An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCC
NATIONAL CYBERSECURITY COORDINATION AND DEVELOPMENT CENTRE
IRELAND

National Cyber Security Centre

Research and Innovation Priorities

November 2025 V1.1

ncsc.gov.ie/ncc-ie/research/

Co-funded by the European Union

An Roinn Dlí agus Cirt, Gnóthaí Baile agus Imirce
Department of Justice, Home Affairs and Migration

CYBER IRELAND
IRELAND'S CYBER SECURITY CLUSTER

The National Cyber Security Centre plays a central role in improving the State's cybersecurity resilience. As part of that work, we engage on an ongoing basis with researchers, research institutions, funding bodies and industry bodies across Ireland.

Contents

Background

The National Cyber Security Centre (NCSC) plays a central role in improving the State's cybersecurity resilience. As part of that work, we engage on an ongoing basis with researchers, research institutions, funding bodies and industry partners across Ireland. The areas set out below represent a living statement of the NCSC's research and innovation interests. They reflect the challenges identified through a formal research needs development process, internal and external stakeholder engagement, the findings of the National Cyber Risk Assessment and the emerging priorities shaping the next National Cyber Security Strategy and wider Government and European Union policy.

These topics are not intended to be exhaustive, nor do they represent a guarantee of partnership or co-funding. They are designed to serve three purposes:

1. **To provide a signal to research institutions** about areas of national importance where new evidence, methods, and insight would be of significant value to the State.
2. **To inform the wider ecosystem,** including Government departments, agencies, funders and industry, about the types of capabilities and knowledge that will underpin Ireland's long-term cyber resilience.
3. **To support evidence-based policy-making and operations** within the NCSC and across Government by encouraging research that addresses practical, real-world national needs.

The NCSC cannot collaborate on every project or work with every research group directly. However, progress across any of these areas will strengthen the national cyber ecosystem, contribute to improved collective resilience, and help ensure that the State is equipped to respond to a rapidly evolving threat environment.

We expect this list to evolve over time. As technologies change, as new risks emerge, and as Ireland's policy, economic and societal context develops, the NCSC will update these priorities to ensure continued relevance and alignment with national needs.

We welcome engagement from researchers and institutions who are working in, or planning work in, any of the areas identified below.

Priority Research Areas

1. Strategic Cyber Security and Sovereignty

Ireland is a small, open, highly digitalised economy that depends on global technology supply chains, cloud platforms, and foreign-owned infrastructure. Understanding the limits and opportunities of "operational sovereignty" is essential to ensuring that the State can securely provide public services, regulate critical sectors, and maintain national resilience while operating in this interdependent landscape.

- How can Ireland best assess the security, resilience and dependency implications of critical services hosted on foreign controlled cloud providers?
- What metrics would best help to quantify loss of operational sovereignty (e.g. single vendor risk, risks of reliance on non-EU technology vendors. etc.) for critical services within the State?
- What are policies that could assist in developing indigenous capabilities?
- What is the level of dependency on infrastructure where Ireland has low direct participation (e.g. satellite networks)?
- What will be the medium to long term implications for the Irish cybersecurity ecosystem from EU regulations that have Digital Sovereignty elements (e.g. EU ownership and control requirements, protection of data from unauthorised 3rd country access etc.)?
- How effective are sovereign cloud initiatives in improving resilience for Irish public sector systems?
- What national policies would substantially reduce risk without unduly harming cloud adoption and digital transformation?
- How can Ireland balance open research collaboration and intellectual property protection in cybersecurity R&D?
- What areas/sectors within the State are most exposed to cyber threats?
- What areas/sectors within the State should be prioritised for risk assessments from a cybersecurity perspective?

2. Behavioural Research and Cyber Psychology

Human behaviour remains the most widely exploited vulnerability. Understanding cognitive bias, motivation, trust, burnout, organisational culture, and communication practices is critical to designing effective interventions, shaping security policy, and improving national cyber hygiene across sectors.

