Media and communications
Sector terrorism threat assessment

Terrorism threat
Threat visualistion

Data Centres

POOL Re SOLUTIONS

Terrorism threat
Threat visualisation

Terrorism Threat to Data Centres

- There is a realistic possibility that terrorist actors could have the intent to conduct attacks against data centres in the UK due to their role as Critical National Infrastructure (CNI) and the potential to cause significant disruption through any such attack.[1]

- It is highly likely that any terrorist attack conducted against a data centre at this time would be conducted by an individual or small cell using a low sophistication methodology. E.g., Fire as a Weapon, Vehicle as a Weapon.

- There is a realistic possibility that terrorist actors in the UK could have the capability to conduct a high sophistication attack against a data centre in the UK. E.g., Improvised Explosive Devices (IED), Firearms, etc. The complicated nature of plotting a high sophistication terrorist attack makes it highly likely that there would be greater opportunity for UK police and security services to disrupt potential attacks.

- It is almost certain that any attack conducted against a data centre in the UK would prioritise disruption and/or damage to site infrastructure, rather than targeting individuals present at the site.

- The assessments in this report were made using the PHIA Probability Yardstick, for further information please see the Assessment Methodology section below.

Previous terrorist incidents related to data centres in the UK

- Terrorist actors have previously demonstrated the intent and capability to conduct attacks against data centres and related infrastructure in the UK, including:
  - **2007 UK:** Reporting suggests that an al-Qa'ida affiliated cell plotted to conduct an attack against the Telehouse Europe facility in London. The individuals allegedly "appeared to be planning to infiltrate the "hub", possibly to blow it up from the inside". The exact nature of the plot remains unclear.[2]
- Terrorist actors have previously demonstrated the intent and capability to conduct attacks against data centres and related infrastructure globally, including:
  - **2025 USA:** On 20 February 2025, Ethan Early, 25, was reportedly charged with an act of terrorism after he allegedly threatened to burn down a data centre in Memphis, USA. The data centre reportedly belonged to an AI startup founded by Elon Musk. The motivation behind the alleged plot remains unclear at this time.[3]
  - **2025 USA:** On 08 August 2025, Brandon Russell, 30, was sentenced to 20 years in prison for conspiring to conduct an attack against Maryland's power grid. Russell reportedly intended to organise "sniper attacks" against electrical substations. At trial, it was alleged that the planned attacks could have caused approximately $70m in damage. Russell was inspired by an Extreme Right-Wing ideology.[4]
  - **2021 USA:** On 01 October 2021, Seth Aaron Pendley, 28, was sentenced to 10 years in prison after he plotted to conduct an Improvised Explosive Device (IED) against an Amazon Web Services data centre in Ashburn, Virginia, USA. Pendley was arrested in April 2021 after allegedly attempting to obtain an IED from an undercover FBI officer and plotting to "kill off about 70% of the Internet".[5]
  - **2013 USA:** On 16 April 2013, reporting suggests that multiple snipers fired for approximately 20 minutes at an electrical substation in San Jose, California, USA. The perpetrators reportedly escaped undetected and disabled 17 transformers that carried power to Silicon Valley.[6]

Other potential threats to data centres in the UK

- It is likely that any terrorist attack conducted against a data centre in the UK would be conducted by an individual adhering to an Extreme Right-Wing or Left-Wing, Anarchist, or Single Issue (LASIT) terrorist ideology due to the ideologically driven intent to cause significant disruption to infrastructure in pursuit of their ideological goals.

- It is unlikely that Islamist terrorists would currently have the intent to target data centres in the UK due to the ideologically driven intent to conduct mass casualty attacks against members of the public, rather than infrastructure.

- It is likely that individuals adhering to an accelerationist ideology would pose an emerging threat to data centres in the UK. Accelerationism advocates for political violence and terrorism to physically destroy society as it currently exists. Targeting CNI is seen as a means through which the collapse of society can be achieved.[7]

- Although it is highly unlikely that any such event would be designated as terrorism, it is highly likely that any successful attempt to significantly disrupt a data centre in the UK through cyber means would require a high level of sophistication and therefore be conducted by a state actor or state-enabled third party.

- It is highly likely that any state supported or sanctioned cyber attack conducted against a data centre in the UK would target infrastructure and business continuity, rather than members of the public and/or human lives.

- Although it is highly unlikely that any such event would be designated as terrorism, there is a realistic possibility that Non-Violent Direct Action (NVDA) activist groups could have the intent to stage protest activity at data centres in the UK as a result of their effect on the environment. E.g., In 2023, activists from the Campaign to Protect Rural England (CPRE) opposed the building of a 12-building data centre campus.[8]

Continued

- There is a realistic possibility that staff employed at UK data centres could pose an Insider Threat in several ways, including:
  - Staff employed at data centres could allow individuals with terrorist intent to gain access to high-security data centre sites.
  - Staff employed at co-located data centres could exploit access to a shared facility to access and/or damage another organisations' data.
  - Staff employed at data centres could be an attractive option for hostile actors seeking to gain access to data centres and the data they hold.[9]
- For further information on the threat posed to Data Centres in the UK, visit the National Protective Security Authority's (NPSA) Data Centre Security guidance here: Data Centre Security: System & Information Security, NPSA

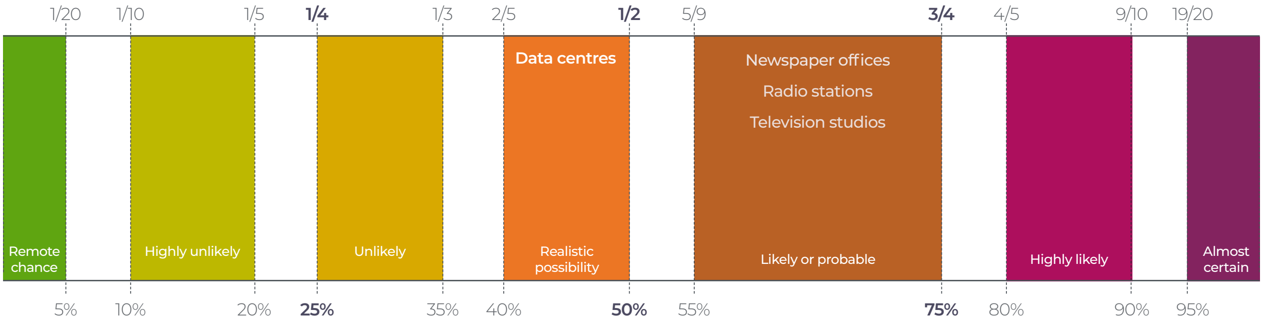
Threat visualisation

The diagram below outlines the intent of terrorist actors in the UK to conduct attacks against newspaper offices within the media and communications sector.

Terrorist intent can be defined as the desire and/or determination of an individual to conduct an attack against any given site.

The intent of terrorist actors to conduct an attack against the media and communications sector in the UK is subject to change based on the assessments outlined in this report.

Note: The terrorism threat to any given site is not based solely on intent, but also the capability of terrorist actors in the UK as outlined in this report. Terrorism threat is also mitigated by the UK's countrywide terrorism risk mitigation infrastructure including both public and private security and safety capabilities.



Assessment Methodology

The assessments made in this report have been made using the Professional Head of Intelligence's "Probability Yardstick" (above). The Probability Yardstick is a standardised instrument used to provide a professional standard for intelligence assessment.

- **Almost certain:** An event has a greater than 90% chance of occurring.
- **Highly likely:** An event has a 76% to 90% chance of occurring.
- **Likely:** An event has a 55% to 75% chance of occurring.
- **Realistic possibility:** An event has a 40% to 54% chance of occurring.
- **Unlikely:** An event has a 25% to 39% chance of occurring.
- **Highly unlikely:** An event has an 10% to 24% chance of occurring.
- **Remote chance:** An event has a less than 10% chance of occurring.

Time spans

- **Short Term:** 0 – 6 Months.
- **In the next 12 months.**
- **Medium Term:** 12 months – 5 Years.
- **Long Term:** 5+ Years.

Continued

Intelligence cut-off date: 26 January 2026

For more information please contact solutions@poolre.co.uk

Bibliography

1. Data Centres are defined within this report as physical locations that store computing machines and their related hardware equipment. Data housed in UK Data Centres can range from photos taken on smartphone to patients' NHS records and sensitive financial investment information
   Data centres to be given massive boost and protections from cyber criminals and IT blackouts - GOV.UK (www.gov.uk)
   Data centres as vital as NHS and power grid, government says - BBC News
2. Al Qaeda plot to bring down UK internet (thetimes.com)
   Did Terrorists Target UK Data Center?: Data Center Knowledge, News and analysis for the data center industry
3. Man who threatened to burn down xAI's Memphis data center charged with terrorism - DCD
4. Office of Public Affairs: Maryland Woman and Florida Man Charged Federally for Conspiring to Destroy Energy Facilities, United States Department of Justice
   Neo-Nazi leader sentenced to 20 years for plot to attack Maryland's power grid: US news, The Guardian
5. Right wing terrorist gets 10 years for plotting to blow up AWS data center - DCD (datacenterdynamics.com)
   Foiled Plot to Attack Amazon Reflects Changing Nature of Data Center Threats, Data Center Frontier
6. Sniper Attack On Calif. Power Station Raises Terrorism Fears : The Two-Way, NPR
7. The Targeting of Infrastructure by America's Violent Far-Right – Combating Terrorism Center at West Point
8. Data centre protests are on the rise, but are they effective? (techerati.com)
   Not just nimbys – why data centre protests are on the rise: Raconteur
   Big Tech's New Headache: Data Centre Activism Flourishes Across the World, Media@LSE
9. People risks for users: NPSA

Pool Re Solutions Limited
Equitable House 47 King William Street London EC4R 9AF

poolre.co.uk

Disclaimer

The contents of this document including any opinions are for information purposes only and for your own use. None of the contents should be construed as the provision of advice.

Although Pool Re Solutions Limited (**"PReS"**), its group companies, agents and staff (together the **PReS Entities**) have taken reasonable care that the information contained in this document is accurate at the time of this document, no representation or warranty (including liability towards third parties), expressed or implied, is made (or accepted) as to its accuracy or completeness or fitness for any purpose by the PReS Entities. The PReS Entities have no obligation to update the information contained in this document or notify you of any such updates or provide any additional information which may be relevant to the information contained in this document. Under no circumstances will the PReS Entities be liable for any direct, indirect, incidental, special or consequential loss or damage caused by reliance on or use of this information.

The terms and conditions of this legal notice shall be governed by and construed in accordance with the laws of England and Wales.