

Supporting Briefing Document
Oireachtas Joint Committee on Artificial Intelligence
6 October 2026
David J. Hickton

I am David Hickton. From 2010 to 2016, I served as United States Attorney for the Western District of Pennsylvania, the chief federal law enforcement officer for the district, appointed by President Barack Obama. In that role, cybersecurity and cybercrime became a significant part of my work, including cases involving state-sponsored actors and major transnational cybercrime.

In 2014, our office brought the first criminal indictments of identified members of China's People's Liberation Army for hacking American companies to steal intellectual property.¹ Within weeks, we also indicted one of the world's most prominent Russian cybercriminals, whose organisation was responsible for hundreds of millions of dollars in losses and whose case included one of the earliest major ransomware prosecutions.² These and other cases gave me a very direct view of how quickly cyber threats can evolve and how difficult it is for institutions to respond after those threats have become established.

In 2017, I founded Pitt Cyber, an interdisciplinary academic think tank to formulate policy as we sit at the intersection of rapidly changing technology and slow-moving norms, conventions, and laws. We have worked on youth education and workforce development in partnership with the United States Air Force Association. We have also done substantive work in other areas such as election security, disinformation and artificial intelligence, and decision-making algorithms.

My work in Ireland has developed through a number of closely connected relationships. I hold a Visiting Professorship at Trinity College Dublin's (TCD) School of Law, and Pitt Cyber has developed a partnership with the Research Ireland ADAPT Centre at Trinity focused on research and teaching around the safe and ethical use of AI. That work now connects with the Trinity Centre for Digital Security and Societal Resilience, and Cyber Citizens, a National Initiative for Digital Resilience and Cyber Literacy led by the UCD Centre for Cyber Resilience Education in partnership with ADAPT at TCD, Oide Technology in Education, Webwise and Pitt Cyber at the University of Pittsburgh, with support from the Research Ireland Discover Programme. Cyber Citizens brings together strands designed to strengthen cyber resilience across different parts of society. Cyber Sense works with schools, families and libraries, while Cyber Smart for Public Leadership, which I co-lead, focuses specifically on elected representatives and public officials and on issues of responsible AI, cyber resilience and digital trust.

With that context, there are so many issues I would love to discuss with you but will today focus upon three:

¹ <https://www.justice.gov/archives/opa/speech/attorney-general-eric-holder-speaks-press-conference-announcing-us-charges-against-five>

² <https://www.justice.gov/usao-wdpa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware>

Protecting the Most Vulnerable

We all know how quickly fraud is evolving with the scale, speed, and accessibility of AI. Once crude schemes are now polished and convincing, especially to those most often targeted—including older adults and children.

We need to build civic resilience, practical skills, and general awareness among our most vulnerable populations. Pitt Cyber has been doing that by creating public digital skills workshops around topics like avoiding frauds and scams, keeping kids safe online, and finding reliable health information online. This curriculum was created with local organisations who understand the needs of their communities.

Cyber Citizens is building the same capacity in Ireland. The initiative has two interconnected strands. *Cyber Sense* works with schools, families, and libraries. A national Youth Panel consultation brought together young people to share their experiences of life online and discuss the digital issues that matter most to their generation.

My strong recommendation is that Ireland recognise trusted intermediaries already working with vulnerable populations, including libraries, schools, youth services and community groups, as part of the wider infrastructure of cyber resilience and ensure that they are equipped to play that role.

The same principle applies to public leadership. Through *Cyber Smart*, we are working specifically with elected representatives and public officials. Public leaders do not need to become technical experts, but they do need enough understanding to ask the right questions, recognise risk, understand where responsibility lies and know when specialist advice is needed. Building that confidence is itself part of institutional resilience.

But I also urge the Committee to consider additional structural action. AI is enabling scams and frauds at a scale and speed that no education effort, however excellent, can fully defend against. Expecting individuals to be the primary line of defence against transnational criminal enterprises using AI to generate cloned voices, deepfake calls, and personalised phishing messages is unrealistic. Preparedness and personal digital hygiene help but effective protection requires institutional interventions and coordinated state-level security frameworks.

