Sprite+

Security, Privacy, Identity, Trust,
Engagement, NetworkPlus

ANNUAL REPORT 2025

CONTENTS

DEMOGRAPHICS

ACTIVITIES IN 2025

29 projects funded

8 events

4 workshops

FUNDING

35 grants allocated, totalling **292k**

MEMBERSHIP

1139 members, of which **259** are Expert Fellows

136 higher education institutes

182 from academia

313 from other sectors

161 industry

61 small-medium enterprises

66 government

10 self-employed

14 third sector

A MESSAGE FROM OUR DIRECTOR

It's been quite a year for SPRITE+ and something of a critical one for the TIPSS field, as the AI zeitgeist has intersected heavily with everything we do.

We decided to break the moratorium on discussing AI as, although things have not exactly quietened down, they do seem to have reached something of a dynamic equilibrium. So, we focused our annual Expert Fellows Meeting on all things AI and have formed a community of interest to take the work forward. Our first job was to produce a set of explainers, each giving a short introduction to an important interaction between AI and TIPSS.

Our Deep Dives are all now running or about to start, with the last two on Neurotechnology and XR having recruited research fellows to start in the new year.

Our collaborations are building too. For instance, our sandpit in June was a collaboration with SALIENT, the resilience research hub. Resilience and TIPSS go hand in hand, so it was a natural partnership, and this has been recognised by the UKRI who invited us to jointly bid for funds under the safer streets call – watch this space!

Another partnership that is going well is with Greater Manchester Combined Authority. They are working with us on our TIPSS in Digital Cities and Connected Places deep dive and the goal for that project is to come up with a charter for digital cities – a set of principals to engender citizen trust. This is vital work – as the Toronto waterfront debacle illustrated. Digital cities can and should enhance citizens' lives, not be imposed upon them.

Tech for good is a great aspiration, but if it's to be more than that, then work needs to be done across the piece; technical, policy, legal, and we believe that SPRITE+ is contributing to all of the above.

Professor Mark Elliot

SPRITE+ BACKGROUND

SPRITE+ is the UK Network Plus for Security, Privacy, Identity and Trust in the Digital Economy, funded by engineering and physical sciences research council (EPSRC).

Our mission is to deliver interdisciplinary engagement between people involved in research, practice, and policy relevant to digital trust, identity, privacy, and security (TIPS).

SPRITE+ is funded until 31st August 2027. In this phase, we aim to build our membership, expand the breadth and depth of our innovation, and deepen our impact through proactive engagement.

SPRITE+ operates according to four interrelated principles:

1. Interconnection:
Making magic in the joins. Digital TIPS challenges and opportunities are best addressed with interdisciplinary government-industry-citizen engagement.

2. Diversity:
Great innovation from diverse voices. Our commitment to equality, diversity, and inclusion (EDI) is woven through all our activities. We take practical steps to encourage and facilitate participation.

3. Challenge:
Encouraging challenges to traditional perspectives. We embrace cybersecurity perspectives, but we actively seek to broaden and challenge our understandings of digital TIPS for the benefit of society.

4. Collaboration:
Support; Communicate; Network. We work closely with cognate organisations and networks with an ethos of collaboration, and seeking opportunities for leverage and support, not duplication.

This report focuses on SPRITE+'s recent activities between October 2024 and September 2025.

OUR AIMS

As SPRITE+ evolves and expands, its aims and deliverables have also evolved and expanded.

Our focus areas are identified as below:

1. Expand our TIPS network:
Harness the expertise and collaborative potential of national and international TIPS communities.

2. Identify and prioritise future TIPS research challenges:
Establish a horizon-scanning function, and run innovation forums; Produce academic papers and white papers; Stimulate discussion at our network events.

3. Explore and develop priority research areas to enhance our collective understanding of future global TIPS challenges:
Run four intensive projects, co-created with partners to optimise relevance and impact.

4. Stimulate innovative research to advance understanding of digital TIPS:
Sandpit projects; Industry led problem calls.

5. Deepen engagement with TIPS research end users across sectors to accelerate knowledge exchange:
Hold research showcase events, involve stakeholders in workshops, and hold events hosted by project partners.

6. Understand, inform and influence policymaking and practice at regional, national and international level:
Drawing on other activities – feed through into policy and practice; Give early notice to stakeholders of critical socio-technical change.

These form the basis of the various work packages across SPRITE+.

ACHIEVING OUR AIMS

SPRITE+ is achieving its aims through engagements with the SPRITE+ community, Project Partners, Academia and Government.

Activities across the reporting period include: a Sandpit on TIPS and Resilient Futures Annual Showcase; Academic Industry Meeting (AIM) Day; Workshops; Expert Fellows Meeting; Human-centric Cybersecurity Partnership (HC2P) Innovation Fora and the commencement of our Deep Dive Projects.

These activities have fostered collaboration between academics, industry professionals and government to further research and practical outputs in the TIPS space. A summary of each can be seen on the following pages.

2025 SHOWCASE

On the 8th September, we held our annual showcase online. In a series of 15-20-minute talks, participants heard from the awardees of the 2024 sandpit on 'Living in an authentic world' including:

- **MICHA - Benevolent Bots for Combatting Misinformation in Online Health Forums: User Attitudes and Design Requirements** - *Philip Fei Wu, Royal Holloway, University of London.*
- **FinFraudSIM: Financial Fraud Simulative Analytic Research Platform** - *Lena Podoletz, Lancaster University Law School & Edward Apeh, University of Bournemouth.*
- **UNMASKED: The Theatre of Inauthenticity** - *Luca Viganò, King's College London.*
- **Improving and Understanding Misinformation Correction Acceptance: Insights from the Fact-Checked Project** - *Grégoire Burel, The Open University.*

Please see the appendix for further information regarding these projects.

