



A Short History: 2019-2026

Overview

Founded in 2019 as a UNSW Canberra spin-off, the Social Cyber Institute was initially part of the Social Cyber Group. It was built on the idea that cyber security is a social science. In 2024, the Institute was incorporated as its own limited company, with the Social Cyber Group being discontinued. The Institute became an independent, volunteer-run not-for-profit. Its mission has embraced AI as a principal research theme. In 2026, it sought to consolidate its governance and begin the move to fully-funded operations by the end of 2027. The Institute has more policy influence and reach than its size suggests.

Origins: a commercial question, 2018–2019

The Institute began with a commercial question rather than an academic one. In 2018 UNSW's Enterprise Division, led by Dr Elizabeth Eastland, convened a briefing for venture capitalists at UNSW Sydney to show investors what university research had produced. Eastland asked Professor Greg Austin, then at UNSW Canberra, to organise the one-day event. Standing alongside the engineer inventors he asked a different question: how do you commercialise social science research on cyber security? Austin and a colleague, Professor Glenn Withers, answered with a single proposition: “cyber security is now a social science”. The Social Cyber Group and its affiliated Institute were founded out of that presentation, a spin-off from UNSW Canberra.

Three people were involved. Austin brought a decade of cyber and China policy work overseas and the design of Australia's first master's degree in cyber security, strategy and diplomacy in 2015. Professor Glenn Withers AO brought institutional weight from another direction: eminent Australian economist, former Chair of the Australian Council of Learned Academies, immediate past President of the Academy of the Social Sciences in Australia, and Chair of the Global Development Learning Network set up by the World Bank. Lisa Materano brought delivery capability as chief executive of Blended Learning International, a registered training organisation and itself an ANU spin-off with some 20 years standing. The three leaders (security think tanker, economist academician, and a vocational education operator) provided a combination of talents that explains much of what the Social Cyber Institute became: research-led, but never purely academic and always socially motivated.

The intellectual foundation followed in 2019, when Austin and Withers published *Creating Social Cyber Value*, setting out the claim the Institute has argued ever since: that the determinants of security in cyberspace are social and organisational at least as much as technical, and that the social sciences therefore have a first-order role rather than a supporting one.

The slow build, 2019–2022

For several years, the influence of the founders travelled through their other affiliations in parallel with their continuing commitment to the “social cyber” idea. Key focal points of the founders' work in these years included cyber emergencies and resilience, cyber security education, national security aspects of cyber capability and cyber power. Adam P. Henry joined the team as a Senior Adviser, with them all providing original policy research sometimes badged as “Social Cyber Institute” and sometimes as their other institutional associations. Notable products led by members of the Social Cyber team in these

years involving leadership roles or their authorship, most often under other institutional banners, included:

- ‘Social Science Research and Intelligence in Australia’, Australian Academy of the Social Sciences, 2019, 31 pp, co-authored paper
- National Cyber Emergencies: The Return of Civil Defence* (Abingdon Oxon: Routledge, 2020) 246pp, edited volume
- Cyber Security Education: Principles and Policies* (Abingdon Oxon: Routledge, 2020) 226pp, edited volume
- “Comprehensive resilience in contagion, economic shock and other disasters”, Submission to Senate Select Committee on Responses to Covid-19, Social Cyber Institute, 2021
- Cyber Capabilities and National Power: A Net Assessment* (London: IISS, 2021) 200pp, co-edited volume, and contributing author
- ‘Measuring Reputation Loss from Cyber Attack’, co-authored consultancy report for the NSW Government, 2021
- ‘Assessing Cyber Military Maturity: Strategy, Institutions and Capability’, IISS, 2022, co-authored, 49pp
- ‘Military Ambitions and Competition in Space: The Role of Alliances’, IISS, 2022, co-authored, 37 pp
- ‘Opportunity, Threat and Dependency in the Social Infosphere’, in Paul Cornish ed. *Oxford Handbook on Cyber Security* (Oxford: Oxford Univer
- Great Power Offensive Cyber Operations: Experiments in Cyber Power*, (London: IISS, 2022) 100pp, co- authored volume

That pattern of leverage through people rather than payroll was not a transitional phase. The Institute has always been larger than its “minimalist” payroll: its capacity is measured not by who it employs, but by who will work with it and the influence of its research-based ideas. This is still how the Institute operates.

Consolidation, 2023

2023 was the year the Institute began to establish a stronger institutional identity. In April it made two submissions to the panel reviewing Australia's cyber security strategy: one proposing a standing framework for evaluating national cyber policy, and one setting out a Six Point Institutional Plan for Revitalising Australian Cyber Policy. The preference visible in that pairing, evaluation architecture over advocacy, has been a signature predisposition since.

The same year produced Research Paper 1/23, Austin and Withers on Valuation of Reputation Damage for Transport Cyber Attack; Austin's co-leadership of the second volume of the IISS Cyber Capabilities and National Power study, covering a further ten countries; and sessions at the Australian Cyber Security Conference in Canberra and Melbourne, where the founders presented Cyber Organisational Insight, drawn directly from the 2019 paper. Internationally, the Group signed a memorandum of understanding with the Kyiv-based Cyber Diia platform, whose executive director Professor Andrii Paziuk was an adviser Ukraine's Minister of Digital Transformation.

Independence and the Fellows, 2024

Two structural changes in 2024 mattered more than any publication. The Institute was established as an independent not-for-profit company, formally separate from the Social Cyber Group, which remained for-profit and which housed the Social Cyber and Tech Academy. The Academy business has been transferred to Blended Learning International.

The Institute at that time became a registered company limited by guarantee with its registered office in Melbourne and a satellite office in Canberra Australia. It operates as a non-profit organisation. It is common in Australia for non-profit organisations to register as a company limited by guarantee.

The Social Cyber Group continued to provide logistic, promotional and infrastructure support on a pro bono basis to the Institute. Office holders in the two companies on registration were identical, but it was expected that in due course the leadership of the Institute would be expanded and or modified independently of any leadership changes in the Social Cyber Group.

On 1 March 2024, the Institute launched a Fellows programme and an open call for papers. By 23 April 2024, seven researchers had committed to the inaugural cohort of Fellows and it grew quickly to fourteen. The Institute was, and remains, staffed by volunteers.

Output rose sharply and diversified beyond its founders especially through its Fellows, who also carried the branding of their university or home organisation simultaneously with that of the Social Cyber Institute. Dr Brendan Walker-Munro's October submission to the Parliamentary Joint Committee on Intelligence and Security was cited several times in the committee's advisory report. Professor Dan Svantesson analysed the Musk–Australia takedown standoff in *The Conversation*. Professor Katina Michael gave the interview on the Ticketmaster breach that ran globally. Austin published on ASIO's threat assessment, on China's military buildup and on the incoming ASD Director-General. He released a discussion paper on Australia's Cyber Surge analysing the largest expansion of Australian cyber capability since 1947. He was an invited panellist at NATO's CyCon in Tallinn.

The year closed with the 29 November launch of the Australia–India Joint Technology Assessment for Peace and Stability, hosted formally by ANU and InKlude Labs, funded by DFAT, but with all six Australian participants associated with the Social Cyber Institute. Technology impact assessment now had a funded international vehicle.

Widening the aperture, 2025–2026

In 2025 Professor Katina Michael joined the Institute's board. She was founding editor-in-chief of *IEEE Transactions on Technology and Society*, and six years director of Arizona State University's Society Policy Engineering Collective. At the UK Academy of Information Systems annual conference in Newcastle, Michael, Withers and Austin convened a track on privacy, trust and responsibility on Michael's initiative.

In 2026, the centre of gravity shifted decisively toward artificial intelligence. Major research now runs across four fronts: AI Consequences for Australia, Cyber War and Peace, Online Hate Speech and Violent Extremism, and the Australia–India technology impact assessment work. A three-way partnership with centres in the United Kingdom and United States examines AI's effects on cyber security employment in Australia. In 2026, the Institute launched its project on AI Consequences for Australia.

Webinars as a key outreach

The Institute has built its webinar and workshop series as a core outreach tool, connecting academic research with practitioners in business and government. The webinars bring together a wide range of voices, from cybersecurity practitioners at major financial institutions to legal scholars researching information warfare. Sessions have covered topics such as the impact of network attacks on stock markets. Other webinars have examined cyber resilience lessons drawn from the Russia/Ukraine war, with contributions from legal scholars in Kyiv and AI-focused researchers based in Sydney. The program has also tackled questions of information warfare readiness within Australia, considering options like civic engagement and structured response. This tool figured prominently in the government-funded research project on Australia India technology impact assessment. Each session is typically recorded and made available afterward, allowing wider access beyond the live audience thanks to the Education Director, Lisa Materano.

The Institute and the Social Cyber Group, though now legally distinct, retain important relationships, especially through the executive workshop program launched by the Social Cyber and Tech Academy. The overlap between the leaders of two bodies has ensured mutual synergies between their activities.

Media footprint

The Institute's media footprint by 2026 reflects the Institute's think-tank orientation, prioritising policy influence and expert commentary over broad public-facing news coverage. Overall, SCI's profile has grown steadily through its directors' individual reputations and its niche but consistent presence in defence, technology, and cyber-policy dialogues internationally. A notable highlight was Austin's involvement in an extended special report in 2025 by Bloomberg News on China's hacking ecosystem.

Our 2027 Ambition

Eight years on, the Institute is small, volunteer-staffed and more influential than its size suggests. Its method has been consistent since 2019: treat security in cyberspace as a social science problem, build evaluation frameworks rather than policy campaigns, and extend reach through fellows, partnerships and the standing of its people rather than through headcount. Our main goal now is to move to fully-funded operations by the end of 2027 and to consolidate our influence.