



CRANE

strengthening the Cyber Security research community

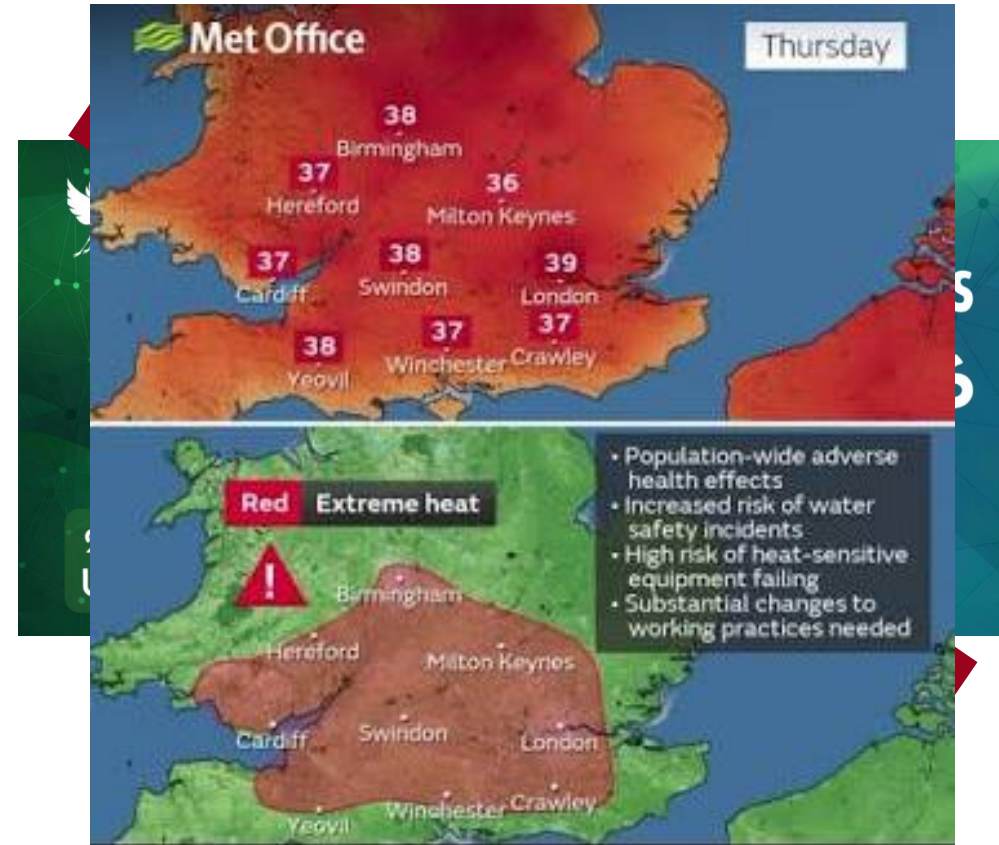
update, June 2026

This event will be
recorded, and made
available online.





Launch Webinar July 2025



Review of the year

Current Activity

Plans for the future (+Learned Society)

Call for proposals

Technology Trends and Horizon-Scanning

ecosystem

research activity

strengthening the cyber security research community

leading-edge

sustainability

strengthening the cyber security research community

researchers and careers
across the disciplines
outward-looking
regional priorities
international benefit

horizon-scanning
technology trends
emerging need and opportunities



engagement with business
and government
policies and priorities



pilot project funding

strengthening the cyber security research community



special-interest groups and working groups
nurturing existing expertise



supporting existing collaborations
building new ones
regional activity, clusters

learned society





CRANE Annual Report

YEAR ONE: ending March 2026

KPIs and other numbers

Table 1: Membership

Mailing list launched in May 2025. Membership database launched in Jan 2026.