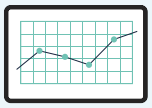
- What are the key motivating factors for threat actors? Are there any factors that are unique to Ireland with respect to this?
- How can our understanding of attacker and defender psychology improve? Examining motives, tactics, and decision-making of threat actors and defenders.
- What is the best approach to balancing cyber autonomy with human oversight - with increasing AI automation in cybersecurity how much control needs to be retained by humans?
- How do we better understand how the public engage with new technology and its associated cybersecurity risks?
- With respect to cybersecurity, how can we understand the pain points, needs and perceptions of Irish citizens and provide supports to address these?
- How does organisational culture in Irish entities influence reporting behaviour for cyber incidents, and what could be done to increase timely disclosure?
- Which messaging strategies would most effectively increase cybersecurity awareness and the adoption of cybersecurity best practice among Irish citizens?
- What behavioural metrics should Ireland implement to measure national improvements in cybersecurity awareness and culture?
- How does remote and hybrid work affect cybersecurity behaviour in Irish employees?
- What policies and incentive structures would be most effective to motivate SMEs to invest in cybersecurity?

3. Cybersecurity Skills and Capacity Building

Many countries, including Ireland, face a mismatch between graduate skills, employer expectations, and emerging workforce needs. A strong skills pipeline is essential for resilience across public administration, critical sectors, and industry. Evidence-based approaches are required to shape policy, education pathways, apprenticeships, and workforce planning.

- What education and apprenticeship models would be most effectively deployed within the State to assist in bridging the cybersecurity skills gap?
- How can Ireland foster collaborative cybersecurity research while protecting strategic IP and sensitive research?
- How can the State best support facilitating research access to EU funding?
- How should Ireland design and prioritise publicly funded cybersecurity R&D calls to maximise indigenous capacity and potential for IP development?
- Which metrics can be used to reliably measure R&I impact and progress on National cybersecurity resilience over time?
- Which accreditation and continuous professional development (CPD) pathways encourage retention of senior cyber staff in Ireland?
- How can Ireland incentivise lifelong learning in cybersecurity to keep pace with rapidly changing threats?

4. Regulatory Impact Analysis



New European cybersecurity mandates (NIS2, CRA, DORA, AI Act... etc.,) are reshaping sectors across the economy. Understanding the real-world impact of regulation on organisations, supply chains, costs, innovation, and compliance behaviour will help the State implement requirements proportionately and effectively.

- What is the current and future impact from IE and EU cybersecurity legislation?
- What level of preparedness is in place by in-scope entities to meet EU cybersecurity regulation (NIS2,CRA etc.) by sector?
- What are the best metrics for assessing any unintended consequences of cybersecurity legislation on businesses, innovation, and national security?
- Which compliance pathways (self-assessment, third party certification... etc.,) are most cost effective for Irish vendors to meet EU cyber regulations?
- Which metrics best quantify the societal benefit in Ireland from EU cybersecurity regulation?
- What transitional supports are needed for Irish SMEs to meet upcoming EU cybersecurity product regulation?
- How can the State best provide accessible information to Irish Citizens on navigating emerging cybersecurity regulation?
- What are the risks and consequences for Ireland if there is significant divergence between cybersecurity legislation in the UK compared to the EU?
- How will the implementation of EU cybersecurity regulation (e.g. NIS2, Cybersecurity Act, Cyber Resilience Act etc.) affect Irish SMEs' market access and compliance costs over the next 2–5 years?
- What are the projected economic impacts on the Public and Private sector from proposed EU data sovereignty measures?

5. Electoral Security and Cyber Interference

Democratic processes face growing threats from DDoS attacks, disinformation, social engineering, data compromise, and malign foreign influence. Ireland must understand and mitigate the risks to electoral infrastructure, political parties, and public trust.

