Centre for Emerging Technology and Security
EXPLAINER

The Alan Turing Institute

The EU AI Act: National Security Implications

Rosamund Powell
August 2024

*This is part one of a CETaS Explainer series on the **national security implications of international AI regulation initiatives**.*

All views expressed in this CETaS Explainer are those of the author, and do not necessarily represent the views of The Alan Turing Institute or any other organisation. We are grateful to Connor Dunlop, European Public Policy Lead at the Ada Lovelace Institute, and experts from the Special Competitive Studies Project, for reviewing an earlier version of this CETaS Explainer.

Introduction

The EU AI Act is expected to be the most consequential legislative framework for artificial intelligence (AI) to date. This new regulation will have significant implications for national security, both in the EU and beyond. This CETaS Explainer identifies key considerations for the national security community when preparing for the implementation of the Act.

What is the EU AI Act?

The EU AI Act is the first comprehensive, international regulation for AI. It aims to **protect fundamental rights** in the face of risks posed by AI and to **ensure AI is developed and used safely.** It was approved by the Council of the European Union on 21 May 2024 and **comes into force on 1 August 2024**.[1]

What are the key provisions of the Act?

- Establishes a tiered, **risk-based approach** to AI regulation.
- Imposes **outright bans** on AI systems deemed to pose **'unacceptable risk'**.
- Imposes **new obligations on developers of high-risk AI**, such as mandatory risk management processes and technical safety documentation.
- Introduces specific **provisions for 'general-purpose' AI models**, and transparency requirements around limited-risk AI systems.

What is the scope of the Act?

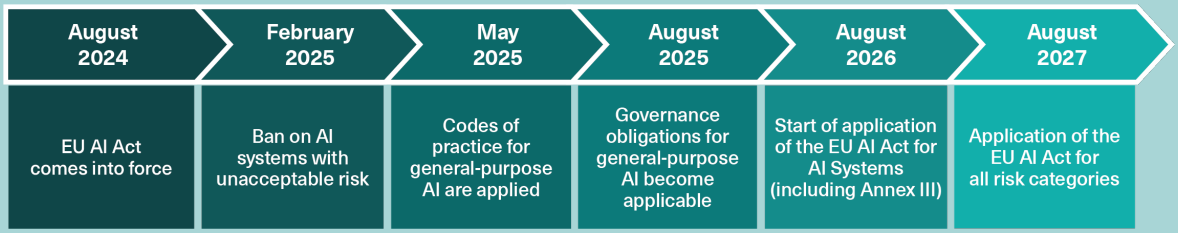
- The Act has **extra-territorial** scope and will apply to all organisations operating inside the EU, even if they are based elsewhere.[2]
- **Sectoral exclusions** are made for AI applications in **national security** and **defence** as well as for AI developed purely for **scientific research and development**.
- Some **specific provisions** are also made for **open-source** AI, for **law enforcement** applications, and for **public security**.[3]

Where does the EU AI Act sit in the broader regulatory landscape?

- The EU AI Act is the **first legislation of its kind** given its international scope and comprehensive requirements, but it is not the only relevant AI regulation globally.
- Several other regulatory efforts in Europe and elsewhere will have significant impacts:
    - Internationally, the **Council of Europe Convention on AI and Human Rights** was adopted in May 2024 and will be ratified later in 2024.[4]
    - National governments have also made progress. Most notably, **the US Executive Order on AI** was issued in October 2023,[5] while **AI Regulation in China** emerged even earlier (including key regulations in 2021, 2022, and 2023).[6]
    - Finally, certain local legislation will be significant, especially **state-level AI regulation in the US** which is progressing rapidly.[7]
- It is also crucial to situate the EU AI Act within the context of other EU digital regulation, most notably the general data protection regulation (**GDPR**), the **Digital Markets Act**, and the **Digital Services Act**.[8]

