



# 2026 Prospectus

*Strategic perspectives for leaders*

*Research-based learning*

*Career change to cyber policy*

# Partnering for Professionalism



## Social Cyber & Tech Academy

The Social Cyber & Tech Academy specialises in advanced professional education on cyber power, organisational resilience and technology governance, drawing on decades of international research and practice. Its leaders are active in policy debates and education delivery in Australia, Asia and Europe. It is a spin-off from the University of New South Wales Canberra.

## Blended Learning International (BLI)

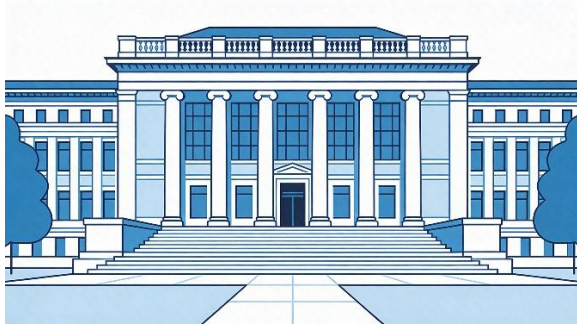
Blended Learning International brings two decades of experience in designing, governing, and assuring high-quality professional education to its collaboration with the Social Cyber and Tech Academy. Since 2003, BLI has worked across Australia and the Indo-Pacific to support the development and delivery of complex, policy-intensive learning programs, drawing on strong foundations established through its origins at the Australian National University. In this collaboration, BLI provides learning design leadership, governance frameworks, and quality assurance processes that underpin the Academy's programs and ensure they meet rigorous professional and educational standards.



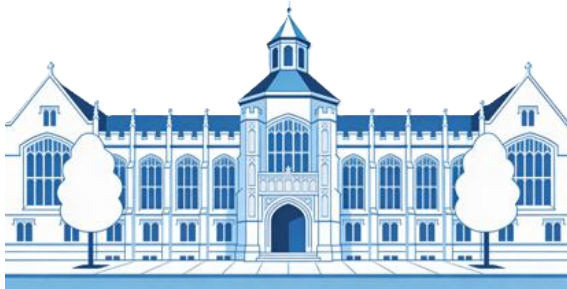
## Our unique offering

For Executives: Challenge workshops and briefings  
For Early and Mid-Career: Interactive lecture-based courses  
For Career Changers: Fascinating Insights into the world of cyber and tech policy

Harvard University



King's College London



## Where we have lectured or mentored

Harvard University  
The Australian National University  
Monash University  
Kings College London  
Australian Defence College  
Defence Intelligence Organisation  
Diplomatic Academy of Vietnam  
Cambridge University  
ANZ School of Government  
University of New South Wales  
Canberra  
QANTAS  
Commonwealth Bank  
Global Development Learning  
Network (World Bank)

## Where did we lead in cyber and tech education policy in 2025?

- Worked in a team of eight Australian and Indian researchers to develop a syllabus on technology impact assessment under a grant from the Australia India Cyber and Critical Technologies Program
- sponsored a delegation to Australia to establish an AUKUS network of cyber educators based on existing US/UK efforts
- Co-facilitated a panel on social responsibility aspects of artificial intelligence in higher education, to curate 11 papers at the annual conference of the UK Academy of Information Sciences
- Led a table-top exercise on cyber crisis for Malaysian officials in Kuala Lumpur

