Siân Berry MP
Brighton Pavilion
House of Commons
London SW1A 0AA

22 April 2026

The Rt Hon Darren Jones MP
Chancellor of the Duchy of Lancaster

The Rt Hon Chi Onwurah MP
Chair, Science, Innovation and Technology Committee

The Rt Hon Matt Western MP
Chair, National Security Strategy (Joint Committee)

By Email

Dear Darren, Chi, and Matt,

We are writing as a group of MPs concerned that the Government needs to take action to ensure the resilience of UK digital systems in the event of threats of or actual interference by a foreign government.[1] We are aware that this topic is a current concern of the Science, Innovation and Technology Committee, which Chi chairs. Additionally, we know that the Joint Committee on the National Security Strategy, which Matt chairs, is responsible for scrutinising the structures for government decision-making on national security, particularly the role of the National Security Council and the National Security Adviser.

The National Risk Register, which is maintained by Darren as the Chancellor of the Duchy of Lancaster, identifies the risks that: "would have a substantial impact on the UK's safety, security and/or critical systems at a national level."[2] It lists a number of potential risks of cyber-attacks by foreign powers (Cyber risks, pages 51-6). It also lists State attacks on financial payment systems (pages 58-9) and risks of conflict and instability (pages 179-186). It contains a "range of risks that are representative of the risk landscape," which are evaluated for its "worst plausible manifestation of that particular risk" (page 11).

However, the document does not address risks related to service discontinuation, interference, or attacks that may result from foreign states using legal powers to compel service providers and manufacturers. This is despite such scenarios appearing to meet the threshold for a 'substantial impact' at the national level. The interaction between such risks and those of conflict and instability, including within NATO, is also omitted. Such risks are, we believe, demonstrably 'plausible' and have been raised in the previous Parliament in relation to Huawei.[3] Action was taken regarding the potential for state interference from dependence on Huawei equipment. Similar concerns have been raised regarding Lenovo.[4] Analogous dependencies on companies with similar external legal obligations can reasonably be understood as presenting a clear and acute national-level risk.

It may be argued that the risks of cut offs, sanctions, or repurposing of systems for foreign surveillance are roughly analogous to other threats already in the risk register, particularly the 'cyber attacks' scenarios. While the risk register contains a 'range of risks that are representative of the risk landscape', these acute risks are differently mitigated from general cyber attacks. For example, service discontinuity caused by sanctions can be alleviated

Siân Berry MP
Brighton Pavilion
House of Commons
London SW1A 0AA

through backup systems, but in this case the backup system cannot use (the same) technology from the same nation state as the original supplier.

To manage these risks, France is moving to sovereign open source desktop and collaboration tools for its senior civil service, to reduce risks of surveillance or service discontinuation.[5] The German Bundeswehr is moving to OpenDesk, an open source productivity system developed by the German government to mitigate the risks,[6] while other German emergency authorities are deploying OpenDesk as a backup technology.[7] In contrast, the UK is contracting Palantir to deliver core components of the Ministry of Defence's data systems; the National Risk Register ought to articulate the risks of this approach.[8]

European banks are also taking action to protect themselves against interference from the US by building their own electronic card payments system.[9] Similarly, the UK banking sector is taking action to mitigate against the potential for US interference in the UK card payments system, despite this risk lacking an articulation in the UK Risk Register.[10]

Some of the exacerbating factors for these risks are articulated as a set of 'chronic risks,' such as: "reliance on digital platforms and digital services for services and interactions," "concentration of risk through dominance of global tech," and "impacts from use and capability of artificial intelligence (AI)," which the register explains are dealt with through a separate, confidential process (page 18). A synopsis of the chronic risks is provided but gives little indication of the range of problems and mitigations identified, nor of their likely efficacy.[11]

However, the potential for state interference or threats being made is not in itself a 'chronic' risk, this is a specific and acute risk that could be made real in a range of circumstances that have been made very apparent in recent months.

France, Germany, Denmark and the Netherlands have engaged in national debate about the nature of these risks, believing them to be real, plausible eventualities, and have developed strategies to deploy what they believe are appropriate mitigations.[12] A great deal of evidence and risk assessment has been published.[13] They have digital strategies which identify 'digital sovereignty' as an objective, for security and economic reasons. These strategies go some way to mitigating the risks mentioned above. Indeed, both the French and German sovereign software systems are benefiting the UK tech sector as well as their own, as they involve two UK-based open source software manufacturers, Element.io and Collabora.[14]

The UK public debate on digital sovereignty is significantly hampered by the secrecy surrounding the mitigation strategies for the 'chronic' risks mentioned in the National Risk Register. This contrasts with open discussions and analysis in other European countries. While there may be aspects of the current documents that need to be kept secret, this cannot and must not apply to the whole analysis.