Timeline

Figure 1: Timeline for the implementation of the EU AI Act



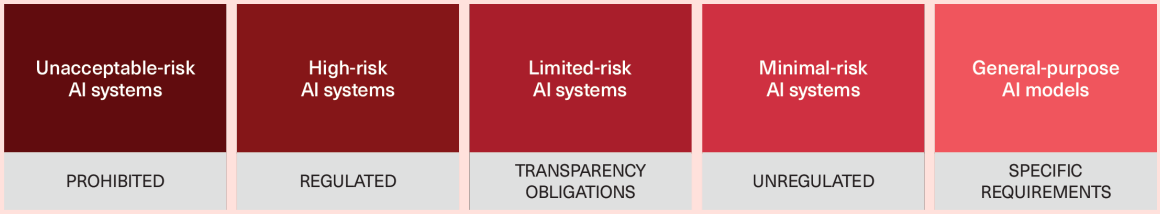
Source: Alexander Thamm, "EU AI Act Timeline," https://www.alexanderthamm.com/en/blog/eu-ai-act-timeline/.

The Risk-Based Approach

The EU AI Act takes a 'risk-based approach' to AI regulation to ensure the burden of compliance is proportionate to the risks posed by AI systems. In the final AI Act, AI systems are divided into five categories, each with different requirements (Figure 2).

- AI systems which pose an 'unacceptable' level of risk are outright banned, including social scoring systems and the inference of emotions in workplaces and educational institutions.[9]
- Most obligations, including the need to establish a risk management system throughout the AI lifecycle and to draw up technical documentation, are reserved for 'high-risk' AI system developers.[10]
- The EU Commission has emphasised that most AI systems currently fall into the 'minimal-risk' category and will face no regulatory requirements.[11] However, given the rapid pace of change in AI, clarity may be needed on whether this is still the case as the Act comes into force.
- Specific provisions are introduced for general-purpose AI models, proportionate to the level of risk. These include transparency obligations, self-assessment and mitigation of systemic risks, reporting of serious incidents, conducting model evaluations and ensuring cybersecurity protections.[12]

Figure 2: The risk-based approach in the EU AI Act



Source: Alexander Thamm, "EU AI Act Timeline," https://www.alexanderthamm.com/en/blog/eu-ai-act-timeline/.

Exclusions from the EU AI Act

The EU AI Act includes several sectoral exclusions, while certain sectors are still within scope of the Act but come with specific provisions (Figure 3).

Figure 3: Exemptions from the EU AI Act by sector

Sector	Defence and military	National security	Law enforcement	Public security	Scientific research and development	Open-source AI
In scope for the EU AI Act?	✕	✕	SPECIFIC PROVISIONS	SPECIFIC PROVISIONS	✕	SPECIFIC PROVISIONS

Source: Author's analysis.

The National Security Exclusion

Why is national security excluded?

An exclusion for national security was added to the Act for two reasons:

1. National security remains the sole responsibility of Member States, in accordance with Article 4(2) TEU (Treaty on European Union).
2. The specific nature and operational needs of national security activities, and specific national rules applicable to those activities.[13]

How is the scope of this exclusion defined?

1. This exclusion applies to both public and private entities developing AI systems solely for national security purposes.
2. The exclusion does not apply to any dual-use technologies that are also used outside of the national security context.
3. A definition of 'national security' is not provided within the act.[14]

Why has this exclusion been disputed?

The exclusion for national security has been debated extensively, both during EU AI Act negotiations,[15] and by human rights groups.[16] Key discussion points include:

1. The lack of clarity on the scope of 'national security'.
    - Some argue that 'national security' is not clearly defined in EU law, with significant variation in how the term is interpreted by Member States, leading to concerns around where the lines should be drawn between what is and is not excluded from the Act.[17]
    - These arguments are made despite the Court of Justice of the European Union formally defining national security for the first time in 2020 as a responsibility that 'encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.'[18]

2. Potentially blurred boundaries between 'national security' and 'public security'.
    - Public security is in scope of the AI Act with several specific provisions and exceptions,[19] but excluded entirely from related EU legislation (e.g. the Data Act).[20]
3. Arguments from human rights groups around the need to regulate AI in high-stakes national security contexts.
    - Several human rights groups have argued that the exclusion for national security 'is not justified under EU treaties' and that exemptions must be 'assessed case-by-case, in line with the EU Charter of Fundamental Rights.'[21]
    - The high-stakes nature of national security AI use cases has led to particular concerns around sensitive uses of AI going unchecked in contexts such as migration, surveillance, and biometrics. For example, concerns have been raised around surveillance technologies with potential to disproportionately impact marginalised groups and around risk assessment technologies used in the migration context.[22]

Why Does the EU AI Act Still Matter for National Security?