We also had the opportunity to hear from our Innovation Fora hosts on:

- **Building swift trust in supply chains: bridging technology with social interactions** - *Dr Nikolai Kazantsev, University of Cambridge.*
- **Do you know your AI from your Generative AI**? - *Dr Huma Shah, Coventry University.*
- **Verifiable AI with Self-Sovereign Identity, a Socio-Technical Exploration** - *Nicky Hickman, Cheqd.*

Later, our AIM secondment awardees gave talks on their collaborative projects, including:

- **Post-Quantum Signature Implementation using PUF** - *Arnab Biswas, Queen's University Belfast.* Supporting partner: CryptoQuantique
- **Design and Execution of Cybersecurity Exercises for Realistic Data Collection** - *Çağatay Yücel, University of Bournemouth.* Supporting partners: Nvidia & Queen's University Belfast
- **Reinforcement learning for intrusion response in network security** - *Matthew Reaney, Queen's University Belfast.* Supporting partner: BT Group.
- **An AI-based Approach for Detecting Advanced Persistent Threats (APT) in Large Networks** - *Edward Chuah, University of Aberdeen.* Supporting partner: BT Group.
- **Improving Cybersecurity Through Culture: Temperature Platform and its Development** - *Lena Podoletz, Lancaster University Law School, & Midori Nishioka (Social Machines LTD)*

Please see the appendix for further information regarding these projects.

The recordings of these talks can be found on the **SPRITE+ YouTube channel**.

EXPERT FELLOWS MEETING

The 2025 Expert Fellows Meeting, framed around the current discourse about Human-AI relations was held at Radisson Hotel, York on the 6th-7th May with 64 attendees.

On day one, four talks were delivered focusing on the themes of: Cybersecurity, the future of AI, human-centric AI, AI ethics and standards, and AI regulation. These talks were:

- **A fireside talk by Dame Wendy Hall**, *University of Southampton, with Mark Elliot, SPRITE+ Director, University of Manchester.*
- **'Securing the Future: Industrial Research Insights on Leveraging AI for Cybersecurity'** – *Zeba Khanam, BT Group Research Manager.*
- **'AI, Trust, Identity, Privacy and Security'** – *Marie Oldfield, Oldfield consultancy*
- **'AI Regulation, or: How I Learned to Stop Worrying and Love the Online Safety Act'** - *Andreas Haggman, Ofcom*

On day two, the event started with a social design jam introduced by *Sownak Roy, Senior Engineering Manager at Cheqd*. The discussion centred around '**how can we build, develop and maintain healthy and trustworthy AI-human relations?'**.

Our closing keynote talk was from *Kanta Dihal, a lecturer at Imperial College London*. It was centred around **the stories humans have constructed about intelligent machines across ages and cultures**.

At the end of the Expert Fellow Meeting, there was a call for working group participants that had a strong response. The writing group will produce and document the SPRITE+ collective position on AI with eight AI explainers in the works

MEMBER EVENTS

SPRITE+ encourages members to run their own TIPS focused events. Members proposals should be creative and multidisciplinary, with up to £1500 available to run the event.

CAN WE TRUST AI WITH OUR WORK? EXPLORING TRUST, PRIVACY & SECURITY WITH AI TECHNOLOGY

On the 4th September, Elfredah Kevin-Alerechi, Founder and Chief Technological Officer of JournoTech hosted an event in London, bringing together 26 experts in government, industry and research, exploring the use of AI in journalism. The event started with a keynote speech by the host, who explored the uses and misuses of AI in journalism. Then, two sessions exploring modern applications of end-to-end encryption and the impacts of AI on EDI were presented, which led to fruitful discussion.

The event was interspersed with opportunities for networking and cross-field engagement, with researchers emphasising practical solutions to data privacy and AI use, whilst journalists highlighted the challenges of AI in the media landscape.

This event allowed JournoTech to showcase their AI platform NewsAssist, which helps media professionals summarise, transcribe and analyse documents. Participants highlighted the practical uses of AI in journalism and how to mitigate risks and maintain trust and data privacy in the face of an AI-driven world.

THE IMPACT OF EMERGING AND CONVERGING TECHNOLOGIES ON BIOSECURITY AND ITS EDUCATION: A SCOPING WORKSHOP.

On the 3rd-4th October, Professor Lijun Shang of the Biological Security Research Centre, London Metropolitan University hosted an event in London bringing together 16 international experts from America, Germany, China, and UK across academic institutions, civil society, coalitions and industry as well as members of the BSRC Staff.

Speakers at the workshop highlighted the need to develop realistic and measured assessments of risk and reflected on the need for a more behavioural-based approach to mitigate risks by building a robust culture of responsibility.

The workshop underscored that effective governance of emerging technologies depends on integrating technical vigilance with human-centred responsibility. While technological progress will continue to reshape the risk landscape, the participants emphasised that cultivating ethical awareness, adaptive education, and behavioural understanding will be critical for maintaining biosecurity and the norm against the use of CBW. Biosecurity education should evolve in tandem with scientific and technological change, ensuring that researchers, educators, and policymakers remain attuned to new forms of risk and responsibility.

INTERNATIONAL GRANT CALL

Sprite+
Security, Privacy, Identity, Trust, Engagement, NetworkPlus

UNSW Institute for Cyber Security

In 2025 we looked to strengthen our international partnerships and opened applications for the Bilateral SPRITE-IFCyber seed funding to support exchange visits between UK and Australian TIPSS researchers. The Institute for CyberSecurity (IFCYBER) is based at the University of New South Wales (UNSW) and is similarly transdisciplinary.

After a match-making process, joint applications were submitted to SPRITE+ and IFCYBER for reciprocal research visits. The successful applicants are listed below:

- *(SPRITE+) Dr Andrew Dwyer and (IFCyber) Dr Miranda Bruce:* **'Whole of Society for Cyber Power? A comparative analysis of privacy, identity, and trust in Australia and the UK'.**
- *(SPRITE+) Prof Hamed Haddadi and (IFCyber) Dr Arash Shaghaghi:* **'Protocol-Aware Traffic Shaping for Privacy-Preserving Encrypted Communications'.**
- *(SPRITE+) Dr Hossein Rahmani and (IFCyber) Dr Morteza Saber:* **'Assessing the accessibility of AI-based Face anti-spoofing technology for marginalised Australian communities'.**
- *(SPRITE+) Dr Ruba Abu-Salma and (IFCyber) Dr Rahat Masood:* **'Inclusive Privacy Protection for Marginalised Populations in Online Environments'**.
- *(SPRITE+) Dr Yongyu Zeng and (IFCyber) Jiaojiao Jiang*: **'Social Exclusion and Cyber Deception Social Network, Persuasive Language, and the Dynamics of Online Fraud'.**

£30,324.00 has been awarded across the projects which will be reported on in the 2026 Annual Report.

EARLY CAREER RESEARCHERS

Our programme of ECR-focused activities is helping equip PhD students, post-docs, and first-time lecturers with skills in research collaboration and end-user engagement through invaluable guidance, mentoring, training, and opportunities to network across sectors and disciplines.

FUTURE LEADERS WORKSHOP

RBOC Network

On the 11th September, we held a futures leaders conference at the NEC Campus, Birmingham, in collaboration with RBOC.

In a series of workshops, 18 participants were challenged to make decisions based on a series of real-world scenarios. With their group leader, their choices were evaluated, considered and challenged.

The goal was for early-career researchers to develop the necessary skills in timely and efficient decision-making required of them to become informed and capable leaders.

SUMMER SCHOOLS

HC2P (HUMAN-CENTRIC CYBERSECURITY PARTNERSHIP) 2025

SPRITE+ funded three PhD students, Monira Nazmi Jahan, Ammara Yasin and Anyi Liu, based at UK universities, to attend a two-week summer school hosted by the Université de Montréal and the University of Ottawa, Canada.

The two-week summer school called the 'Human-centric Cybersecurity partnership 2025' programme ran from the 9th-20th June. Here, participants had the opportunity to learn, challenge and research three main topics relating to human-centric cybersecurity, including regulation, behaviour and society.

Over the intensive two-week period, PhD students had the unique opportunity to collaborate on pertinent cybersecurity challenges, engage with leading figures in the cybersecurity community, participate in workshops, be mentored by professionals working in prestigious

industries, including IBM, and get to know their peers in an informal setting. All whilst exploring the beauty of Canada's most vibrant cities.

Most importantly, our students could expand on their own research and develop new frameworks incorporating HCP's research themes of addressing the relationship between people and cybersecurity.

Blog posts from the awardees can be found on the SPRITE+ website.

STRATHCLYDE INTERNATIONAL PERSPECTIVES ON CYBERCRIME SUMMER SCHOOL 2025

From the 25-29th August, the University of Strathclyde hosted their eighth Cybercrime Summer School for which SPRITE+ funded six PhD students to attend.

The summer school consisted of a one-day research symposium followed by four days of lectures and workshops with contributions from 23 speakers and highly engaged participants. Building not only on their current research topics but also broadening their scope of the field of cybersecurity, attendees also had the opportunity to network with other international post graduate researchers in their field from Germany and Canada, sparking potential for future fruitful collaborations.

Participants had the opportunity to engage with important and quality presentations on:

- cybercrime,
- critical infrastructures,
- disinformation,
- AI and
- data security.

Blog posts from the awardees can be found on the SPRITE+ website.

ACADEMIC-INDUSTRY MEETING DAY (AIM DAY)

On the 25th April, we held our annual Academic Industry Meeting (AIM) Day, designed to facilitate partnerships between industry experts and academics working on cognate issues in TIPS. The event was successfully held at PLEXAL London and included senior academics, Early Career Fellows, governmental agencies, SMEs and representatives from major tech companies.

Here, academics had an opportunity to present their research, representatives from industry could host a 'problem call', and both had the chance to network. The aim was to create partnerships between academia and industry. To facilitate this, SPRITE+ provided funding of up to £10,000 per partnership, in the form of secondments for Expert Fellows and funded placements for PhD students.

This was achieved through:

- Three-minute elevator pitches by attending academics on their research, expertise and proposed secondment topics.
- Three-minute elevator pitches by industry on their research and innovation challenges, and secondment opportunities for collaborative research. Non-academic organisations could also attend AIM Day without presenting.
- Regular networking breaks gave attendees a chance to meet and discuss potential collaborations.

From this event, we are funding seven projects including **four Expert fellow secondments** and **three PhD internships** worth up to a **total of £46K.**

INNOVATION FORA

Innovation Fora are academic forums which seek to develop, create and stimulate research developments in trust, identity, privacy and security (TIPS). Here, a leading group of academics and industry fellows discuss and develop a research framework on a certain theme for the development of better practices and policies around TIPS. Each innovation Fora is expected to produce an output that advances research in TIPS.

In 2025, SPRITE+ ran three Innovation Fora: 'Innovations in Data Synthesis', 'Digital Identities: A Policy Hackathon' with Chatham House and 'AI and Policing: TIPS Innovation Forum' with the N8PRP. We also funded three Innovation Fora: 'Best Practices for Trust in the Use of Generative AI Tools', 'Verifiable AI with Self-Sovereign Identity: A Socio-Technical Exploration' and 'Building Swift Trust in supply chains: Bridging Technology with Social Interactions'.

SPRITE+ has committed to co-designing two additional Innovation Fora and funding a further two in 2026.

SPRITE+ RUN INNOVATION FORA

INNOVATIONS IN DATA SYNTHESIS

On the 24th-25th July we ran an Innovation Fora on Innovations in Data Synthesis. We invited a multidisciplinary group of academics to speak on synthetic data, a field of research which encompasses anything from generative models to rule based simulations.

Talks included:

- **Using saturated count models for data synthesis** - *Robin Mitra, University College London.*
- **A brief introduction to SynDiffix and the Anonymity Loss Coefficient** - *Paul Francis, Max Planck System for Software Systems.*
- **A paradigm for creating synthetic data with utility and privacy assessment** - *Gillian M Raab, University of Edinburgh.*
- **Agent-based models to generate synthetic data** - *Dr. Julia Kasmire, University of Manchester.*
- **Two Worlds United? Synthetic Data in Computer Science and Statistics** - *Jörg Drechsler, Institute for employment research.*
- **Synthetic Data – a data owner's perspective** - Iain Dove, Office for National Statistics.
- **Applications of Evolutionary Data Synthesis** - *Mark Elliot, University of Manchester.*
- **Generating Private Databases with Markov Chain Monte Carlo** - *Harry Ros McArthur, University of Melbourne.*
- **The Simulacrum: Enabling real-world patient studies with privacy preserving synthetic data** - Lora Frayling, Health Data insight.
- **Federated Synthetic Data Generation** - *Rudolf Mayer, SBA Research.*
- **Generative AI Software for High-Fidelity Household Load Profiles** - *Centre for Net Zero.*

CHATHAM HOUSE HACKATHON

On the 9th, 11th and 18th September, we hosted an online Hackathon in collaboration with Chatham House's Common Futures Conversations Community on digital identity systems policy. This Innovation Fora was aimed at researchers, students and professionals up to the age of 35 and encouraged innovative and cross-directional thinking. Participants had the opportunity to hear from leading figures, including representatives from SPRITE+, and the Tony Blair institute.