Australian National University



Australian Defence College



# 2026 Programs



**Crisis in Tech Diplomacy**



**Cyber Organisation Stress Test**



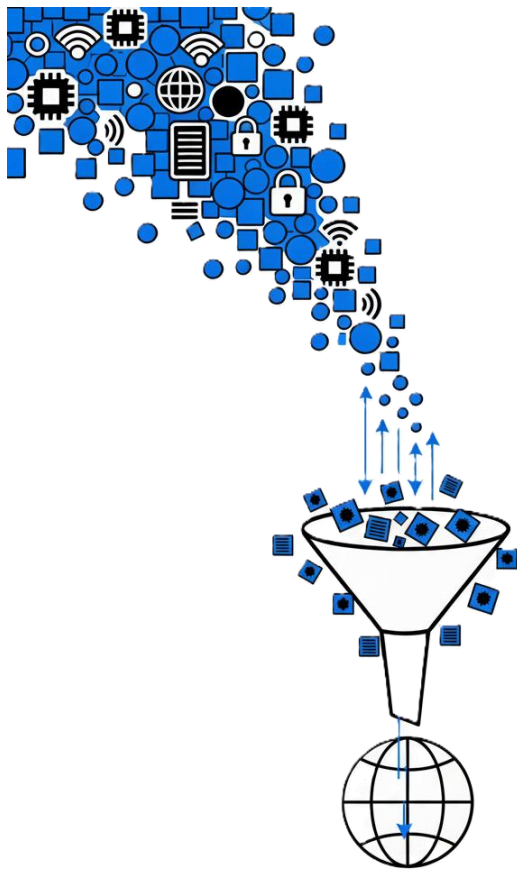
**Cyber and Tech Policy in China**



**Economics Principles for Cyber and Tech**



**Public Policy Principles for Cyber and Tech**



# CRISIS IN TECH DIPLOMACY

No country has the capacity to assess the impact on society, politics or the economy of all the individual technologies flooding global markets or the many creative apps based on them. This challenge workshop introduces key concepts, current dilemmas, and practical insights for managing this escalating crisis in technology policy. It is built around the concept and practices of Technology Impact Assessment (TIA). TIA is the systematic analysis of the impacts arising from the use of technologies. This includes both specialist assessment of their technical performance characteristics and cost-benefit considerations as well as consultations across diverse stakeholder groups (such as government, industry, academia, and society) to determine broader social, political, legal or economic consequences.

## Learning focus

- Understand the emerging “crisis in technology diplomacy”
- Examine real-world obstacles to whole-of-government tech impact assessment
- Identify new roles for diplomats, regulators and corporate leaders in tech governance

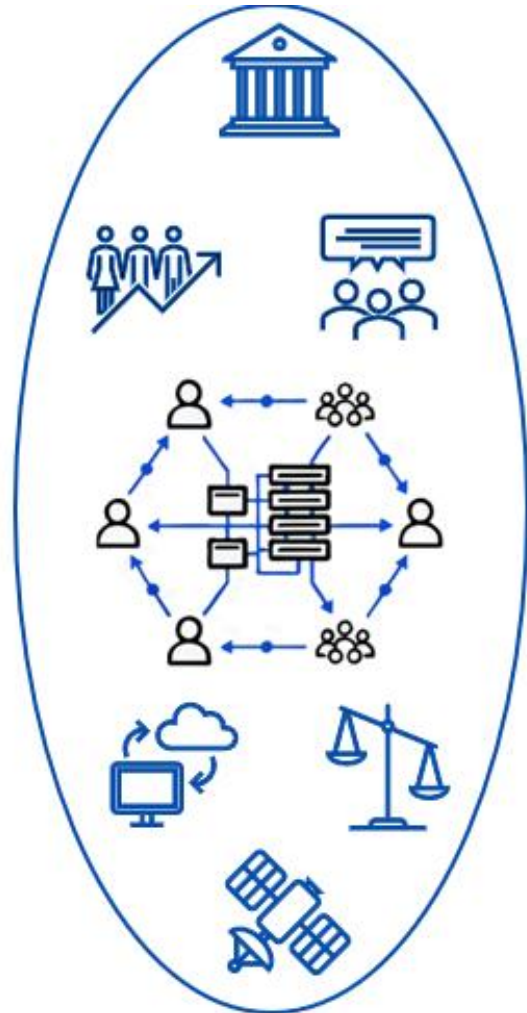
**Format:** 2 days × 3.5 hours (7 hours total), Thursdays 3:00–6:30 pm AEDT

**Dates:** 9 & 16 July 2026; 10 & 17 September 2026; 12 & 19 November 2026

**Facilitator:** Professor Greg Austin

# CYBER ORGANISATION STRESS TEST

This workshop helps senior executives prepare for strategic cyber challenges, lead cyber security change, and review the impact of their initiatives. Building on the paper *Creating Social Cyber Value*, participants diagnose their organisation's "cyber social system" (inside and outside the firm): culture, incentives, knowledge flows and external relationships. Inspired by Kevin Mandia's call to "know your organisation", the program goes beyond technical controls to show how to mine collective organisational knowledge—systems topology, people, processes, suppliers and infrastructure—for strategic advantage in cyber defence and resilience.