There is also a wider structural issue. Recent investigative reporting has raised important questions about the economic incentives surrounding online fraud and fraudulent advertising.³ We are looking at a business model where the parties best positioned to stop the harm have an economic reason not to move too fast. Where platforms benefit financially from advertising ecosystems in which fraudulent activity occurs, the costs can fall disproportionately on individual users and wider society.

³ <https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/>

No amount of digital literacy education changes that incentive structure. Legislatures should therefore consider how they can hold platforms accountable when they enable fraud. We should be requiring obvious fundamentals, like verification and basic transparency of advertisers, fraud-reporting systems, and privacy-by-default protections.

Access: The Risks of Growing Economic Inequality

For years the United States thought that bridging the digital divide was as simple as access to devices and broadband. This access is important, but the skills to use those devices and services are just as important. Without government action, AI is likely to only exacerbate and entrench current problems and inequalities. In terms of economic inequality, there is a real risk that those with the skills to use AI and access to top-tier paid tools will compound their advantages, and others without those skills and points of access will fall further behind; while having their data from using these “free” tools exploited. This will be true for individuals, communities, and smaller organisations, including small and medium enterprises;⁴ and local governments—a demographic Pitt Cyber has been studying in relation to AI adoption and governance.

Ireland is well placed to confront this challenge. ADAPT at Trinity has significant research and public-engagement around responsible AI, accountability, inclusion and AI literacy. I would urge the Committee to treat AI literacy and access to low-cost or free high-quality, privacy-preserving AI tools as a core part of digital inclusion policy to curb the economic inequality that AI might bring. AI literacy should include proper instruction on governance for important public institutions like local governments.

But it’s not just skills gaps that drive inequality. Who is realising the financial gains from AI? Who is bearing the cost? AI infrastructure can generate considerable economic value, but it also places demands on energy, physical infrastructure and communities. Policymakers therefore need good evidence about where the benefits accrue and where the costs fall. As AI adoption accelerates, ensuring that its economic and societal benefits are shared as widely as possible should remain an important part of the policy discussion.

Jobs: Preparing for Workforce Disruption

A related issue is the concern about how AI will impact jobs. I come from Pittsburgh, a region that lost much of its steel industry in the 1980s. The region still feels the effects of this today. AI may bring change on an even larger scale across many sectors at once, and faster.

The reality is that you cannot manage what you do not measure. Around the world, workforce policy on AI is being made without accurate data. There is bipartisan legislation⁵ in the US Senate to add AI questions to federal labor surveys to capture the extent of job impact. Creating the right data infrastructure to identify not only job loss due to AI, but its impact on entry-level jobs, on the changing nature of work within individual job sectors, the possibility of wage stagnation, and what new jobs are being created and what new skills are needed is not a simple task. But it will rapidly pay dividends. Ireland has the chance right

⁴ <https://news.microsoft.com/source/emea/features/trinity-college-dublin-and-microsoft-ireland-research-shows-a-widening-ai-maturity-gap-between-smes-and-large-organisations/>

⁵ <https://www.congress.gov/bill/119th-congress/senate-bill/3339/text>

now to capture this kind of data, which will in turn allow it to respond with mitigation efforts to curb the coming effects of AI workforce disruption.

Pitt Cyber has been working in the space of workforce development for some time—but what is coming will require more than just skilling young people; it will also involve re-skilling current workers whose jobs are likely to change and morph due to AI exposure. That will require innovation and new kinds of education and accreditation programs for adult learners. My recommendation is that Ireland carefully measure AI's effects on work now, region by region, sector by sector, and invest in innovative upskilling and retraining pathways *before* displacement arrives rather than after.

Across all three areas, one lesson from the American experience is that we have too often waited for harms to become visible before responding to them. Ireland does not have to do the same. With this Committee's work, and with Ireland's Presidency of the Council of the European Union this year, Ireland has a chance to show that governing AI well means looking beyond the technology to the people and institutions it affects.

Our work through the Trinity Centre for Digital Security and Societal Resilience and Cyber Citizens are practical contributions to that effort. We want to bring together young people, families, communities, researchers and public leaders to learn and respond to different perspectives and situations. As our work develops, I would be very happy to share those insights, and the lessons from our wider transatlantic collaboration, with this Committee.

Thank you.