Participants engaged in a Hackathon where they were tasked to develop a policy solution on digital identities. Exploring models where either the government, the private sector or a decentralised system would manage digital identity systems.

The policy solutions were presented to a panel of judges from both Chatham House and SPRITE+ members with backgrounds in industry and law.

The policy solutions are on the SPRITE+ website along with the winning group's presentation.

AI AND POLICING IN CONJUNCTION WITH THE N8PRP

On the 25th September, we held an Innovation Fora exploring AI and Policing. We brought together academics and members of the police force to develop a research protocol on the use of AI in policing, exploring themes of TIPS.

Themes broached included:

- The Role of AI in Modern/Future Policing
- Trust in AI Systems for Policing
- Identity, Surveillance, and Privacy
- AI and forensics

SPRITE+ FUNDED INNOVATION FORA

BEST PRACTICES FOR TRUST IN THE USE OF GENERATIVE AI TOOLS

On the 22nd May, Dr Huma Shah, assistant professor at Coventry University, ran an event on public perceptions of AI and generative AI (GenAI). First, questions were gathered through a GDPR compliant survey before a hybrid (online/in-person) international panel of 135 participants was encouraged to engage in a thought-provoking discussion on 'Do you know your AI from your Generative AI?'.

The event underlined that public perceptions around AI are completely captured by Gen AI, including generative text, images and videos. Concerns were raised that private data was being compromised, copyright law infringed, and trust and personal autonomy imperilled. With the increase in individuals using Gen AI for personal, academic and cooperate work.

On the 17th June, a roundtable was conducted on the pedagogical challenges of students' use of AI. Including whether to limit, encourage or incorporate AI in educational settings.

Across the two-day event the themes discussed were as follows:

- Trust in AI
- AI in healthcare
- AI models
- Copyright, Fair use, EU AI regulation
- Daily AI use including generative AI tools
- Mental health and online engagement

- GenAI in Education, changes and challenges to current pedagogical practise

At the end of the event, participants were encouraged to submit a post-event survey that would form the basis of a peer-reviewed paper around the topic of generative AI use and public awareness.

VERIFIABLE AI WITH SELF-SOVEREIGN IDENTITY: A SOCIO-TECHNICAL EXPLORATION

In collaboration with co-investigators: Ankur Banerjee and Javed Khattak, Cheqd hosted a Policy Hackathon.

With the use of AI and AI agents proliferating the cyber and public sphere, questions on how to develop, manage and design AI tools are vital. Therefore, the aim of this hackathon was to answer: 'How should we design, build and operate AI Agents for healthy and trustworthy relationships with humans and the natural world?'

Therefore, 84 participants, including social scientists and members from industry, were invited to discuss and demonstrate how decentralisation and self-sovereign identity technologies can create secure and trustworthy AI agents.

From the event, two guides were produced, which serve as a framework for developers of autonomous systems and those more broadly interested in the environmental applications and cultural effects of AI agents. A report on the novel social design methodology of this Innovation Fora was also produced.

This can be found on the SPRITE+ website.

BUILDING SWIFT TRUST IN SUPPLY CHAINS: BRIDGING TECHNOLOGY WITH SOCIAL INTERACTIONS

On the 27th March, Dr Aniekan Essien, along with Dr Nikolai Kazantsev, hosted a workshop on how technology can build "swift trust" within supply chains. The Innovation Fora started with a presentation by the hosts on the importance of trust in today's digital climate. Dr Svetlana Abramova added to the discussion by presenting a keynote on how cryptocurrencies and blockchain technologies create privacy, but also affect trust.

Participants were then split into three parallel sessions covering:

- The impact of central bank digital currencies on SMEs
- Social design for trust in digital ecosystemsSwift trusts in supply chains

Then, after talks which widened the discussion to broader data science themes, by Dr Palie Smith and Dr Mark Elliot, a panel discussion was conducted on how trust can be built and maintained during the merging of human and digital interactions.

SANDPIT

Sandpits are generative workshop forums typically held over five days, which welcome participants from multidisciplinary fields to engage in innovative discussions around a theme. The workshops can include: understanding the scope of the problem, creating shared terminology, and sharing expertise and highlighting research gaps. The outcomes of a sandpit are not predefined but often a range of outputs are presented from whitepapers, peer-reviewed articles and funding for a larger collaborative research project (UKRI, 2025).

In June 2025, we held our fifth annual Sandpit, with the theme 'TIPS and Resilient Futures'. Participants engaged in three online workshops and a two-day residential held in Crewe Hall Hotel. Up to £162K of funding was made available to participants from the Sandpit, with successful projects having the opportunity for 'Phase-1' funding from SPRITE+ to create a 'proof-of-concept' project, with the chance to apply for on-funding from SALIENT.

In 2025 SPRITE+ funded five projects:

- Beyond Mistakes,
- Building Societal Resilience,
- EVERESTS,
- Lex Lata 2075,
- Opening our eyes to the Panopticon, and
- RESCHAIN.

These projects will be funded for four months with their outputs ranging from peer-reviewed articles to webinars, policy briefs and reports.

DEEP DIVE PROJECTS

Our Deep Dive Projects identity four key and current research gaps in TIPS. All Deep Dive projects, at a minimum, aim to employ a key researcher who is responsible for conducting a year long research project, whose activities include conducting workshops where academic, industry and policy makers engage and produce outputs in the form of reports or research papers.

DEEP DIVE 1: TRUSTWORTHY DIGITAL IDENTITY

Identity is a core part of TIPS, and a key component of trustworthy digital systems.

