Hypothetical scenario for planning purposes. Not a forecast.

When Networks Are Under Strain

A hypothetical scenario of escalating hybrid threats for UK resilience planning, from grey-zone pressure to conflict, and how offline preparedness information helps households and communities



Illustration: AI-generated, fictional. *An ordinary terraced street during a prolonged power cut.*

Published by: Preptorum Ltd, company no. 16410799, 68 Frognal, London NW3 6XD

Date: 15 October 2026

Status: Hypothetical scenario for planning purposes. Not a forecast. It is not an official assessment.

Independence: Preptorum Ltd is an independent company. It is not affiliated with, or endorsed by, any government department, LRF or council. Its drives are built from published GOV.UK, NHS and LRF guidance.

Executive summary

This paper sets out a hypothetical, day-by-day scenario in which hybrid pressure on the UK from Russia escalates over about a month, through serious disruption to infrastructure, into armed conflict. It is a planning tool, not a forecast, and escalation at any stage is not inevitable. It is anchored in what has been reported publicly as of 15 October 2026, and it looks at how offline preparedness information can help households and communities at each stage.

What is real now (sourced)

- **Hybrid activity is ongoing.** MI5's Director General said on 13 October 2026 that Russia remains "aggressor number one" and is escalating hybrid warfare while staying below the NATO Article 5 threshold. [1]
- **Sabotage, drones and cable damage.** Germany formally attributed the August 2026 explosive-drone attack at Leipzig/Halle Airport to Russia. Drone incidents at or near MoD sites rose to 340 in the year to August 2026. Baltic cable cases (Eagle S, Fitburg) are now in the Finnish courts. GNSS spoofing reaches deep into Europe. [2–6]
- **Data centres have been struck.** Between 7 and 12 October 2026, Ukrainian drones hit three Yandex data centres in Russia. Two shut down, and cloud, email, payments, taxis, smart-home devices and third-party services were disrupted. A strike on a Sberbank data centre followed on 14 October. Sber said its services were normal, but outage monitors recorded a surge in user complaints. [7–10]
- **Single points of failure.** Real outages show how fast everyday life degrades when one node fails: the Iberian blackout (April 2025), the Heathrow substation fire (March 2025) and CrowdStrike (July 2024). [11–14]

What the scenario shows

Under stress, the online channels people now rely on for official advice tend to be affected early: websites, apps, mobile data and digital landlines, which need mains power after the PSTN switch-off (deadline 31 January 2027). [18] The UK Government Resilience Action Plan and the 2025 Strategic Defence Review both call for a "whole-of-society" approach and a better-prepared public. [15–16] The shared concern is simple. If guidance lives mainly online, it can be hardest to reach at the moment it is most needed.

How offline information helps

- **Saved guidance:** Published GOV.UK, NHS and LRF guidance can be saved in advance and read on a charged laptop or device with no network connection.
- **Offline search:** A search tool that runs on the device helps people find the relevant published guidance when there is no signal. People then act on that guidance themselves.
- **Kept current:** Saved guidance can refresh whenever a connection returns, so it stays current until networks drop. It can be refreshed again through community hubs.
- **Where it is held:** Households; community hubs in libraries, schools, village halls and care homes; in English, Welsh and Gaelic.

When preparation matters most

Preparation is easiest before disruption, in the early phases of the scenario (Days 0–10), while networks are healthy. Once disruption starts (Day 11 onwards), what people already have at home or at their local hub is what they can use, and hubs can help keep it current.

1. Purpose, scope and caveats

- **Hypothetical.** Everything in Sections 4–5 is invented to support planning discussions. It is not a prediction, an intelligence assessment or a statement of UK Government views.
- **Sourced context.** Section 2 uses only publicly reported facts, cited in the Sources list. Where attribution is not formal or a case is still before the courts, Section 2 says so.
- **No operational detail.** Infrastructure is described only by the broad public categories already discussed in open sources (for example "undersea cables" or "data centres"). There are deliberately no site names, locations, vulnerabilities or methods.
- **Fiction is labelled.** Characters in the vignettes are fictional. Illustrations are AI-generated and show no real place or person.
- **About the guidance.** Preptorum drives are built from published GOV.UK, NHS and LRF guidance. Preptorum Ltd is not affiliated with, or endorsed by, any government body. The offline search helps people find published guidance; it does not give medical advice. Nothing in this scenario depends on phone helplines being reachable.

2. Where we are now: the real-world context (October 2026)

2.1 Russia's hybrid campaign against Europe and the UK

- **UK threat level.** On 13 October 2026, MI5 Director General Sir Ken McCallum said Russia is "aggressor number one" and that Russian military and intelligence services are "once again escalating their attempts at hybrid warfare", staying below the NATO Article 5 threshold. He cited a cyber-attack on Polish energy infrastructure and the Leipzig drone plot. He urged critical-infrastructure operators to act "the day before, not the morning after". [1]
- **Sabotage in the UK.** A Swindon man was charged in September 2026 under the National Security Act, allegedly for researching drone factories for sabotage on behalf of a person linked to the GRU Volunteer Corps. This is a charge, not a conviction. [2] The GRU Volunteer Corps was designated in July 2026 under the new National Security (State Threats) Act 2026. The Home Office factsheet says new powers were needed "to keep pace with the evolving threat landscape". [17]
- **Drones over UK defence sites.** The MoD recorded 340 drone incidents at or near defence sites in the year to August 2026, up from 250 in 2025 and 126 in 2024 (FOI data reported by The Independent). [3]
- **Drones over European airports.** On 1 September 2026, Germany said Russia was responsible for the 4–5 August explosive-drone attack at Leipzig/Halle Airport and closed a Russian consulate in response. [4] In September 2025, Copenhagen and Oslo airports closed for hours after drone sightings, and Poland shot down Russian drones that entered its airspace. [19, 20]
- **Cyber-attacks on energy.** In late December 2025, a destructive cyber-attack hit Polish renewable generation and a combined heat and power plant serving nearly 500,000 customers. A blackout was averted. The UK and EU formally attributed the attack to Russia's FSB in July 2026. [21, 22]
- **Councils and public services.** Pro-Russian hacktivists (NoName057(16)) have repeatedly knocked UK council websites offline with DDoS attacks. In January 2026 the NCSC warned that Russian-aligned groups continue to target UK local government and critical infrastructure. [23, 24]
- **Undersea cables.** Finland's Court of Appeal revived the Eagle S prosecution (Christmas Day 2024, Estlink 2 power cable plus four telecom cables) on 27 August 2026. The Fitburg trial over damage to Finland–Estonia cables on 31 December 2025 opened in September 2026. Both cases are still before the courts. [5, 25] NATO launched Baltic Sentry in January 2025. [26]
- **GNSS jamming and spoofing.** Lithuania reported in May 2026 that Russia can falsify GPS signals deep into Europe, with Kaliningrad-based spoofing infrastructure greatly expanded. [6]

2.2 Strikes on Russian data centres (October 2026) and their reported effects

These strikes have been reported by multiple outlets, including BBC, AP, Reuters, POLITICO and The Record:

- **7–8 October:** Drones hit a Yandex data centre in Sasovo (Ryazan region) overnight on 7–8 October 2026, starting a fire and forcing a full shutdown. [8]
- **9 October:** A second Yandex data centre in Kaluga was hit on 9 October, damaging part of its infrastructure. [8]
- **11–12 October:** A third, in Vladimir, was hit overnight on 11–12 October. Yandex said: "The data center has shut down completely, and the remaining infrastructure is unstable. The platform is operating in emergency mode." Together the three sites have about 115 MW of capacity. [7, 8]
- **14 October:** Drones hit Sberbank's data centre at Balakovo (Saratov region). Sber said "all Sberbank systems and services are operating normally", but Russian outage-monitoring services reported a surge in user complaints about the app. [9, 10]

Impact as reported:

- **Services:** Yandex Cloud (about 64,000 customers in mid-2026) was disrupted, along with email, taxis, food delivery, Yandex Pay, the Alice assistant and smart-home devices. More than a dozen third-party services hosted on Yandex were also hit, including retailers, internet providers and the Russian segment of TikTok. [8]
- **Resilience:** Yandex told cloud customers to make alternative recovery plans rather than rely on failover inside its own infrastructure. It moved to share load with rival providers and changed its terms to exclude liability for drone-strike outages. It said it was "very difficult to provide a timeline for restoring the equipment". [8]
- **Government response:** Russia's digital minister said his ministry was working with the Defence Ministry on protecting the facilities. [8] President Zelensky described the strikes as retaliation for Russian attacks on Ukrainian data centres. Those attacks damaged at least six facilities in late September and cut fixed-line internet for about 100,000 Kyiv-area households on 23 September. [8]

Why this matters for UK planning (analysis, not a sourced claim)

Data centres and telecoms have now been struck by both sides in the Russia–Ukraine war. When several sites are affected within days, services hosted in the same place can fail together: payments, apps, smart devices, digital-only public services and the websites people would go to for guidance.

Even redundant cloud designs struggled, and organisations were told to plan for recovery outside the provider.

For households, the practical point is that "it's on the website" is not on its own a resilience plan. A local, offline copy of published guidance is a simple, low-tech complement.

2.3 Closest UK and European examples of systemic failure (non-hostile)

- **Iberian blackout, 28 April 2025.** The Iberian blackout of 28 April 2025 took down the whole Spanish and Portuguese grid in seconds through an overvoltage cascade. ENTSO-E's final report (March 2026) found no single cause. [11, 12] It is a reminder that grids can fail at national scale without any attack.
- **Heathrow substation fire, March 2025.** A fire at a single substation closed Heathrow for most of a day. NESO's review found that reconfiguring the airport's internal network took 10–12 hours. [13]
- **CrowdStrike, 19 July 2024.** A faulty update crashed about 8.5 million Windows devices. In England, GP practices lost access to records and appointment systems and had to switch to paper. [14]

2.4 UK official framing

- **National Risk Register 2025.** A public, dynamically updated register of the most serious acute risks. It includes cyber-attacks on critical national infrastructure and national power failure. [27]
- **UK Government Resilience Action Plan.** Published 8 July 2025. Its priorities are to assess UK resilience continuously, help individuals, businesses and communities prepare, and strengthen the public sector. It points the public to GOV.UK/Prepare and sets up a Cabinet Office-led Home Defence Programme. [15]

- **Strategic Defence Review 2025.** Published 2 June 2025. It calls for a whole-of-society approach to homeland defence and resilience. [16]
- **Emergency Alerts.** The second national test went to compatible phones on 7 September 2025. [28] It depends on mobile networks being up.
- **PSTN switch-off.** Landlines move to digital by 31 January 2027. Digital landlines do not work in a power cut unless there is battery backup (at least one hour for those who rely on them). [18]

Taken together: a growing share of trusted guidance now reaches the public through channels that depend on power and connectivity. Government has recognised this in its resilience planning. Offline preparedness information is meant to complement that work, not replace it.

3. Infrastructure categories in open-source discussion (public-level view)

These are the categories public reporting and official documents already discuss. They are listed only to help plan public impacts. No specific sites, weaknesses or methods are described.

Category	Public-level description and impact
Undersea cables and interconnectors	International data and power links (Baltic precedent). Impacts: slower internet, price spikes, reduced import capacity.
Electricity grid and substations	Regional or national outages (Iberian and Heathrow examples). Impacts on everything downstream.
Data centres and cloud regions	Concentrated digital services (Yandex precedent). Impacts: payments, apps, public-service websites.
GNSS (GPS) timing and navigation	Jamming and spoofing (Baltic precedent). Impacts: navigation, logistics, systems that depend on timing.
Telecoms and mobile networks	Mast power, core networks, DDoS. Impacts: loss of signal, data, digital landlines and alerts.
Water and wastewater control systems	Industrial control systems (the Polish energy incident shows the operational-technology risk). Impacts: boil-water notices, pressure loss.
Transport and airports	Drone disruption (Copenhagen and Leipzig precedents). Impacts: closures, stranded travellers, supply delays.
Councils and NHS IT	DDoS and ransomware (UK council precedents, CrowdStrike example). Impacts: paper fallback, delays.
Media and information space	Disinformation, fake “official” messages, spoofed alerts. Impacts: confusion, panic buying, mistrust.

4. The hypothetical scenario: Day 0 to Day 30+

Before reading

This scenario is fictional and simplified. Timings are compressed so that each stage can be discussed. Real crises are messier, slower or faster, and may stop at any phase. Diplomacy, deterrence and allied action could halt escalation at any point. All characters are invented.