## Learning focus

- Build deep cyber organisational insight as a leadership capability
- Strengthen internal governance and cross-functional collaboration on cyber
- Evaluate current cyber change programs against social cyber value principles

**Format:** 2 days × 3.5 hours (7 hours total), Thursdays (3:00–6:30 pm AEDT)

**Dates:** 6 & 13 August 2026; 8 & 15 October 2026; 3 & 10 December 2026

**Facilitator:** Professor Greg Austin

# CYBER AND TECH POLICY IN CHINA



This one-day intensive offers a critical, research-based tour of China's evolving cyber and technology policy, grounded in over 15 years of scholarship by Greg Austin, including two and other studies. Participants examine Beijing's informatisation strategy through rarely used primary sources—internal planning documents, national “information society” blueprints, technical ministry reports and elite speeches—rather than recycled secondary commentary. The course introduces a nine-value framework for evaluating China's digital governance ethics and invites participants to apply it to censorship, surveillance, and data governance. It also highlights under-examined gaps between central visions and local implementation, and offers fresh, evidence-based perspectives on China's cyber power and US–China cyber stability debates.

## Learning focus

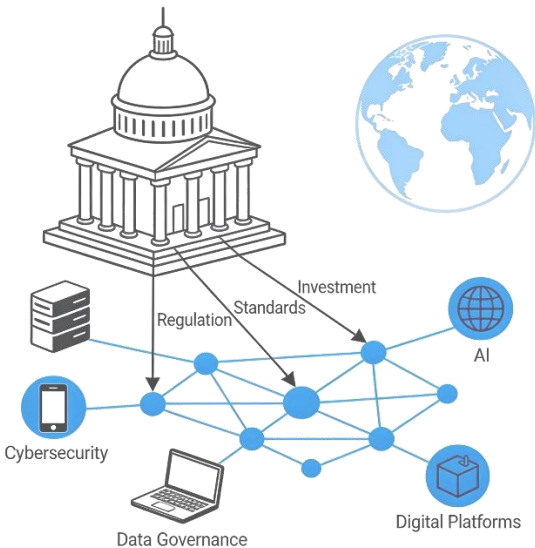
- Understand China's cyber and tech policy architecture and underlying values
- Analyse central–local implementation gaps and their strategic implications
- Reassess “cyber superpower” narratives with institutional and capacity evidence

**Format:** 1 day × 7.5 hours

**Dates:** 30 July 2026; 27 August 2026; 1 October 2026; 26 November 2026; 15 December

**Facilitator:** Professor Greg Austin

# PUBLIC POLICY PRINCIPLES FOR CYBER AND TECH



An executive-level overview of how governments design and implement policy responses to cyber and technology challenges. Participants examine why public intervention is needed in cybersecurity, digital platforms, AI, and data governance, and how policy tools — regulation, standards, investment, taxation and international cooperation — are deployed in practice. Using analytic frameworks and real-world cases, the course builds practical insight into governance models, policy trade-offs and implementation challenges in fast-moving tech environments.

## Learning focus

- Understand public policy processes for cyber and tech, both principles and practice
- Review the government instruments used for technology and cyber security
- Evaluate major policy initiatives in the cyber and tech field.