SPRITE+ is working with the **Trustworthy Digital Identity programme at the Alan Turing Institute**, leveraging its connections and current Gates Foundation grant to develop an international network, including from developing nations interested in mitigating TIPS risks of and to digital identity

This multidisciplinary project seeks to understand the current scope and challenges of trustworthy and reliable national digital identity systems. The aim is to work with researchers and develop the appropriate methodologies, tools and frameworks to address the legal, social, technical and legal dimensions of digital identity.

We aim to answer:

- How can we build resilient digital identity systems?
- How can digital ID be breached/compromised?
- Who can be excluded from digital identity systems and in what ways?

In May 2025, we commissioned a researcher to conduct a deep dive project to address our research questions. To date we have run one online workshop in July focusing on Resilience in Digital Identity - Systemic Risks from Emerging Technologies. Additional workshops are planned for 2026.

DEEP DIVE 2: TIPSS IN DIGITAL CITIES AND CONNECTED PLACES

Greater Manchester (GM) is a growing and urban digital city implementing digital infrastructure in the regions of healthcare, transport, education, welfare, policing and security. Therefore, GM is a perfect laboratory to explore the processes and challenges of creating an inclusive, innovative and trustworthy digital city.

SPRITE+ in conjunction with Greater Manchester Combined Authority (GMCA), will highlight GM's digital ambitions and create a framework of good practise.

The aim: to create a charter for being an innovative and trustworthy digital city.

The objective: to use GM as a test case to develop a charter to define what makes a trustworthy connected place? And explore to what extent are these universal vs place-specific?

To date we have run two workshops with GM stakeholders and the public to feed into the construction of the charter. A rapid evidence review is underway and additional workshops and research outputs are planned for 2026.

DEEP DIVE 3: EXTENDED REALITY TIPS

Extended reality encapsulates technologies which seek to blend physical and digital environments, including virtual reality (VR), augmented reality (AR), and mixed reality (MR). Advancements in computational power have led to the steady rise of XR technologies (Ball 2024).

SPRITE+ expects advancements in XR over the next decade. Using Capgemini's "3 C's" principle, we expect XR evolution will be driven by:

- Convergence: merging XR with other, previously distinct, technologies
- Combination: using XR with other technologies for a specific purpose
- Compounding: technological advancements in XR and other emerging technologies building on each other.

In this Deep Dive we aim to build a community of interest that will address two broad questions:

- What are the most significant ways in which the convergence, combination, and compounding of extended reality and other emerging technologies could transform and disrupt TIPSS in the medium and longer term?

- What are the societal, technological, legal and ethical, and research implications of such disruptions?

In June we held a Community of Interest event that brought together around 40 Members and Expert Fellows. 16 rapid talks presented an impressive range of cross-disciplinary empirical data and scholarly analysis on risks and harms, and potential mitigations. This Community of Interest will run alongside the Deep Dive project which has to date employed a researcher to start at the beginning of 2026.

DEEP DIVE 4: NEUROTECHNOLOGY TIPSS

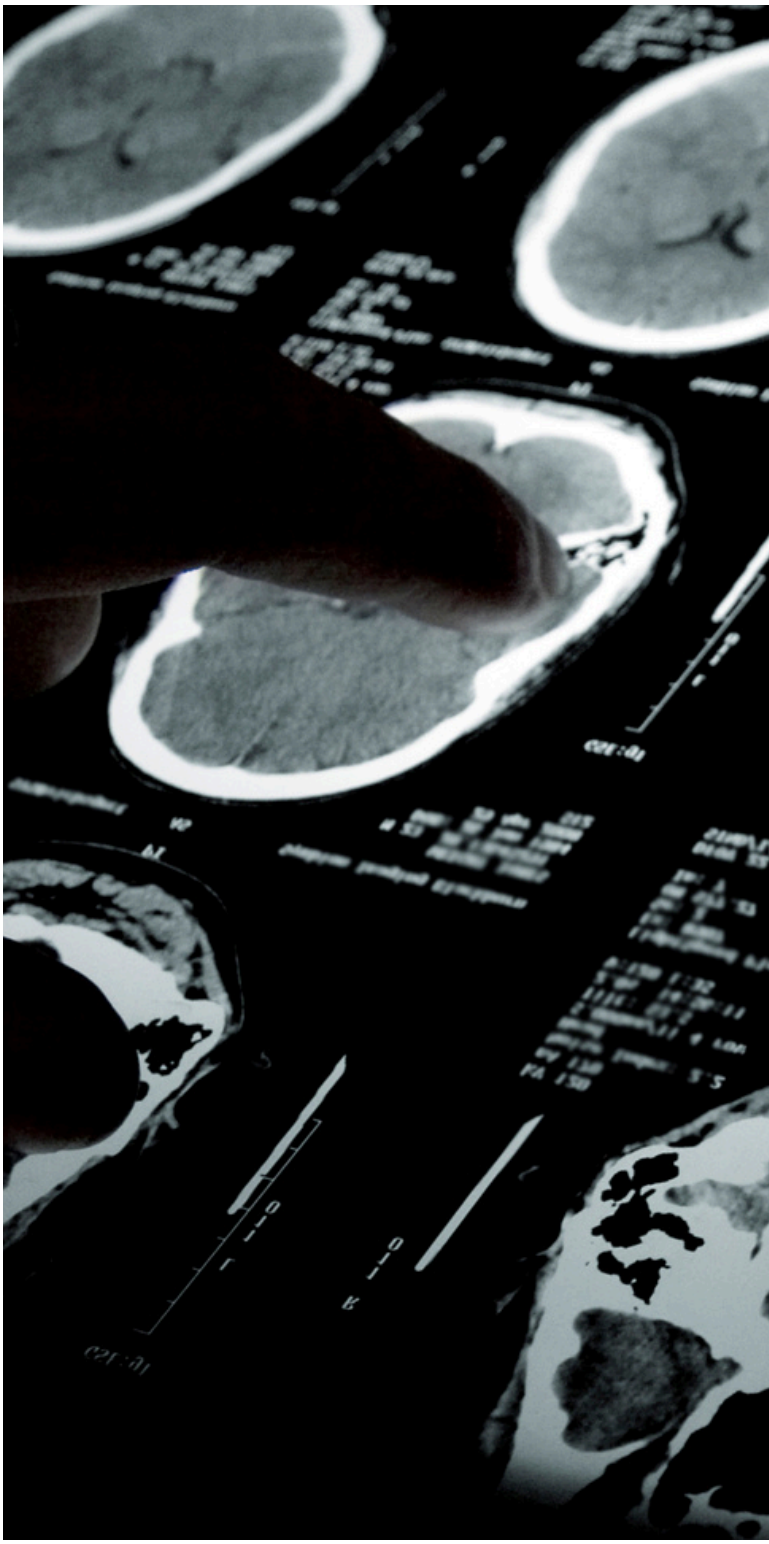
This Deep Dive focuses on the future expansion of neurotechnology and its implications on TIPS. Neurotechnology encompasses technologies that interface with the brain and nervous system, ranging from invasive neural transplants to non-invasive imaging tools such as EEGs (Ienca & Andorno, 2017; Yuste et al., 2017).

Similarly to XR, we expect Neurotechnologies to develop, change and evolve in relation to other emerging technologies such as XR and AI, according to the "3 Cs" principle developed by Capgemini.

We aim to build a community of interest to address two overarching questions:

- What are the most significant ways in which the convergence, combination, and compounding of neurotechnology and other emerging technologies could transform and disrupt TIPSS in the medium and longer term?
- What are the societal, technological, legal and ethical, and research implications of such transformations?

The community of interest will form in the later stage of 2025 and in earnest in 2026 with the commencement of a researcher.



ENGAGEMENT

SPRITE+ has intensified industry engagement over the last year.

Bringing industry perspective is essential to supporting the kind of research that makes a real-world difference. This was achieved through a number of events including the **AIM Day** - as described above - and the Sandpit.

The **SPRITE+ 2025 Sandpit**, held in collaboration with SALIENT, successfully brought together SPRITE+ Members and Expert Fellows to explore innovative ideas around Trust, Identity, Privacy, and Security (TIPS) and Resilient Futures. Industry partners Thales and Wavestone played a key role, offering real-world perspectives and practical insights that helped participants shape their research ideas to address current and emerging challenges in both digital and physical domains.

The **SPRITE+ Project Partner Challenge** is pivotal in addressing real-world challenges organisations face with cutting-edge research. An example of such a project is the **SPRITE+ Project Partner Challenge: Evaluating Fraud and Cyber Crime Behaviour Change Campaigns**, an ongoing collaborative research project funded through the SPRITE+ network in partnership with the City of London Police. The project focuses on assessing the real-world impact of public awareness and behaviour change campaigns designed to reduce fraud and cybercrime. Building on recommendations from HM Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS), the research team is working closely with law enforcement partners to develop a theory-driven, outcomes-based evaluation framework that measures actual behavioural change rather than just awareness. The project is also piloting innovative data collection methods to better understand how different campaign formats influence user behaviour, with findings expected to inform future national strategies for tackling online fraud and enhancing cyber resilience.

SPRITE+ is in discussions with a number of potential projects partners for more exciting and impactful Project Partner Challenges.

All **SPRITE+ Deep Dives** involve engagement with a wide range of stakeholders and connecting with new communities. For example, through Deep Dive projects such as **Deep Dive 4: NeuroTech TIPSS**, SPRITE+ is actively connecting with the vibrant neurotech community, fostering a growing network of interest, and planning a series of exciting events and collaborative projects as part of the Deep Dive initiative.

SPRITE+ has actively participated in **major conferences**, including the Security and Policing Conference, BIGSASIG, Manchester Tech Festival, ICE2025, and IGPP, using these platforms to raise its profile, engage with a wide range of stakeholders, and strengthen connections with industry partners.

MEMBERSHIP

Throughout 2025, SPRITE+ membership has grown by **120,** including **14 new Expert Fellow**s.

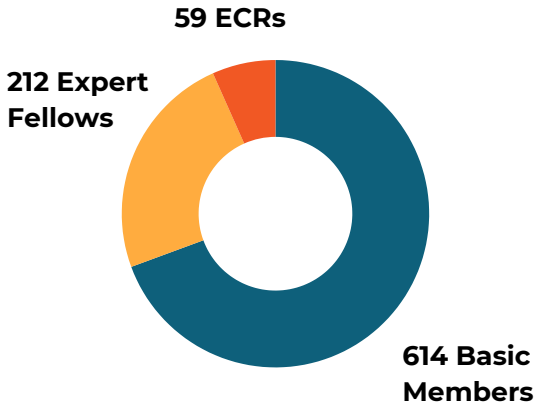
The SPRITE+ membership is broad, although heavily biased towards the Higher Education sector, with **826** members coming from **136 institutions** world-wide. In 2025 SPRITE+ has been strengthening its links with government and industry and will continue to do so in 2026 with the Deep Dive Projects focusing specifically on this group.

Overall **22.8%** of our membership are **Expert Fellows** with **211 academic expert fellows** and **48 professional practice expert fellows**.

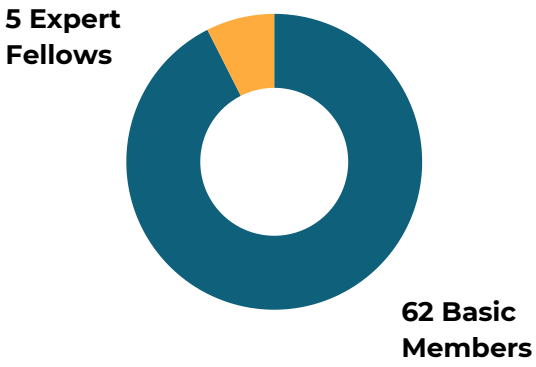
In 2025 we have introduced a number of initiatives targeted at Expert Fellows. These include: **Expert Clinics** – where organisations can meet with an Expert for an hour to discuss a challenge they may be having; **Project Partner Challenge Grants** – where organisations come to SPRITE+ with a challenge where they require expert input and after a tender process, the expert will second into the organisation to complete a project funded either jointly by SPRITE+ and the organisation or, solely by SPRITE+ and; **Lunch and Learn** - where SPRITE+ Expert Fellows have the opportunity to hold a TEDX style talk on their expert topic.