	Mar-26
Total Mailing List Size	639
Total Membership	258
UK Academic	224
Business/Prof Network	14
Public Sector	2
O/S Academics	16
Other	2

Table 2: Engagements

Events	Attendee Number
CRANE Events	
Launch Webinar	
AI and Machine Learning Workshop	
Robotics and Automation Workshop	
Industry Roundtable, Glasgow	167
SIG/WG Meetings	18
Research Practices SIG Session 1	17
Inclusive Careers SIG Session 1	18
Economics Cyber SIG Session 2	
Safe and Secure Robotics SIG Planning Meeting	31
Regional Seminars (NB: Attendee numbers for regional seminars are estimated as they are open access)	5
South East: AI and Cyber Security for Society	5
Northern Ireland: Cyber-Resilient Innovation	12
North East: Detection of AI-Generated Images Using Combined Uncertainty	29
Measures and Particle Swarm Optimised Rejection Mechanism	55
Wales: Multiparty Computation for Privacy Preserving Computing	30
Total number of event attendees	30
	25
	442

Table 3: Calls

Calls	Application Number
Call for SIG proposals (Oct-25)	
Sprite+/CRANE AI Sandpit (Awarded is number of Sandpit attendees)	



Current SIGs and WGs

Details on CRANE website

Inclusive Careers
WG

Research Practices
SIG

Learned Society
Formation WG

Safe and Secure
Robotics SIG

SANE (Secure,
Accountable, and
Efficient Networked
Systems) SIG

AI-Cyber SIG

Economics of Cyber
security SIG

Scottish regional CRANE meeting

Are you a cybersecurity researchers in Scotland? You are invited to join us at CRANE's first Scottish regional CRANE event of 2026! Come join us and hear about the Scottish... [Read more](#)

Cyber-Resilient Innovation Seminar

Taking place on 26th March this hybrid event is open to researchers, students, and industry professionals, and is part of CRANE's regional seminar series and organised in collaboration with Ulster University, Belfast, NI. This seminar will explore how cybersecurity awareness and research can support innovation, resilience, and responsible digital transformation.

A Whole Systems Approach to Securing Industrial CNI Systems – SEMINAR

CyberFocus and the University of Manchester are supporting CRANE as regional delivery partners for a new North West cybersecurity hybrid seminar series open to all with an interest in cybersecurity. Abstract: The increased convergence between Operational Technology (OT) and generic ICT capability, and the 'sudden connectivity' to environments

CRANE – NE Regional Cyber Security Seminar Series

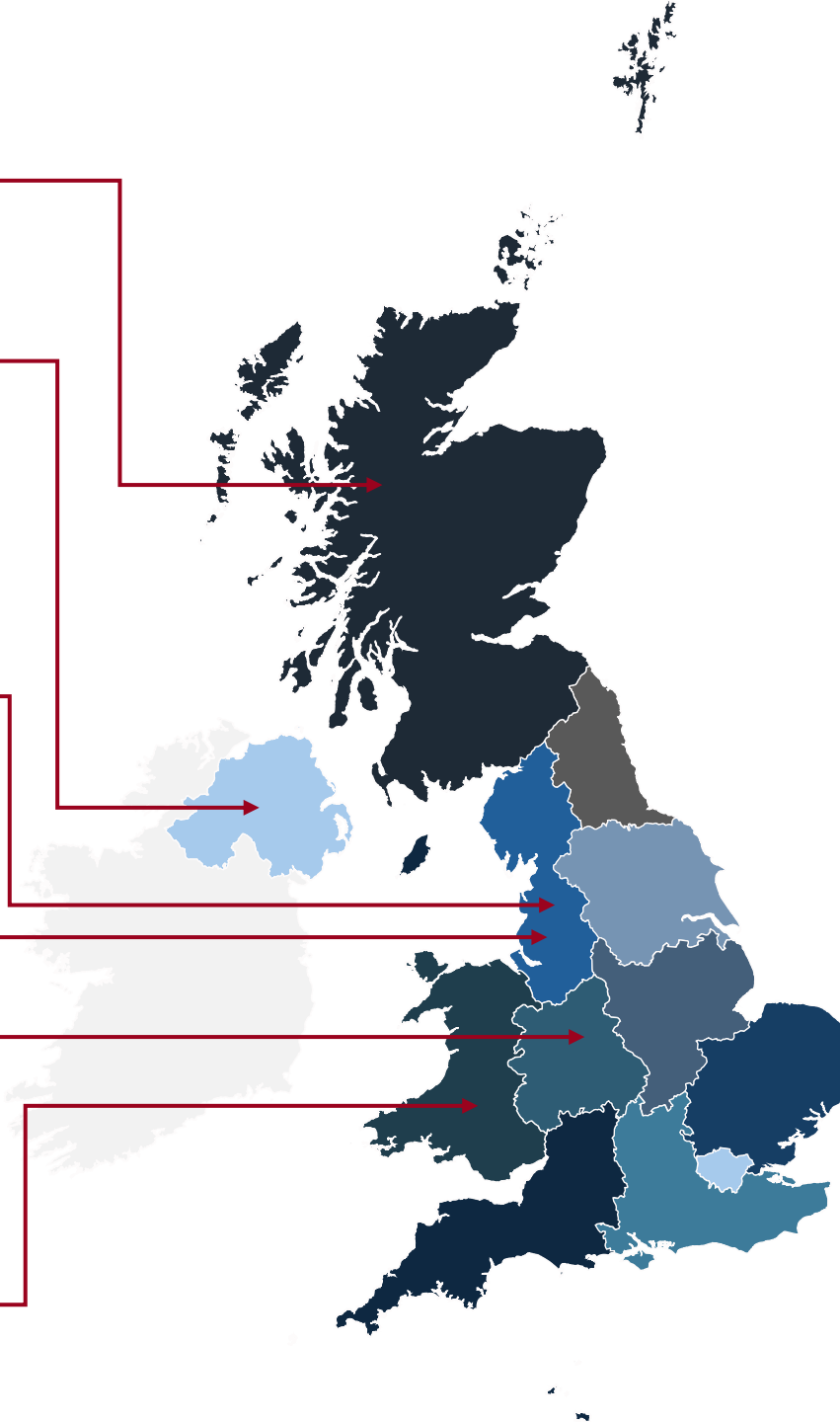
The inaugural 'CRANE – NE Regional Cyber Security Seminar Series' will be held at Northumbria on 27 March (Friday) from 10:00 – 13:00, focussing on NE universities and industries supported... [Read more](#)

CRANE West Midlands Regional Seminar – Cyber Security Emerging Threats

This seminar has been organised as part of the CRANE West Midlands regional seminar series. The event will include thematic talks, networking sessions, collaborative discussions, and research showcase activities aimed at fostering new partnerships and advancing cyber resilience research and innovation within the West Midlands and beyond. Participants from

Wales Regional Seminar Series: Multiparty Computation for Privacy Preserving Computing

MPyC is a Python package introduced in 2018 as a versatile framework for programming MPC solutions. This seminar discussed aspects of secure multiparty computation taking MPyC as primary example. It highlighted developments in usability, security, performance, and deployment of MPyC typical for the wider developments in MPC, touching on a wide range of topics such as outsourcing, threshold cryptography, fixed-point arithmetic, vectorized processing, and public verifiability. Watch the event recording here.





Technology Trends and Horizon-Scanning Report 1

Adam Joinson, Mark Ryan, Emma Walker,
Lynne Coventry, and Namrata Primlani



CRANE Phase One Pilot Projects Call

Securing Trust, Autonomy, and Resilience in Future Cyber Ecosystems

Call document

Publication date: 15th June 2026
EOI required by: 13th July 2026, 4:00pm UK time
Closing date: 31st July 2026, 4:00pm UK time

Item	Details
Funders	CRANE, under EPSRC Grant EP/Z534845/1
Funding type	Pilot research projects
Total funding available through this call	Up to approximately £580,000
Maximum project value	Up to £62,500 full economic cost (FEC) of which CRANE will fund 80% (£50,000)
Smaller project values	£22,500 FEC (of which CRANE will fund £20,000) £12,500 FEC (of which CRANE will fund £10,000)
Project duration	Up to nine months
Expected project start	October to December 2026
Expected project end	April to June 2027
Submission route	EOI: Submit your EOI before 13th July 2026 via: this link . Full Proposal: Submission portal will be available on the CRANE website by 30 June 2026 with a submission deadline of 31 July 2026.
Contact	crane@cs.ox.ac.uk

Summary

As part of [CRANE's](#) mission from EPSRC to strengthen the UK's cyber security research community, the network is funded to support pilot research projects. CRANE is structured into three phases across its five-year term, and this is the main call for proposals in phase one. Each phase includes a *technology trends assessment* process, and the report of this for phase one will be published alongside this call. That report has informed the topics of the call, and provides more context and detail on these.

We invite proposals from researchers at EPSRC-eligible organisations for projects in the topics detailed below. Your project must put cyber security at the centre of the research and explain the security threat, vulnerability, assurance challenge, or resilience problem that it will address. Although speculative and adventurous proposals are welcome, you should consider how to ground the project in a genuine use case or practical need.

We expect to fund a portfolio of feasibility studies, pilot projects, policy-focussed research, programme grant definition work, impact acceleration activities, and development work that can shape larger future research programmes or investments. You should set out a focused,

credible foundation for future research, translation, or

scati definition of research and should generally align to be at demonstrator phase or to go beyond technology only support activities that could be funded through a you cannot use this funding for studentships or student through a training grant.

CRANE member and employed at an organisation unding. You can [check your organisation's eligibility](#) ibility rules are relaxed, so if you are an early-career t to your organisation's policies, may request funds to D student and not employed in a research role, you are pply if you are solely based in an industrial

rtunity and encourage applications from [early-career](#) ly-career researcher in your own right, or with a mentor mmends this arrangement. More established research

single institution, or as a collaboration. While you do not nstitutions or with industry, as a Network+ we welcome ic sector, civil society, and international collaborations /or foster interdisciplinarity. You do not need to provide y relevant in-kind contributions, such as access to ies, or partner expertise. In the case of a collaborative m the lead organisation is needed, and although there is are available only to EPSRC-eligible research

st one proposal submitted for this call. You can be a oposals (whether lead or not).

for

ectly addresses one or more CRANE priority topics and y challenge at the heart of the work. Your application why the research is timely, and what contribution the k. While proposals may focus on technical dimensions, s (such as human aspects, governance, policy, and d in the context of emerging technologies.

r of your project. This may include a route to future orative programme, an open-source artefact, a brief, a standards contribution, a new industry or ble route by which the research could be

ust, Autonomy, and Resilience in Future Cyber l increasingly consist of autonomous and semi- oth cyber and physical domains. These smart infrastructure, distributed sensing systems, ents, alongside AI-enabled cyber tools for software on-making. Such systems will evolve continuously d models, and increasingly collaborate with both i, traditional static notions of "secure-by-design" ectures must instead be adaptive, resilient, and ng dynamically to changing environments, aviour.

mples of relevant research areas, but they are not

ritical infrastructure and organisational processes, ta, models, and outputs becomes a foundational a include methods for establishing or verifying the d content and protecting AI training and attacks, as well as methods for detecting erated data. Proposals might consider issues where AI systems increasingly interact with and

erging as highly networked, mobile, multi-sensor ack surfaces. Service robots, healthcare systems raise new challenges at the intersection my. Examples of topics include maintaining stems in open and potentially adversarial munication, coordination, and data handling efence against surveillance, covert sensing, and

AI collaboration

enerate software, monitor infrastructure, analyse onal decision-making. As these systems become ators, they introduce new forms of systemic risk

CRANE community
CRANE All-Hands meeting (E system)
dline
jins

ocs.ox.ac.uk. For questions bmission deadlines, contact

ge and process your funding uirements. We will treat gement Team and peer

ree months after the end of les Members' data more

alongside this call, and to be



Leadership Team



Andrew Martin
Professor of Systems Security
Department of Computer Science
University of Oxford



Lynne Coventry
Professor of Cybersecurity
Department of Cybersecurity and Computing
Abertay University



Adam Joinson
Professor of Information Systems
School of Management
University of Bath



Steven Murdoch
Professor of Security Engineering
Department of Computer Science
University College London



Mark Ryan
Professor in Computer Security
School of Computer Science
University of Birmingham

CRANE

Keeping it all running

Project team



Heather Browning-Lee
Programme Manager
Department of Computer
Science
University of Oxford



Maya Comfort
Communications Officer
Department of Computer
Science
University of Oxford



Pauline Perez
Project Administrator
Department of Computer
Science
University of Oxford

Community Advisory Board

Dr. Pamela Richards (University of Central Lancashire) – Chair
Prof. Andrew Martin (University of Oxford) CRANE PI
Prof. Adam Joinson (Bath University) CRANE Co-I
Prof. Steven Murdoch (UCL) CRANE Co-I
Prof. Mark Ryan (University of Birmingham) CRANE Co-I
Prof. Lynne Coventry (Abertay University) CRANE Co-I
Prof. Shujun Li (University of Kent)
Prof. Steven Furnell (Nottingham University)
Prof. Muttukrishnan Rajarajan (City St George's, University of London)
Prof. Siraj Ahmed Shaikh (Swansea University)
Prof. Lorenzo Cavallaro (UCL)
Dr. Lucas Cordeiro (University of Manchester)
Prof. Bill Buchanan (Edinburgh Napier University)

