and establish Plans and Procedures for identifying, responding to and recovering from Space Weather Events.

Defence could also strengthen international systems of communication and coordination to leverage the capabilities of partners and limit the risk of unilateral misidentification of near-Earth objects.

References and further reading

Chapman, S. C., Horne, R. B., & Watkins, N. W. " Using the aa index over the last 14 solar cycles to characterise extreme geomagnetic activity." *Geophysical Research Letters* 47 (2020), e2019GL086524. https://doi.org/10.1029/2019GL086524.

Oughton, Edward J. "The Economic Impact of Critical National Infrastructure Failure Due to Space Weather." *Oxford Research Encyclopedias.* 20 November 2018. https://doi.org/10.1093/acrefore/9780199389407.013.315.

Baum, Seth D. "Uncertain human consequences in asteroid risk analysis and the global catastrophe threshold." *Natural Hazards* 94, no. 2 (2018): 759-775.

UK Department for Business, Energy and Industrial Strategy. "UK Severe Space Weather Preparedness Strategy." 2021.

United States National Science and Technology Council. "National Space Weather Strategy and Action Plan." 2019.

Hamilton, Chase. "Space and Existential Risk: The Need for Global Coordination and Caution in Space Development." *21 Duke Law & Technology Review* 1-60, (2022).