BREAKDOWN OF MEMBERS

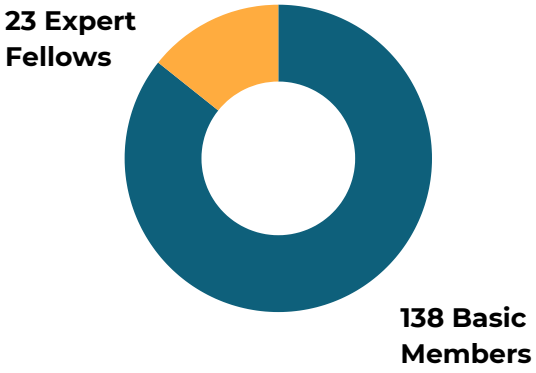
ACADEMIA: 826



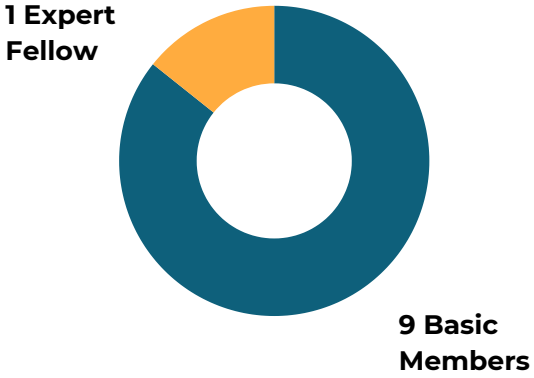
GOVERNMENT: 67



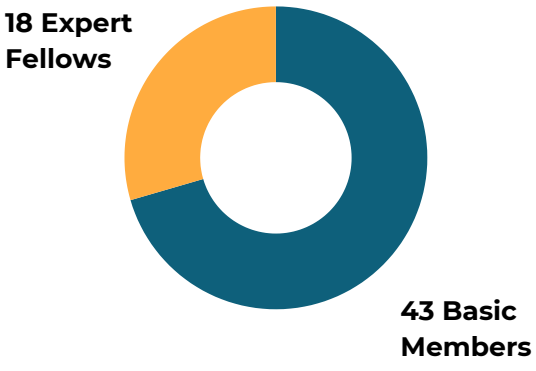
INDUSTRY: 161



SELF-EMPLOYED: 10



SMES: 61



NGOS & CHARITIES: 14

APPENDIX

Across 2025, the projects SPRITE+ funded in 2024 came to a conclusion and started to report on their progress and outcomes. The reports from the 2024 Sandpit " Living in an Inauthentic World", AIM Day secondments and Innovation Fora can be seen below.

SANDPIT PROJECTS

The 2024 Sandpit "Living in an inauthentic world" funded four projects at a total of £104K. The projects and their summaries can be seen below. All projects presented at the 2025 Showcase and can be seen online.

BENEVOLENT BOTS FOR COMBATTING MISINFORMATION IN ONLINE HEALTH FORUMS: USER ATTITUDES AND DESIGN REQUIREMENTS

PI Philip Fei Wu, Royal Holloway, University of London

This project aimed to address the spread of health misinformation in online forums. While generative artificial intelligence (GenAI) contributes to the proliferation of online health misinformation, it also presents opportunities to utilise the same technology for content moderation and the correction of misinformation. This project focused on understanding what users require and how they feel about using GenAI-powered 'benevolent bots' that interact with users in online maternal health forums to help combat misinformation.

The full report can be found here on the SPRITE+ website.

FINFRAUDSIM: FINANCIAL FRAUD SIMULATIVE ANALYTIC RESEARCH PLATFORM

PI Lena Podoletz, Lancaster University Law School

FinFraudSIM aimed to address the problem of online financial fraud. Fraud is the most common crime type in the UK. The Crime Survey for England and Wales registered over 3.8 million fraud incidents in the year ending in September 2024 (1). In 2023, 80% of fraud cases were deemed to be cyber offences (2). Financial fraud can cause great harm to individuals, businesses and other organisations, such as charities, as well as to the public sector and the whole of society. Such harms include financial loss, emotional distress, and loss of trust in society. According to the UK Finance Annual Fraud Report, in 2023 alone over £1.1 billion was stolen through fraud (3). Despite considerable efforts by the police, Government, financial institutions and other stakeholders, fraud is still on the rise with a 19% increase in the number of incidents in 2024 compared to the year before (1).

The complex and dynamic nature of financial fraud, particularly online fraud, demands innovative intervention strategies. While some technologies, like

behavioural biometrics and device analysis, have proven effective in early fraud detection, a comprehensive, interdisciplinary approach is crucial to ensure maximum protection for end users, especially as reimbursement laws evolve. Existing research related to online financial fraud has been often siloed with social scientific and technological perspective rarely converging. This fragmented approach fails to fully address the sociotechnical complexities of fraud. Moreover, current detection and prevention tools are often developed ad hoc, focusing primarily on financial organisations rather than a broader societal context. This gap in comprehensive understanding and integration limits the effectiveness of current interventions.

The full report can be found here on the SPRITE+ website.

UNMASKED: THE THEATRE OF INAUTHENTICITY

PI Luca Viganò, King's College London

The UNMASKED project aimed to develop and apply a synergy of devised theatrical performances and scientific methods rooted in computer science (human-computer interaction, cybersecurity, AI) and psychology to provide a novel approach to tackle the issue of inauthenticity in cyberspace.

The main idea underlying the UNMASKED project is that we can develop theatre as a transdisciplinary and socio-technical research space – a lab (The Theatre of Inauthenticity Lab) – and use this as a mechanism to identify the issues related to inauthenticity, (or expose) them, elicit an appreciation of inauthenticity, understand how inauthenticity is disseminated, and combat inauthenticity when used to harm, deceive and create conflict or tension. The Lab will also provide a means to reason about how to create and consume reliable inauthenticity. To that end, we aimed to develop and stage a devised theatre performance, collaborating with theatre-makers (with expertise in devised theatre) to engage audiences and have a platform to explore inauthenticity in cyberspace.

The full report can be found here on the SPRITE+ website.

