

UK Defence First– Written evidence (NLR0019)

Response to Question 2: National risks with the most severe impact in a reasonable worst-case scenario

UK Defence First welcomes the National Resilience Committee's call for evidence and focuses this submission on the explicit reference to "loss of control of satellite communications" as one of the most severe national risks in a reasonable worst-case scenario. We argue that this risk, already acute, is being materially worsened by proposed international regulatory changes that threaten to erode Britain's ability to maintain reliable, sovereign control over critical satellite infrastructure. In a conflict or major crisis, such loss of control would cascade across defence, critical national infrastructure, cyber security and economic stability, with consequences comparable in severity to a nuclear accident in terms of national paralysis and loss of life.

Satellites are the invisible backbone of modern UK operations. The Ministry of Defence relies on them for command and control, intelligence, surveillance and reconnaissance (ISR), secure communications, navigation and the coordination of joint effects across sea, air, land, space and cyber domains. For critical applications, commercial geostationary-orbit (GSO) networks deliver near-continuous coverage with 99.99 per cent availability - equivalent to roughly 53 minutes of downtime per year - while non-geostationary-orbit (NGSO) constellations provide low-latency connectivity. Maintaining a balanced multi-orbit environment is not optional; it is essential for operational resilience.

Long-standing international rules, overseen by the International Telecommunication Union (ITU), protect this balance through interference protection limits. These limits prevent damaging radio-frequency interference from NGSO systems into GSO networks and have enabled the safe coexistence of more than 11,000 NGSO satellites to date. They

function, in practical terms, like maintaining peripheral vision between satellite systems so that one does not blind the other.

Proposals to weaken or remove these interference protections - advanced primarily by US-based operators such as SpaceX's Starlink (over 10,000 satellites today with around 50,000 planned) and Amazon and Blue Origin (planned 13,000-plus satellites) - would fundamentally alter that equilibrium. In a reasonable worst-case scenario, the changes would permit aggregate interference that degrades GSO availability to well below 90 (or even 80) per cent, introduces outages measured in hours or days annually, and reduces coverage by up to 50 per cent in critical regions such as the Middle East, South America and northern routes. Small user terminals under 45 cm - vital for manpack communications, drone operations and attritable weapons systems - would become unreliable or unusable in contested environments. Even brief interruptions would disrupt real-time decision-making, create gaps in ISR feeds and endanger lives.

The military implications are stark. GSO systems currently support the full spectrum of tactical missions with near-perfect reliability. Increased interference would force reliance on vulnerable NGSO backups that are themselves susceptible to jamming, cyber spoofing and kinetic anti-satellite attacks. In extremis, UK forces could lose effective control of satellite communications at the precise moment it is most needed - during a high-intensity conflict or hybrid operation. This loss of control would not stem solely from adversarial action; it would arise from structural dependence on a handful of foreign commercial providers whose systems dominate orbital spectrum and whose UK presence is minimal. Britain would, in effect, require approval from non-UK entities to conduct military operations, including those linked to the independent nuclear deterrent.

These risks extend directly to national resilience beyond defence. Satellite networks form part of the United Kingdom's digital backbone, supporting emergency services, financial markets, energy infrastructure, aviation and

remote operations. Unstable links blur the boundary between accidental interference and malicious cyber activity, making attribution harder and exploitation easier. Operators would be forced onto less secure backups, increasing exposure to supply-chain compromise and state-sponsored denial-of-service. In a worst-case scenario combining geopolitical tension with regulatory change, the United Kingdom could face simultaneous military blackout and civilian infrastructure failure - a compound shock far exceeding routine outages.

Britain's historical experience underscores the danger of dependence. The United Kingdom was once a pioneer in sovereign space capability: Black Arrow placed Prospero in orbit in 1971, making us the sixth nation to achieve independent launch; Skynet has delivered secure military communications since 1969; and programmes such as Black Knight and Ariel demonstrated technical leadership. Yet successive decisions have left the country without domestic launch capacity and increasingly reliant on foreign providers. The current trajectory risks repeating that error on a far larger scale, ceding control of orbital communications to entities beyond direct British influence.

UK Defence First therefore identifies the potential loss of control of satellite communications as a priority resilience gap that demands immediate attention. The risk is not abstract; preparatory meetings are already under way for the ITU Plenipotentiary Conference in Doha this November and the World Radiocommunication Conference in Shanghai in October 2027, where these types of changes will be debated. Domestic legislation provides a clear opportunity to close the gap. The Cyber Security and Resilience Bill, currently at Committee stage, and the forthcoming Defence Readiness Bill must explicitly treat space assets as critical national infrastructure and require Ofcom - which leads the UK delegation at the ITU - to defend existing satellite interference protections in all international negotiations.

To further mitigate the risk, the Government also should adopt a sovereign British space strategy grounded in national interest. This requires investment in domestic launch sites such as SaxaVord and Sutherland, revival of satellite manufacturing through established firms such as Surrey Satellite Technology, and accelerated development of resilient multi-orbit systems including Skynet 6. Procurement must prioritise UK-based industrial capacity to reduce vendor lock-in, while alliances through AUKUS, Five Eyes and NATO are complemented by the retained ability to act independently. A defence-first approach, with spending rising to at least 5 per cent of GDP, would restore strategic autonomy and deter adversaries who already exploit orbital vulnerabilities.

In summary, loss of control of satellite communications ranks among the highest-impact national risks in a reasonable worst-case scenario. It threatens not only military effectiveness but the broader fabric of UK resilience, including economic stability and public safety. The Committee has a timely opportunity to highlight this gap and urge the Government to oppose regulatory changes at the ITU, align forthcoming legislation with space resilience requirements, and invest decisively in sovereign capability. Failure to act would leave Britain exposed to precisely the strategic vulnerability the inquiry seeks to identify and remedy.

UK Defence First stands ready to provide further oral evidence or technical briefings to the Committee.

9 April 2026