- How effective are current detection and mitigation practices against disinformation campaigns targeting Irish voters on social media platforms?
- What is the current and future assessment of cyber threats to democratic processes (e.g. election interference tactics, disinformation campaigns, and digital voting security)?
- What policy interventions would most reduce the effectiveness of influence operations on the Irish Public?
- How can the State most effectively increase digital literacy, critical thinking and fact checking ability for both individuals and institutions?
- How can Ireland protect voter registration systems and digital services from targeted manipulation and cyber-attacks?
- Which early warning indicators would reliably predict escalations in foreign influence operations aimed at Irish elections?
- Which actions and exercises best prepare Irish election authorities for combined cyber and disinformation operations?
- What are the greatest cybersecurity risks to digital voting and what are the best mitigations that could be implemented to reduce risk?
- What metrics would best measure the success of State cybersecurity resilience investments to protect electoral security?

6. Surveillance, Intelligence, and Encryption

The State must maintain lawful, proportionate access to intelligence while protecting the rights and privacy of individuals. Rapid changes in encryption, device security, and global service provision challenge traditional models of lawful access and oversight. Ireland requires a clear evidence base to shape future legal and technical capabilities.

- What are the most important considerations when collecting data versus the right to privacy?
- Are there cyber implications related to the above, what are the cyber risks?
- How will State enforcement agencies and market supervision authorities operate with the expansion of emerging tech, end-to-end encryption and post-quantum cryptography?
- What is the future of intelligence collection in an encrypted world?
- What systems are needed for secure cross-border cyber threat intelligence and prediction?
- How can alert systems for cyber threats as they move within Ireland and across the EU be best implemented?
- What oversight mechanisms will best ensure accountability and proportionality in cyber operations?
- What needs to be implemented to govern the ethical use of AI in intelligence analysis?

7. Large-Scale Threat Detection and AI-Driven Security

Rapid detection is central to resilience. As systems scale, traditional signatures and rule-based detection may become insufficient. AI-assisted analytics, anomaly detection, LLM-based triage, and large-scale log analysis are now essential tools - but also introduce new risks. Ireland needs independent research to guide adoption.

- What will be the impact of regulation of AI and digital entities, and how can policy makers best adapt to the rapid pace of technological advancements versus regulatory timeframes?
- How can cyber threat intelligence be enhanced through automation?
- What are the risks and benefits of using AI to automate detection, response, and risk assessment?
- How should human intervention thresholds be set to balance automation judgement in SOCs?
- What workforce skills and tooling are needed to integrate AI into an organisation's cybersecurity ?
- What governance models are required to validate or certify AI security systems used in critical public services?
- What are the most critical AI and data sovereignty considerations, how can we ensure where and how citizens data is processed?
- How can statistical modelling for large-scale cyber threat detection be implemented?
- What are the most effective AI-driven approaches for identifying large-scale cyber threats in real time?
- What datasets and testing environments are needed to evaluate where large scale defensive AI could be used to protect Ireland's networks and CNI?

8. Cyber Resilience of Critical National Infrastructure (CNI)

CNI systems (energy, water, health, transport etc.) are increasingly interconnected and exposed to hybrid and cyber threats. Recent incidents underline the need for improved modelling, monitoring, incident response, and cross-sector coordination. Resilience at national scale must be grounded in research specific to Ireland's infrastructure environment.

- What CNI is dependent on shared infrastructure (e.g. external state energy supply) and how is this modelled across sectors?
- What could be implemented to minimise cascade failures because of a cybersecurity incident across Ireland's interconnected critical services?
- If a cyber incident caused an outage on a specific CNI, what would be the impact on services in Ireland?
- Which measures would most effectively reduce systemic risk from services provided by 3rd countries, but which are critical to CNI in the State?
- How can the State best assess and mitigate cyber risks to critical supply chains in sectors central to the economy (tech, pharmaceutical, agriculture, etc.)?
- How could the State best develop zero-trust frameworks for hyper-connected urban environments?
- How should risk modelling for cyber resilience in power grids, telecoms network, and transportation infrastructure be developed?
- What tabletop and live exercise programmes would best prepare the State and CNI entities for responding to simultaneous cyber and physical disruptions?