IMPROVING AND UNDERSTANDING MISINFORMATION CORRECTION ACCEPTANCE: INSIGHTS FROM THE FACT-CHECKED PROJECT

PI Grégoire Burel, The Open University

The proliferation of misinformation presents a major threat to public discourse. While fact-checking offers a potential solution, fact-checks are not always accepted by the public. To understand the reasons behind the rejection of corrections and improve the communication practices of fact-checking organisations, the Fact-Checked project investigated how editorial style, publishing approaches, and communication methods may influence the acceptance, rejection and understanding of misinformation corrections.

Through the gathering of evidence from the literature and the analysis of responses to direct fact-checks, the project identified preliminary factors linked with the rejection of direct corrections. Interviews with international fact-checkers and the annotation of

more than a hundred fact-checks from multiple fact-checking organisations provided insights about the existing and emerging editorial policies and practices followed by fact-checkers.

With an additional survey of a thousand individuals across the UK, the project gathered supplementary insights about the overall perception of fact-checks in the UK and valuable knowledge for fact-checking organisations to develop more effective publication and communication strategies.

The full report can be found here on the SPRITE+ website.

AIM DAY PROJECTS

The 2024 AIM Day funded four academic secondment and one PhD internship totalling £32.5K. The projects and their summaries can be seen below. All projects presented at the 2025 Showcase and can be seen online.

DESIGN AND EXECUTION OF CYBERSECURITY EXERCISES FOR REALISTIC DATA COLLECTION

Çağatay Yücel, University of Bournemouth. Supporting partners: Nvidia & Queen's University Belfast

This secondment was hosted by Cyber AI Hub at Centre for Secure Information Technologies (CSIT) (as an NVIDIA Belfast Secondee) at Queen's University Belfast, with in-person visits taking place from 16th–20th December 2024 and 13th–15th January 2025, and ongoing collaboration maintained through weekly virtual meetings until the end of April 2025.

The primary objective was to design and support Capture-the-Flag (CTF) and hackathon-style events aimed at generating realistic, high-quality datasets for the digital fingerprinting of cyber-attacks. These datasets are intended to advance research in digital forensics and threat detection on NVIDIA GPUs/DPUs.

During the secondment, I contributed to the planning and delivery of cyber range activities that simulated both adversarial and benign behaviours. I carried out technical validation of the CTF infrastructure, replicated attack scenarios, and supported the execution of live events. I also provided specialist knowledge in cybersecurity event organisation and contributed to the design and implementation of an additional hackathon during the placement.

The collaboration will result in the creation of a curated dataset, which is intended to be released as open-source, and will serve as the basis for an academic publication detailing the methodology and research value of such synthetic data in cybersecurity.

My initial plan was to conduct two further visits to CSIT & NVIDIA Headquarters in Santa Clara, California, US and to contribute directly to the writing of the associated academic paper. However, as of 1st May, I commenced a new position of employment, which required me to formally conclude my involvement in the secondment and the related project earlier than intended.

The full report can be found here on the SPRITE+ website.

IMPROVING CYBERSECURITY THROUGH CULTURE: TEMPERATURE PLATFORM AND ITS DEVELOPMENT

Lena Podoletz, Lancaster University Law School

This project was protected by a Non-disclosure agreement and therefore detailed information cannot be provided. Dr Podoletz presented her work with Midori Nishioka (Social Machines LTD) at the SPRITE+ 2025 Showcase and **the recording can be viewed here**.

REINFORCEMENT LEARNING FOR INTRUSION RESPONSE IN NETWORK SECURITY

Matthew Reaney, Queen's University Belfast & BT Group

Rapid and effective response to cyber-attacks is crucial in network security to limit the damage caused by data breaches, ransomware and advanced persistent threats, which can escalate quickly. The longer such attacks remain undetected or uncontained, the more extensive the potential negative impact and losses related to sensitive data, reputation, and business operations, as recently seen in attacks targeting UK retailers.

Developing effective cyber-defence tools, using AI techniques to train active responses to cyber-attacks, is an important emerging research area that has great potential to help network operators contain attacks more quickly and comprehensively than possible by human monitoring and intervention alone. This collaboration between QUB and BT has focused on emerging research on training AI agents to recognise attack patterns within a network, particularly the use of deep reinforcement learning, to create AI tools that can respond and contain attacks with a degree of autonomy.

The full report can be found here on the SPRITE+ website.

POST-QUANTUM SIGNATURE IMPLEMENTATION USING PUF

Arnab Biswas, Queen's University Belfast. Supporting partner: CryptoQuantique

This project relates to digital vulnerabilities and post quantum resilience. Establishing the potential for an ongoing future collaborative relationship between Dr Arnab Kumar Biswas (from Centre for Secure Information Technologies) who is an expert in secure architectural solutions, and CryptoQuantique who are a leading provider of PUF based solutions for Internet-of-Things.

Specifically, the project concerns the design and implementation of a hash based post-quantum signature scheme using PUF. The aim is to use CryptoQuantique's existing PUF solution to design a post-quantum signature scheme. The PUF being used to generate or refresh keys and TRNG-generated random numbers thereby enhancing the signature scheme.

The full report can be found here on the SPRITE+ website.

AN AI-BASED APPROACH FOR DETECTING ADVANCED PERSISTENT THREATS (APT) IN LARGE NETWORK

Edward Chuah, University of Aberdeen.
Supporting partner: BT Group

The cost of cybercrime worldwide is expected to reach $15.63 trillion US dollars by 2029. Consequently, early detection of cyberattacks enables organisations to prevent and mitigate the damage associated with these cyberattacks. Large networks generate huge volumes of data and analysing this is key for detecting cyberattacks.

APTs are prolonged and targeted cyberattacks where an intruder executes various attacks and remains undetected for extended periods of time. Therefore they are one of the most concerning threats organisations face. Several recent advances in deep learning-based anomaly detection and zero-shot learning enable efficient training of complex machine learning algorithms for detecting cyberattacks.

This project will develop an AI-based approach using deep learning and zero-shot learning to solve two major subproblems: (a) model training time, and (b) identify patterns of events associated with APT attacks.

The full report can be found here on the SPRITE+ website.