ECR Advisory Board

Dr Adam Robson (University of Sunderland) – Chair
Dr Mau Yuen (Kevin) Chan (University of Sheffield)
Dr Jeyamoham Neera (Northumbria University)
Dr James Ranjith Kumar Rajasekaran (Northumbria University)
Dr Magdalena Zajackowska (Loughborough University)
Dr Muntadher Sallal (Bournemouth University)

CRANE Advice and Accountability

Independent Steering Group

Chris Johnson (Chief Scientific Advisor DSIT, Queen's University Belfast) – Chair
Prof. Alice Hutchings (University of Cambridge)
Dr. Nick Allott (CEO, NquiringMinds Ltd)
Prof. Angela Sasse (Ruhr University Bochum, Germany)
Prof. Paul Watson (Newcastle University)
Romnik Thind (Portfolio Manager, EPSRC)
Thalia Liang (HP Labs)

Prof. Andrew Martin (University of Oxford) CRANE PI
Prof. Adam Joinson (Bath University) CRANE Co-I
Prof. Steven Murdoch (UCL) CRANE Co-I
Prof. Mark Ryan (University of Birmingham) CRANE Co-I
Prof. Lynne Coventry (Abertay University) CRANE Co-I
Dr. Pamela Richards (University of Lancashire) CRANE Advisory Board Chair



replacement for All-Hands event

CRANE looking ahead

further SIG call

international

wider engagement

inclusion/feedback
survey

mapping project

industry

NCSC

other parts of
government

professional
groups and
consortia

regions + clusters



CRANE looking ahead more

- Five-year programme; three-phase approach
- Phase One ends in March 2027
 - We will review everything we've been doing, and decide what to continue, what to change, what to replace, what to add
- This review will keep us all on our toes
 - CRANE leadership team; SIG leads, and more
 - Also an opportunity to renew our **Community Advisory Board**: elections? nominations?
- Planning for All-Hands 2027
 - opportunity to co-locate other events
 - talk to us about event planning



CRANE much further ahead

- the CRANE grant/project ends in 2030
- by phase 3 we will have refined the things that work and are valuable
- the planned Learned Society will take those forward
- Shujun Li is leading the WG planning this



Learned Society Update

Shujun Li (University of Kent)
Chair, LSFWG (Learned Society Formation Working Group)



Phase One Pilot Projects Call

Securing Trust, Autonomy, and Resilience in Future Cyber Ecosystems

Mark Ryan



The Funding Opportunity at a Glance

Item	Detail
Total pot	Up to £580,000
Max project	£62,500 FEC → CRANE funds £50,000
Mid project	£25,000 FEC → CRANE funds £20,000
Small project	£12,500 FEC → CRANE funds £10,000
Duration	Up to nine months
Start	October–December 2026
End	April–June 2027

CRANE funds **80% of full economic cost** — no match funding required



Why This Call, Why Now?

Future digital ecosystems are changing fast:

- **Autonomous and semi-autonomous AI** operating across cyber and physical domains
- **Robotic platforms, smart infrastructure, distributed sensing**, cooperating AI fleets
- Systems that **evolve continuously after deployment** and collaborate with humans and other AI agents

The old model is broken:

Traditional static notions of 'secure-by-design' has become insufficient.

*Future security architectures must instead be **adaptive, resilient, and continuously verifiable**.*



Three Research Themes

The call is organised around three overlapping areas – proposals may span more than one:

1. **Trust, provenance, and AI integrity**
2. **Secure cyber-physical autonomy**
3. **AI-augmented decision-making and human–AI collaboration**

These are illustrative, not exhaustive – the key requirement is that **cyber security is at the centre** of your research



Theme 1: Trust, Provenance, and AI Integrity

As AI embeds in critical infrastructure, how do we know what to trust?

Example research directions:

- Verifying **provenance and authenticity** of AI-generated content
- Protecting AI training and deployment pipelines against **supply-chain attacks**
- Detecting **manipulated, synthetic, or adversarially-generated data**
- Security in ecosystems where **AI systems increasingly interact with and build upon one another**



Theme 2: Secure Cyber-Physical Autonomy

Robots and physical systems as networked, mobile, multi-sensor attack surfaces

Covers: service robots, healthcare assistants, autonomous infrastructure, drone fleets

Example research directions:

- Security and resilience of cyber-physical systems in **open, adversarial environments**
- Architectures for **secure communication and coordination** across heterogeneous robotic fleets
- Defence against **surveillance, covert sensing, and data exfiltration**



Theme 3: AI-Augmented Decision-Making and Human-AI Collaboration

AI as a collaborative agent alongside human operators – new systemic risks

Covers: AI-generated software, infrastructure monitoring, operational decision support

Example research directions:

- Securing AI systems against **manipulation and unsafe behaviour**
- Ensuring **transparency, explainability, and meaningful oversight**
- Avoiding **automation bias** and maintaining human control
- **Market incentives** for adoption of secure products and services



Project Types

Match your ambition to the available time and budget:

- **Feasibility studies** — test a new idea, method, dataset, or collaboration
- **Pilot research projects** — evidence, pre-demonstrator prototypes, evaluation approaches
- **Policy-oriented research** — translate cyber security evidence into actionable recommendations
- **Impact acceleration / translation** — must stay within TRL 4

You choose the mix of PI time, RA time, and other costs — no prescribed formula



Who Can Apply

Must be

- A full CRANE member
- Employed at an EPSRC/UKRI-eligible organisation

Relaxed rules

- Early-career researchers can apply in their own right and request salary costs
- Solo individual, single institution, or collaboration – all welcome

Not eligible

- PhD students not in a research employee role
- Those solely based in an industrial establishment
- Award panel members

Each CRANE member may **lead at most one proposal** and be named on **at most two**



What a Strong Proposal Looks Like

Your proposal must clearly address:

1. The cyber security **threat, vulnerability, or resilience challenge**
2. Research **question, objectives, and method**
3. **Novelty** beyond existing work
4. Fit with **call topics**
5. Expected **outputs and deliverables**
6. **Legacy** — route to future funding, practice, policy, or community impact
7. **Team, roles**, and in-kind contributions
8. **Management plan**, timeline, and risks
9. **Responsible innovation** — ethics, D&I, trusted research, dual-use



Assessment Criteria

Reviewers will score against seven criteria:

Criterion	Key question
Fit to call	Is cyber security central? Does it match a topic?
Research quality & novelty	Clear question, appropriate method, genuine contribution?
Importance of threat	Does it matter to future tech, practice, or policy?
Deliverability	Is the plan realistic for the size and timeline?
Outputs & legacy	Credible route to impact, further research, or adoption?
Value for money	Resources justified and proportionate?
Responsible research	Ethics, D&I, trusted research addressed?



How to Apply – Documents Required

1. **Project proposal** (free format, within word limit)
 - Up to £10k → 1,500 words | Up to £20k → 2,500 words | Up to £50k → 4,000 words
2. **Financial summary** using CRANE pro forma (with justification of resources)
3. **Commitment letters from external partners** where your project depends on their contributions – but no generic letters of support without specific commitments
4. **Institutional agreement letter** signed by your responsible officer (typically HoD/HoS)

AI tools may be used in preparing proposals – you remain responsible for all content.

We may use AI tools in our evaluation – subject to institutional limitations



Key Dates

Date	Action
Now	Read the call and technology trends report
By 30 June 2026	Submission portal opens on CRANE website
13 July 2026, 4pm	Expression of Interest deadline (mandatory)
31 July 2026, 4pm	Full proposal deadline
Sept 2026 (wk 1–2)	Prioritisation panel
11 Sept 2026	Outcomes notified
Oct–Dec 2026	Projects begin
Apr–Jun 2027	Projects end

EOI asks for: proposer names, title, topic keywords, and budget band – **no changes allowed after submission**



Next Steps

If you are interested

1. **Read the technology trends report** (published shortly)
2. **Submit an EOI by 13 July** — this is mandatory and locks your budget band
3. Prepare your proposal offline — the portal does not support saving work in progress
4. Get your **institutional agreement letter** signed before the 31 July deadline
5. Contact **crane@cs.ox.ac.uk** with questions

Remember: speculative and adventurous proposals are welcome — ground them in a genuine use case



Questions about the call?

crane@cs.ox.ac.uk

crane.ac.uk

The background is a solid blue color. Overlaid on this is a faint, light blue circuit board pattern. A large, dark blue silhouette of a bird, possibly a crow or raven, is positioned on the right side, facing right. The bird's head is turned slightly towards the center. The text "Wrapping up" is written in a white, sans-serif font, centered horizontally and partially overlapping the bird's body.

Wrapping up

Other questions?