Despite these exclusions, the EU AI Act will have significant implications for the national security community, both within the EU and beyond. The national security community should prepare for the following key changes.

Dual-use technologies

The exclusion of national security from the EU AI Act only applies where AI technologies are used exclusively for national security. In any dual-use cases where an AI system is also deployed for civilian, humanitarian, law enforcement, or public security purposes, the AI Act will still apply.[23]

To avoid being underprepared, the national security community must assess the degree to which their use of dual-use AI technologies may fall in scope of the Act. This will be most relevant for two key areas of national security AI innovation, both explored in more depth below:

- AI applications procured or adapted from industry, including open-source AI.
- AI applications shared with other public sector bodies, such as law enforcement.

A shifting industry landscape

Concerns around the potential stifling of industry innovation frequently dominate discussions around the AI Act.[24] The national security exclusions laid out in the Act mean concern around diminished industry innovation may be less acute for the national security community compared to other sectors.

However, two factors combine to mean national security won't be entirely sheltered.

- Recent years have seen the national security community strengthen its relationship with the private sector on AI.[25] Costs make it challenging for national security to justify developing certain capabilities from scratch, for example generative AI capabilities. Instead, third-party AI is often the best way to harness innovation.[26]
- The development of new AI capabilities for defence and national security rarely begins with 'government technologists or defence contractors'.[27] Instead, the national security community are often interested in the same AI systems as everybody else, and in many cases would not on their own constitute a large enough market to make it worthwhile for industry to develop AI products just for them.

If the EU AI Act were to stifle AI innovation in Europe,[28] or hamper the success of start-ups,[29] these dynamics would to some extent impact national security innovation despite exclusions in the AI Act. This problem could become especially concerning if it contributed to a shift in the geopolitical dynamics of AI innovation. It is therefore crucial for the national security community to track the extent to which the AI Act influences global innovation patterns.

Nevertheless, the extent to which the Act will impact industry innovation remains unclear. The staggered implementation of the Act could lessen the EU's first mover advantage, while the more light-touch approach to AI regulation being taken in the US could dampen the influence of the EU approach on the global tech sector.[30] At the same time, EU officials emphasise that innovation is a high priority, for example noting how many AI products will fall into the 'minimal-risk' category and highlighting pro-innovation initiatives such as regulatory sandboxes.[31]

Finally, despite the Act being finalised, further decisions are still to be made, for example in designing Codes of Practice around 'general-purpose' AI models.[32] More time is needed to assess the degree to which the EU AI Act will affect industry, with knock-on impacts for national security.

Impacts on law enforcement

Law enforcement is within scope of the AI Act, with a number of specific provisions and exclusions applied. This will have two key implications for national security.

- Any shared capabilities between national security and law enforcement will need to be reviewed to ensure compliance with the Act, as will the precise division between what constitutes law enforcement activities and national security activities. Civil society groups have argued this distinction could be unclear given the broad definition of law enforcement offered in the act, in the absence of any definition for national security,[33] leading to significant practical challenges in defining *ex ante* whether a technology will be used exclusively for national security, rather than law enforcement.[34] Given that two of the eight AI applications set to be banned in six months are law enforcement technologies,[35] the consideration of law enforcement AI and the EU AI Act should be a priority for national security.

- Law enforcement has been given specific opt-outs from the EU AI Act which could offer lessons for the future of AI in national security. For example, the Act designates that for high-risk AI systems in law enforcement, registration obligations can be fulfilled in a non-public section of the EU database, and that post-market monitoring for high-risk AI systems should not cover sensitive operational data.[36] As EU law enforcement agencies start to implement the Act, the national security community should observe how these non-public options for reporting AI risks develop in practice. Given almost all AI regulation initiatives globally emphasise the importance of transparency obligations for AI developers, it may in the future become important to consider how national security organisations can meet AI risk reporting requirements without revealing sensitive information.

New best practice for AI risk management and human rights safeguards

Despite being excluded from compliance requirements, national security could learn from the best practices set out in the AI Act. For example:

- The requirements set out for 'high-risk AI' include the need to establish a whole-lifecycle risk management system, to ensure appropriate levels of accuracy, robustness and cybersecurity, to draw up technical documentation, and, for public sector deployers, to conduct a fundamental rights impact assessment.[37]

- The requirements set out for 'general-purpose' models with 'systemic risk' include the need for serious incident reporting and adversarial testing.[38]

Some have argued these requirements will be overly cumbersome for AI developers,[39] but if there is one domain in which extra care is required, it is national security where adequate scrutiny at each stage of the AI lifecycle is essential to avoid unintended consequences.[40] National security AI use cases have especially high requirements for cybersecurity, robustness, and accuracy,[41] all of which are set out in Article 15 of the Act.[42] Despite not being included in the regulation, national security agencies across the EU must prioritise addressing AI risks through applying best practice, and in doing so should consider which provisions and best practices set out in the Act they could implement voluntarily.

Additionally, the Act is already helping to accelerate the development of international technical standards on AI, particularly at the European standards development organisations (SDOs) CEN/CENELEC and ETSI. Harmonised technical standards, which are industry-led and voluntary, are key to the AI Act as they will specify how the requirements of the Act can be operationalised by developers. April 2025 has been set as a key deadline for SDOs to publish standards in time for high-risk AI requirements to come into force in August 2026.[43] Again, the implementation of these standards will not be mandated for national security, but they nevertheless provide a useful benchmark for the safe and ethical deployment of AI.

Finally, as the risk management processes set out in the Act become mandatory for industry, there may be benefits for AI procurement in national security. More information will likely be available to national security customers thanks to the Act, as industry suppliers start to comply with requirements around high-risk and general-purpose AI. This has potential to make AI assurance easier for national security. [44]

Conclusion

The national security community must prepare now for the implications of the EU AI Act, focusing especially on how the Act will affect law enforcement and industry innovation. At the same time, they should take stock of the potential benefits that can be harnessed as a result of the Act, especially thanks to progress on international technical standards and the expected increase in AI risk documentation from industry.

References

1. European Commission, "AI Act," https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai; Council of the European Union, "Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI," Press release, 21 May 2024, https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/.

2. Tim Hickman, "The EU AI Act's extraterritorial scope – Part 2," White & Case Article, 9 May 2024, https://www.whitecase.com/insight-our-thinking/eu-ai-acts-extraterritorial-scope-part-2.

3. Daniel Castro, "The EU's AI Act Creates Regulatory Complexity for Open-Source AI," Center for Data Innovation, 4 March 2024, https://datainnovation.org/2024/03/the-eus-ai-act-creates-regulatory-complexity-for-open-source-ai/.

4. Pascale Davies, "Council of Europe adopts first binding international AI treaty," *Euronews*, 17 May 2024, https://www.euronews.com/next/2024/05/17/council-of-europe-adopts-first-binding-international-ai-treaty.

5. The White House, "Fact sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence," 30 October 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.

6. Matt Sheehan, "China's AI Regulations and How They Get Made," Carnegie Endowment for International Peace Paper, 10 July 2023, https://carnegieendowment.org/research/2023/07/chinas-ai-regulations-and-how-they-get-made.

7. Cobun Zweifel-Keegan, "US State AI Governance Legislation Tracker," IAPP Article, last updated 25 June 2024, https://iapp.org/resources/article/us-state-ai-governance-legislation-tracker/.

8. White & Case, "AI Watch: Global regulatory tracker – European Union," White & Case Insight, 21 May 2024, https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-european-union.

9. "High-level summary of the AI Act," EU Artificial Intelligence Act, Future of Life Institute, last updated 30 May 2024, https://artificialintelligenceact.eu/high-level-summary/.

10. Ibid.

11. Latham & Watkins, *EU AI Act: Navigating a Brave New World* (Latham & Watkins LLP: July 2024), https://www.lw.com/en/admin/upload/SiteAttachments/EU-AI-Act-Navigating-a-Brave-New-World.pdf.

12. European Commission, "AI Act," https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

13. European Parliament, "Artificial Intelligence Act," https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

14. European Parliament, “Artificial Intelligence Act,” https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

15. Gian Volpicelli, “EU’s AI talks sputter over intrusive security loopholes,” *Politico*, 7 December 2023, https://www.politico.eu/article/ai-act-negotiations-enter-their-19-hour/.

16. European Center for Not-for-Profit Law, “Scope of the EU Artificial Intelligence Act (AIA): Military Purposes and National Security,” no date, https://ecnl.org/sites/default/files/2022-03/ECNL%20Pagers%20on%20scope%20of%20AIA%20ECNL_FINAL.pdf; European Disability Forum, “EU’s AI Act fails to set gold standard for human rights,” 3 April 2024, https://www.edf-feph.org/publications/eus-ai-act-fails-to-set-gold-standard-for-human-rights/.

17. Morrison Foerster, “EU AI Act – Landmark Law on Artificial Intelligence Approved by the European Parliament,”14 March 2024, https://www.mofo.com/resources/insights/240314-eu-ai-act-landmark-law-on-artificial-intelligence#section11; European Center for Not-for-Profit Law, “Scope of the EU Artificial Intelligence Act (AIA): Military Purposes and National Security,” no date, https://ecnl.org/sites/default/files/2022-03/ECNL%20Pagers%20on%20scope%20of%20AIA%20ECNL_FINAL.pdf

18. European Center for Not-for-Profit Law, “Scope of the EU Artificial Intelligence Act (AIA): Military Purposes and National Security,” no date, https://ecnl.org/sites/default/files/2022-03/ECNL%20Pagers%20on%20scope%20of%20AIA%20ECNL_FINAL.pdf.

19. European Parliament, “Artificial Intelligence Act,” https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

20. Morrison Foerster, “EU AI Act – Landmark Law on Artificial Intelligence Approved by the European Parliament,” 14 March 2024, https://www.mofo.com/resources/insights/240314-eu-ai-act-landmark-law-on-artificial-intelligence#section11.

21. European Disability Forum, “EU’s AI Act fails to set gold standard for human rights,” 3 April 2024, https://www.edf-feph.org/publications/eus-ai-act-fails-to-set-gold-standard-for-human-rights/; European Center for Not-for-Profit Law, “ECNL Position Statement on the EU AI Act,” 26 July 2021, https://ecnl.org/news/ecnl-position-statement-eu-ai-act.

22. Access Now, “Joint statement – A dangerous precedent: how the EU AI Act fails migrants and people on the move,” 13 March 2024, https://www.accessnow.org/press-release/joint-statement-ai-act-fails-migrants-and-people-on-the-move/; European Disability Forum, “EU’s AI Act fails to set gold standard for human rights,” 3 April 2024, https://www.edf-feph.org/publications/eus-ai-act-fails-to-set-gold-standard-for-human-rights/.

23. European Parliament, “Artificial Intelligence Act,” https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

24. Nima Montarezi, “The EU AI Act: Necessary regulation of a barrier to innovation?,” *Business Reporter*, 29 May 2024, https://www.business-reporter.co.uk/ai--automation/the-eu-ai-act-necessary-regulation-or-a-barrier-to-innovation; Hugo Guzman, “Innovation Concerns Grow Over EU AI Regulation,” 7 September 2023, Law.com, https://www.law.com/international-edition/2023/09/07/innovation-concerns-grow-over-eu-ai-regulation-378-229822/; Javier Espinoza, “Europe’s rushed attempt to set the rules for AI,” 16 July 2024, *Financial Times*, https://www.ft.com/content/6cc7847a-2fc5-4df0-b113-a435d6426c81.

