Department for Science, Innovation and Technology Call for Information: Secure AI infrastructure

UCL's Policy Impact Unit provides professional policy engagement expertise across the Faculty of Engineering, collaborating with leading researchers to help incorporate evidence into the policy decisions.

Neuroware is an Innovation & Knowledge Centre (IKC) led by UCL, with a consortium of leading UK institutions[1]. Neuroware connects industry partners, researchers, investors, policymakers and networks nationally and globally to accelerate the development, commercialisation and adoption of neuromorphic hardware. Our consortium of experts makes us uniquely placed to contribute to this Call for Information. This submission will highlight the benefits of neuromorphic computing and prove it is an effective tool for enabling a more efficient and secure AI ecosystem.

This submission has been prepared by Latisha Gordon, Policy Adviser at the UCL Policy Impact Unit and Neuroware Innovation & Knowledge Centre.

Consultation was undertaken with the following academic experts:

- **Professor Tony Kenyon**, Director of Neuroware & Professor of Nanoelectronics & Nanophotonic Materials, Department of Electronic & Electrical Engineering, UCL
- **Dr Adnan Mehonic**, Associate Professor in Nanoelectronics, Department of Electronic & Electrical Engineering, UCL
- **Professor André van Schaik**, Furber Chair of Neuromorphic Systems Engineering, Director of the International Centre for Neuromorphic Systems, The University of Manchester
- **Professor Steve Furber**, Professor Emeritus, Department of Computer Science, The University of Manchester

---

Neuromorphic computing is technology inspired by biology, designed to mimic the neural systems found in the human brain. Neuromorphic chips operate in a fundamentally different way to the silicon chips found in traditional computers. In the brain, processing and memory functions are performed by neurons and synapses in a single location. Conventional computers that we use today have separate memory and processing units. Neuromorphic computers will perform these tasks on one chip. This will remove the need to transfer data between memory and processing units, which will speed up processing time and reduce the energy use involved.

[1] Including Cambridge, King's College London, Imperial, Manchester, Oxford, Sheffield, Strathclyde, and the National Physical Laboratory

In the medium term, hybrid conventional computers with neuromorphic chips could vastly improve performance relative to conventional machines. Long term, a new, fully neuromorphic computer will be fundamentally different and powerful for specific applications (from natural language processing to the operation of driverless cars). Neuromorphic computing offers a major opportunity to positively transform the way in which we operate as a society – from tackling the sustainability crisis, to improving national security and driving economic growth.

Question 1: How do you assess the risks to the confidentiality and integrity of model weights, sensitive data, and system configurations in AI compute environments? How is your organisation or sector working to address these risks?

1. Neuroware provides the structure, scale and support to turn the potential of neuromorphic computing into real-world impact. Neuromorphic systems will be less reliant on large, centralised training sets and can instead learn in more adaptive, "biological" ways, reducing exposure to malicious data manipulation**.** This contrasts with conventional large language models, which have deep embedded bias structures shaped by their extensive training data.

2. One of the promises of neuromorphic technologies is supercharging power-efficient edge computing and enabling sensitive information to remain on local devices – such as wearables, smart cameras and medical sensors – rather than being transmitted to the cloud, significantly reducing exposure to cyber-attacks. By analysing data locally, **neuromorphic systems minimise the number of external data transfers, lowering the risk of interception or tampering and boosting UK resilience**. It also means a reduced reliance on one company's product, where any potential outages[2] could cause significant delays worldwide, including for UK government departments, and pose a threat to critical national infrastructure. **Neuromorphic approaches are therefore an increasingly effective means of strengthening AI security by combining reduced data exposure with more resilient, biologically inspired learning mechanisms**.

3. In 2025, a UCL researcher completed a two-year Royal Academy of Engineering fellowship[3] with HMG Communications Centre looking into the resilience of neuromorphic systems to cyber-attacks. The results[4] show that **neuromorphic systems can be made robust to adversarial attacks, while simultaneously driving energy efficiency,**

[2] https://www.bbc.co.uk/news/articles/cev1en9077ro

[3] https://raeng.org.uk/programmes-and-prizes/programmes/uk-grants-and-prizes/support-for-research/uk-ic-postdoctoral-research-fellowships/

[4] https://pubs.aip.org/aip/aml/article/3/1/016111/3335208

compared to other computing systems. Neuromorphic systems promise substantial efficiency gains, potentially extending battery life in low-power edge applications such as temperature and position sensors. At the same time, they offer a pathway to reducing the energy demand of large-scale data centre computing, thereby lowering greenhouse gas emissions associated with digital infrastructure.

Question 2: What current or emerging technologies, methods, or architectures could improve the security of AI infrastructure in large-scale compute environments?

4. **Neuromorphic systems are being delivered, and hardware capabilities are already in manufacture, however there is scope for wider adoption across the AI ecosystem**. In terms of technical feasibility and timelines for deployment, large scale neuromorphic systems are already being deployed. For example, the University of Manchester has been supporting an open service on its million-core SpiNNaker system since 2016[5], and in 2025 SpiNNcloud Systems GmbH started shipping datacentre-scale SpiNNaker2 systems co-developed by Manchester and TU Dresden within the EU Flagship Human Brain Project.

5. For smaller data sets (such as a fit-bit or Oura ring), whilst the hardware is there, the algorithms are not. Therefore, we are 5-10 years from deployment for these technologies. Researchers at UCL have already built prototype neuromorphic chips – a major step in developing this new technology. In the next 3-5 years, researchers at UCL expect to be using their chips to increase the efficiency of conventional computers by creating 'hybrid' machines.

6. **Whilst the UK has existing capabilities in this space, there is a strong case for aligning more closely with our European partners,** in order to build the level of sovereign capabilities to rival large powers, such as the USA and China. The UK has some systems strengths but is too small and not on the right scale to do everything on its own, without Europe.

7. Under the recent UK-Netherlands Innovation Partnership[6], artificial intelligence and computing technologies is mentioned as one of the three areas for further collaboration. Other countries, including the USA, Switzerland and Italy, have invested heavily and are making significant progress. It is vital the UK leverages its bilateral relations across Europe to drive forward progress.

---

[5] https://www.scieng.manchester.ac.uk/tomorrowlabs/spinnaker/

[6] https://www.gov.uk/government/publications/uk-netherlands-innovation-partnership/uk-netherlands-innovation-partnership

8. **Many challenges, including security and privacy concerns and the end of Moore's Law, have the potential to be mitigated to some extent by the use of neuromorphic hardware in the future mix of computing technologies**. More broadly, neuromorphic computing offers the UK an alternative pathway to scale AI capability without exponentially increasing energy consumption or exposing critical systems to growing cyber risk. These characteristics position neuromorphic computing as a strategic technology for secure and sustainable AI deployment in national security contexts and across high growth sectors of the economy.

9. In conclusion, neuromorphic computing offers significant potential for strengthening secure, autonomous AI systems, particularly in environments where limited power availability and poor energy efficiency currently restrict deployment. **Any system operating independently with minimal human intervention stands to benefit from the inherent efficiency and robustness of neuromorphic approaches.** While bespoke neuromorphic technologies can greatly enhance the resilience and performance of AI, realising this potential will require targeted investment from government and industry. The specific features embedded in early neuromorphic systems will depend on which sectors adopt them first, with government users likely to prioritise different security and capability requirements than commercial organisations.