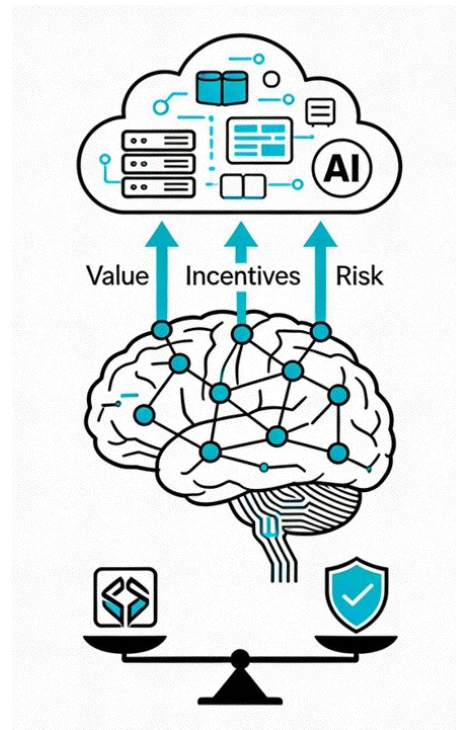
**Dates:** 15 & 29 September 2026  
20 & 27 October 2026

**Format:** 2 days × 3.5 hours (7 hours total), **Tuesdays 3:00–6:30 pm AEDT**

**Facilitator:** Professor Glenn Withers AO

# ECONOMICS PRINCIPLES FOR CYBER AND TECH

This course introduces the core economic forces shaping cyberspace and emerging technologies. Participants explore how digital markets create and distribute value, why market power and concentration arise in platform economies, and how incentives, externalities and information asymmetries affect cybersecurity, AI and other innovations. The program equips leaders with an economic lens for understanding cyber risk, technology-driven productivity change, and the logic behind regulatory and strategic interventions in digital sectors. It provides understanding of markets and engineering, information and bio-technologies.



## Learning Focus

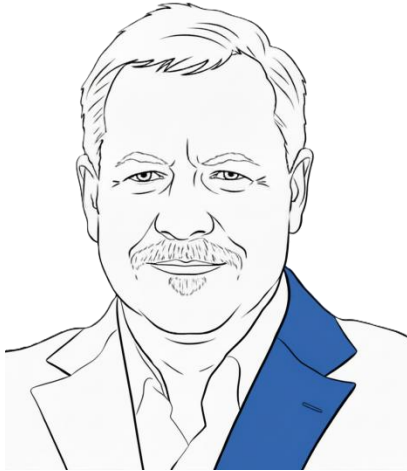
- Understand the nature of markets and their operation for cyber and tech
- Evaluate the operation of those markets for commercial value and for social value
- Learn techniques to manage and benefit from, and improve, market operation.

**Dates:** 14 & 21 July 2026  
11 & 18 August 2026

**Format:** 2 days × 3.5 hours (7 hours total), **Tuesdays 3:00–6:30 pm AEDT**

**Facilitator:** Professor Glenn Withers AO

## Our Educators and Mentors\*



**Professor Greg Austin** is a global leader in cyber policy and international security. He has held posts as Senior Fellow and Head of the Program on Cyber Power and Future Conflict at the International Institute for Strategic Studies (IISS), Professor of Cyber Security, Strategy and Diplomacy at UNSW Canberra, Visiting Senior Fellow in the Department of War Studies at Kings College London, and Adjunct Professor at the Australia-China Relations Institute at the University of Technology Sydney. With thirteen books and leadership of major international research projects, his career spans academia, government, and global NGOs such as the International Crisis Group and EastWest Institute. He has

advised ministers and agencies across the UK, Australia, China, India, Russia, and the United States, as well as the UN, IAEA, and major corporations including AT&T and BT. Holding a PhD in International Relations and a Master of International Law, both from the Australian National University, Professor Austin's work bridges cutting-edge research, strategic policy, and diplomacy.



**Lisa Materano** is the Director of the Social Cyber and Tech Academy, Director for Education at the Social Cyber Institute, and Co-Founder of the Social Cyber Group. She leads the design, management, and delivery of executive and professional education programs in cyber security, public policy, and technology governance across Australia and the Indo-Pacific. An economist by training, she has held senior executive, research, and academic leadership roles, with a career focused on developing high-quality education programs in regulated and policy-intensive environments. Her work sits at the intersection of strategy, governance, and practice, with a strong emphasis on

contemporary, research-informed learning design. She has led large-scale initiatives for government and institutional partners, including a AUD 26 million Australian Government project to establish a Technical College. She serves on the Asia-Pacific Governing Committee of the World Bank-affiliated Global Development Learning Network. Her qualifications include degrees in Economics (Bachelor and Master), a Diploma of Education, and training and assessment credentials.



**Professor Glenn Withers AO** is Emeritus Professor at the Crawford School of Public Policy, Australian National University, and Visiting Professor at UNSW Canberra. A Harvard PhD, he has held academic posts at Harvard, Cambridge, and ANU, and advised governments and corporations globally—from the OECD and US Defense Department to the Prime Minister of Malaysia. In Australia, he has led major national bodies including the National Population Council and Economic Planning Advisory Commission, and was instrumental in establishing the Productivity Commission, Universities Australia, and the Crawford

School of Government. Recognised for developing Australia’s Immigration Points System, he has also served as President of the Academy of the Social Sciences and Chair of the World Bank–affiliated Global Development Learning Network. His extensive publications focus on education, skills, workforce, and population policy.



**Adam P. Henry** is a Senior Fellow Partner at the Social Cyber Institute and a leading specialist in cyber security education, skills, and workforce development. He has designed and led major pilot programs to build Australia’s multidisciplinary cyber capabilities and has briefed ministers and senior officials on national cyber strategies. A former participant in the 2017 Prime Minister’s Cyber Taskforce, he has had a broad cyberspace professional career spanning the APS, a major consulting firm, academia, working in multiple start ups, his own consulting business and industry accelerators and clusters. This provides a unique skill set and understanding of the differing requirements of the Australian economy. He provides expert advice, strategic

briefings, and program design support across cyber policy, workforce development, defence, and national security domains.

*This team works with a network of experts from universities, government, and industry who join as presenters in all of our workshops and courses. A rich portfolio of talent is provided for mutually rewarding experience among presenters and participants.*

# Fee

The fee for each 7-hour workshop or course is set at A\$990 (incl. GST). The fee applies to all July courses and may be increased for courses in later months. Ten complimentary scholarship places are available for people from developing countries to all July courses. Bespoke options are also available for companies and other organisations.

# Registration

Workshops and courses are delivered online via interactive virtual classrooms. Certificates of completion are issued in partnership with **Blended Learning International**.

These programs are delivered as non-accredited professional education. None of the programs listed in this brochure are accredited under the Australian Qualifications Framework. They are however of high relevance to people working in cyber and tech policy.

Early registration is recommended as each cohort is capped at 30 participants to preserve a high-engagement learning environment.

For enrolment or information, contact: [lisa.materano@socialcyber.co](mailto:lisa.materano@socialcyber.co)

# Time Zones

Each program is timed to be as accessible as possible across Asia, the Middle East, Africa and Europe. All courses run from 3pm to 6.30 pm Sydney time.

## Times until daylight saving changes

- Tokyo: 2.00pm–5.30pm
- Singapore: 1:00pm–4:30pm
- Hanoi/Jakarta: 12 noon–3:30pm
- Dhaka: 11.00am–2:30pm
- Delhi: 10:30am–2:00pm
- Dubai: 9:00am–11:30am
- Istanbul/Nairobi: 8:00am–11:30am
- Kyiv/Helsinki: 8:00am–11:30am
- Paris/Warsaw: 7:00am–10:30am

## Times after daylight saving changes

- 1:00pm–4:30pm (after 4 October)
- 12.00 noon–3:30pm (after 4 October)
- 11.00am–2:30pm (after 4 October)
- 10.00am–1:30pm (after 4 October)
- 9.30am–1:00pm (after 4 October)
- 8.00am–11:30am (after 4 October)
- 7.00am–10:30am (after 4 October)
- 6.00am–9:30am (after 25 October)
- 6.00am–9:30am (after 25 October)