25. Rosamund Powell, “Security services need industry-designed AI, but how can they trust it?,” Alan Turing Institute Blog, January 2024, https://www.turing.ac.uk/blog/security-services-need-industry-designed-ai-how-can-they-trust-it.

26. Ibid.

27. Noah Greene, “The EU AI Act could hurt military innovation in Europe,” Encompass Comment, January 2024, https://encompass-europe.com/comment/the-eu-ai-act-could-hurt-military-innovation-in-europe.

28. Pascale Davies, “Could the EU AI Act Stifle GenAI Innovation in Europe? A new study says it could,” *Euronews*, 22 March 2024, https://www.euronews.com/next/2024/03/22/could-the-new-eu-ai-act-stifle-genai-innovation-in-europe-a-new-study-says-it-could.

29. Ricki Lee, “Overregulating AI will lead to start-ups dying on the beach,” Tech Informed, 23 May 2024, https://techinformed.com/global-ai-regulation-eu-ai-act-insights-sim-conference-porto-2024/.

30. Benjamin Cedric Larsen and Sabrina Kuspert, “Regulating general-purpose AI: Areas of convergence and divergence across the EU and the US,” Brookings Article, 21 May 2024, https://www.brookings.edu/articles/regulating-general-purpose-ai-areas-of-convergence-and-divergence-across-the-eu-and-the-us/.

31. “High-level summary of the AI Act,” EU Artificial Intelligence Act, Future of Life Institute, last updated 30 May 2024, https://artificialintelligenceact.eu/high-level-summary/.

32. “An introduction to codes of practice for the AI act,” EU Artificial Intelligence Act, Future of Life Institute, July 2024, https://artificialintelligenceact.eu/introduction-to-codes-of-practice/.

33. Laura Lazaro Cabrera, “EU AI Act Brief – Pt. 2, Privacy and Surveillance,” Center for Democracy and Technology, 30 April 2024, https://cdt.org/insights/eu-ai-act-brief-pt-2-privacy-surveillance/.

34. European Center for Not-for-Profit Law, “Scope of the EU Artificial Intelligence Act (AIA): Military Purposes and National Security,” no date, https://ecnl.org/sites/default/files/2022-03/ECNL%20Pagers%20on%20scope%20of%20AIA%20ECNL_FINAL.pdf.

35. The two prohibited AI practices referenced here are, 1) AI systems for predicting the risk of someone committing a criminal offence and 2) The use of real-time biometric identification in public spaces for law enforcement unless it meets specific conditions of necessity set out in the Act. More detail on these practices can be found in Article 5 “Prohibited AI Practices,” European Parliament, “Artificial Intelligence Act,” https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

36. European Parliament, “Artificial Intelligence Act,” https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

37. “High-level summary of the AI Act,” EU Artificial Intelligence Act, Future of Life Institute, last updated 30 May 2024, https://artificialintelligenceact.eu/high-level-summary/.

38. European Commission, “AI Act,” https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

39. Pascale Davies, “’Potentially disastrous’ for innovation: Tech sector reacts to the EU AI Act saying it goes too far,” *Euronews*, 15 December 2023, https://www.euronews.com/next/2023/12/15/potentially-disastrous-for-innovation-tech-sector-says-eu-ai-act-goes-too-far.

40. Rosamund Powell and Marion Oswald, “Assurance of third-party AI systems for UK national security,” *CETaS Research Reports* (January 2024), https://cetas.turing.ac.uk/publications/assurance-third-party-ai-systems-uk-national-security.

41. Ibid.

42. European Commission, “AI Act,” https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

43. Hadrian Pouget, “Standard Setting,” EU Artificial Intelligence Act, Future of Life Institute, https://artificialintelligenceact.eu/standard-setting/.

44. Rosamund Powell and Marion Oswald, “Assurance of third-party AI systems for UK national security,” *CETaS Research Reports* (January 2024), https://cetas.turing.ac.uk/publications/assurance-third-party-ai-systems-uk-national-security.