We call on the Government to:

1. Include explicit acute risks of state threats of interference in our digital systems in the National Risk Register.

Siân Berry MP
Brighton Pavilion
House of Commons
London SW1A 0AA

2. Lead a national debate on the nature of our digital dependence, from both a security and economic perspective.
3. Provide Parliament and the public with the analysis made for managing the chronic tech risks outlined in the Risk Register, including for "impacts from reliance on digital platforms and digital services for services and interactions", "concentration of risk through dominance of global tech", "impacts from the use of end-to-end encryption", and "Impacts from use and capability of artificial intelligence."

Yours sincerely,

Siân Berry MP
Victoria Collins MP
Clive Lewis MP
Ben Lake MP

---

[1] For Chinese laws that may constitute a threat of interference, see Article 77, "National Security Law of the People's Republic of China (2015)". China Law Translate; Article 35 "Data Security Law of the People's Republic of China (2021)". China Law Translate. Retrieved 21 January 2026 and Article 7, 14 "National Intelligence Law of the People's Republic of China (2017, as amended 2018)". China Law Translate. Retrieved 21 January 2026; Article 18, "Counter-Terrorism Law of the People's Republic of China (2015, as amended 2018)". China Law Translate. Article 28 and 37, "Cybersecurity Law of the People's Republic of China (2016)". China Law Translate. For US powers of data access, see United States v. Microsoft Corp.; "Understanding the implications and risks of the US Cloud Act". Claromentis. 2023-05-10 and Kunert, Paul (2025-07-25). "Microsoft admits it 'cannot guarantee' data sovereignty". The Register. For US powers of sanction, see Boyle, Andrew (2021). "Checking the President's Sanctions Powers". Brennan Center for Justice. Boyle, Adam; Lau, Tim (2021). "The President's Extraordinary Sanctions Powers". Brennan Center for Justice.

[2] Cabinet Office (2025) National Risk Register 2025

[3] "Huawei and 5G" Hansard. Volume 672: debated on Wednesday 4 March 2020

[4] Dos Santon, Nina; Greenwood, George (March 2024) "Security fears over supercomputer deal with Chinese firm Lenovo". The Times.

[5] "L'espace de travail ouvert et souverain des agents de l'État". Gouv.fr; Vaughan-Williams, S. (January 2026) "Why France just dumped Microsoft Teams and Zoom - and what's replacing them" ZDNet.

[6] Pätsch, S. (April 2025) "BWI/Bundeswehr Chooses Open Source by Adopting openDesk" InteroperableEurope

[7] Krempl, S (January 2026) "Microsoft alternative: Social insurers trial OpenDesk for emergencies". Heise.de

[8] "Ministry of Defence: Palantir Contracts". Hansard Volume 853: debated on Wednesday 11 February 2026.

[9] Tamma, P (February 2026) "Mastercard 'urgently' needed, says banking chief". Financial Times. See also EPI website.

[10] Makortoff, K (February 2026) "UK bank bosses plan to set up Visa and Mastercard alternative amid Trump fears". The Guardian.

[11] Cabinet Office and Government Office for Science (2025) "Chronic risk analysis". Gov.uk

[12] Presse- und Informationsamt der Bundesregierung. (November 2025). "Summit on European Digital Sovereignty Delivers Landmark Commitments for a more competitive and sovereign Europe". Federal Government of Germany (Scholz Government). (August 2022). "Digital Strategy - Creating Digital Values Together". DINUM (2023) "Le numérique au sein de l'État". Gouv.fr Carlberg, A. (January 2026) "Open technologies, public procurement and economic impact: lessons from Denmark for Europe's next digital laws". OpenForum Europe. Ministry of the Interior and Kingdom Relations. (December 2025). Vision on Digital Autonomy and Sovereignty of the Government. Rijksoverheid.

[13] For example, Seifried, M., & Bertschek, I. (ZEW). (2021). *Schwerpunktstudie Digitale Souveränität* [Focus Study on Digital Sovereignty]. Federal Ministry for Economic Affairs and Energy (BMWi). Council for Technological Sovereignty / Federal Ministry of Education and Research (BMBF). (2025). *Impulse Paper: Strategically Securing Technological Sovereignty*, BMBF Ministry of Digital Affairs

Siân Berry MP
Brighton Pavilion
House of Commons
London SW1A 0AA

(Digitaliseringsministeriet), Expert Group on Big Tech (Chaired by Prof. Mikkel Flyverbom). (2024). *The Role of Big Tech as Digital Infrastructure*. Digitaliseringsministeriet;

[14] Element (ND) "LaSuite. The office and collaboration suite for the French public administration" Element.io. Collabora (ND) "OpenDesk". CollaboraOnline