9. Quantum-Resistant Cryptography

The global shift to post-quantum cryptography is already underway. Ireland must ensure a secure transition for Government, regulated sectors, and critical infrastructure, while understanding risks from "harvest now, decrypt later" adversaries.

- What implications will quantum-resistant cryptography have on existing tech?
- What issues will quantum-resistant cryptography present for the NCSC and Regulators when managing cyber threats and incidents?
- What actions are needed to ensure we are nationally prepared for quantum-resistant cryptography?
- What are sustainability issues that may present with future large compute (e.g. energy grid)?
- What are the most critical public sector use cases for quantum resistant cryptography?
- How should Ireland best strategically implement a national migration to post quantum cryptography?
- What are the practical capabilities of quantum computing and how can it assist building more secure systems, threat detection, modelling, security protocols etc. ?
- What are the priority systems in the State which require accelerated migration to post quantum cryptography?
- Which pilot programmes could be implemented to best validate PQC performance and manage key rollover risks?
- Which training programmes, upskilling and undergraduate courses are needed to effectively build Irish expertise in PQC deployment and cryptographic engineering?
- How can Ireland best protect systems today to mitigate future harvest and decrypt threats?

10. Cybersecurity Risk Modelling for SMEs

SMEs form the foundation of Ireland's economy but often lack the resources and expertise of larger entities. They are disproportionately targeted by cybercriminals. National policy, grant schemes and guidance all require an accurate picture of SME cyber risk and maturity.

- What policies or initiatives can the State introduce that would be the most effective in reducing barriers for SMEs seeking to apply baseline cybersecurity best practices?
- What are the best methods of assessing the cyber resilience of small and medium enterprises?
- What are the best channels for effective communication on cybersecurity considerations to Irish SMEs?
- What factors most strongly predict cyber resilience in Irish SMEs?
- How can the State effectively measure and track the economic impact of cyber incidents on SMEs?
- What supports would best sustain ongoing cybersecurity improvements among Irish SMEs?
- How can the likelihood and impact of ransomware on Irish SMEs across sectors be best quantified?
- How effective is current guidance and best practices in materially reducing incident rates for Irish SMEs?
- Which public schemes, grants or other supports would most effectively encourage SMEs to implement essential cybersecurity controls?

11. Threat Analysis of Emerging Technologies

New technologies - AI systems, autonomous platforms, edge computing, digital twins, satellite, IoT, immersive environments - are reshaping risk landscapes at speed. Ireland needs forward-looking analysis to anticipate high-impact risks early and guide regulation, investment, and operational planning.

- How do we best define the cybersecurity threats from emerging technologies and what are the most critical areas to be aware of?
- What emerging tech will present the most significant threat from a cyber security perspective?
- What will be the implications on Irish data sovereignty?
- How can we ensure education resources keep pace with the evolving/emerging tech landscape?
- What are the implications for groups in society that may be "left behind" by emerging tech and what is the cyber threat from this?
- What cybersecurity risks follow increased integration of AI systems or other emerging technology into critical public services?
- How should Ireland prioritise R&D to assist with the threat analysis of emerging tech?
- How do we best define and identify the risks associated with AI-generated deepfakes and synthetic identities?
- What are the implications of automated cyber-attacks driven by AI and machine learning?
- How will emerging tech be used as part of combination attacks, where coordinated cybersecurity, disinformation and infrastructure attacks are used by threat actors?

We welcome engagement from researchers and institutions who are working in, or planning work in any of the priority research areas identified in this document.

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Contact Details

National Cyber Security Centre,
Tom Johnson House, Haddington Road,
Dublin 4, Ireland, D04 K7X4

info@ncsc.gov.ie

+353 1 6782333

www.ncsc.gov.ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre