



# CYBERSECURITY BILL

## 6 January Second reading

Contact James Baker [james.baker@openrightsgroup.org](mailto:james.baker@openrightsgroup.org) / 07817 605162

## Raising Digital Sovereignty concerns

The [Cybersecurity and Resilience Bill's second reading](#) is scheduled for 6 January. The Bill aims to make

“provision ... about the security and resilience of network and information systems used or relied on in connection with the carrying on of essential activities.”

The obvious question is: how, in a world of dependence on US big tech vendors, from Amazon, Google and Microsoft, through to Palantir, can the UK government ensure the “security and resilience of essential activities”?

This has been made starkly clear through the switch off of [Microsoft services to the International Criminal Court](#), on the orders of the Trump administration, and is increasingly an active policy concern for European countries, such as Germany, France, Netherlands and Denmark.

Similar concerns were raised by MPs regarding China and Huawei network hardware. Reliance on Chinese tech could have made networks vulnerable to external interference. Risks – whether from Chinese, US or other countries' tech sectors – can and should be managed.

The Cybersecurity Bill therefore offers an opportunity to scrutinise the government's approach to **Digital sovereignty risks**, whether from Chinese technology or dependence on US tech firms, through the second reading debate and amendments. In doing so MPs can seize an opportunity to set a path for growth and innovation in the UK tech sector.

AI exacerbates these risks, as the tech and investment in infrastructure is dominated by US owned tech companies.

## What other governments are doing

In **Germany**, the government has a digital sovereignty strategy, which includes emphasis on chip manufacturing and supply for key industries, emphasis on interoperability, open standards and open source, through initiatives such as the [Centre for Digital Sovereignty \(ZenDiS\)](#), the [Sovereign Tech Agency](#) and the [Federal Agency for Disruptive Innovation \(SPRIND\)](#). Through these, Germany is building the capacity to use and deploy technology it controls, through use of open source tools, often built and maintained in Germany. This includes their approach to AI, and creates opportunities for UK-German collaboration and knowledge transfer.

France has an emphasis on building business capacity in the tech sector, as part of their France 2030 plan, including a great deal of investment which includes open source AI project Mistral.

Both Germany and [France have joined](#) the [Digital Public Goods Alliance](#), which seeks to promote Open Source “Public Goods” globally – increasing digital sovereignty for everyone, by allowing everyone to deploy government digital tech without dependence on tech giants. Governments are sharing digital tools, through projects like [GovStack](#), to ensure they can easily, cheaply, and autonomously, develop secure government tech.

## Missing measures

The Bill should contain measures to ensure that UK essential services are not subject to switch offs or surveillance. We propose:

- A Digital Sovereignty Strategy, to ensure that risks from dependence on hardware, software, or digital services that may be subject to foreign interference are managed and removed or mitigated
- This should require the government to assess risks to national sovereignty through the use of digital technologies and include mitigations in digital procurement and other policies
- Risks include software, hardware and supply chains.
- The strategy should ensure that well known measures such as the use of Open Source software, interoperable systems, are prioritised in the systems the UK uses and maintains, especially for essential services, but also across

government.

- Such a strategy would increase the ability of UK firms to include SMEs to bid for and maintain government systems, expanding opportunities for UK firms, fostering entrepreneurship, stimulating innovation, and deepening the domestic tech sector's capacity

We would be very grateful for support and help raising these issues at Second Reading and in the following stages of the bill.

Published under a Creative Commons Attribution-ShareAlike 4.0 Unported Licence

<https://creativecommons.org/licenses/by-sa/4.0/> except where stated.

Open Rights is a non-profit company limited by Guarantee, registered in England and Wales no. 05581537.