Phase 0: Normal (Day 0)

Today looks much like October 2026. The background is a persistent hybrid campaign, with drone sightings near bases, occasional council website outages, cable court cases in the Baltic and periodic warnings from security services. Most people are aware of it but not worried. Guidance on preparing for emergencies is online at GOV.UK/Prepare and on local LRF and council websites.

Vignette (fictional): *In a valley town in South Wales, the Morgans (two parents, two children and a grandmother nearby) have a torch in a drawer and plenty of phone chargers. Their landline went digital last spring. Like most families, if they ever needed to know what to do, they would "just look it up".*

What fails	Nothing yet. Underlying dependencies: guidance is mostly online, landlines are digital, and most payments are by card.
What the public sees	Normal life. Low awareness of household preparedness.
What officials need	Exercises, community risk registers, public-preparedness messaging (Resilience Action Plan).
How offline information helps	Preparing ahead is easiest now. Households, libraries, schools, village halls and care homes can keep published GOV.UK, NHS and LRF guidance saved offline, and exercises can test what still works with no connection.

Phase 1: Grey-zone provocation (Days 1–5)

- **Day 1.** A significant diplomatic incident between the UK and Russia (fictional) leads to expulsions and sharper rhetoric.
- **Days 2–3.** Several European airports pause flights over drone sightings. Similar incidents near UK defence sites make the news, matching the 2025–26 pattern.
- **Day 4.** A coordinated wave of DDoS attacks briefly takes down several council and transport websites. Fake screenshots of "official" evacuation notices spread on social media.
- **Day 5.** GNSS interference reports increase around the North Sea. Shipping and aviation adopt fallback procedures.

What fails	Individual websites, briefly. Navigation accuracy in some areas.
What the public sees	Inconvenience, some worrying headlines, fake messages circulating.
What officials need	Clear, trusted messaging. Rebuttal of fake notices. Confirmation that business-continuity plans are current.
How offline information helps	Saved guidance keeps refreshing while networks are up. Where published, guidance on how to check official messages lets people test a viral claim against a dated copy of what was actually published.

Phase 2: Escalating hybrid attacks (Days 6–10)

- **Day 6.** Damage to an undersea data cable and, separately, a power interconnector is reported in northern European waters. Investigations begin. Internet traffic reroutes and is slower at peak times. Wholesale power prices jump.
- **Day 7.** Arson at a logistics depot linked to defence supply. Police treat it as possible state-linked sabotage, as with recent UK cases.
- **Day 8.** Ransomware hits a regional NHS IT supplier. Some appointments revert to paper, as during CrowdStrike in 2024.

- **Days 9–10.** Officials warn that further disruption to critical infrastructure is possible and remind the public of preparedness advice. Shops see early panic buying of bottled water, batteries and camping stoves.



Illustration: AI-generated, fictional. *A council emergency planning officer keeping paper logs during a systems outage.*

Vignette (fictional): *Priya, an emergency planning officer at a fictional district council, spends Day 9 printing contact lists and running the council's paper fallback log. Her concern is the public, not her team: "If the website's down and the phones are jammed, how do people get the advice we've already written?" In the store cupboard is a box of offline guidance drives held for the LRF's rest centres. She sets them to update overnight.*

What fails	Some international bandwidth. Parts of NHS administration. Supply chains for some goods.
What the public sees	Slower internet, rising prices, cancelled appointments, empty shelves for some items, growing anxiety.
What officials need	Get preparedness advice to the public before networks are stressed. Brief community partners. Pre-position resources in rest centres and hubs.
How offline information helps	While networks are still healthy, hubs, care homes, schools and libraries can check that saved guidance is in place and current. Simple "how to use it offline" instructions help, in Welsh and Gaelic where needed.

Phase 3: Systemic disruption (Days 11–18)

- **Day 11.** A cyber-physical incident (fictional) causes rolling regional power cuts across parts of England and Wales. Restoration takes hours in some areas and days in others.
- **Days 11–12.** Mobile masts run down their backup batteries. Mobile data, then voice, becomes patchy. Digital landlines go silent once their own backup runs out. Emergency Alerts reach only phones still on a working network.
- **Day 12.** Card payments fail where terminals or networks are down. Cash runs short. Fuel forecourts close or ration because pumps and payment need power.
- **Day 13.** A major cloud region used by many UK businesses and some public services suffers prolonged disruption. Public-service websites are unreachable or very slow in affected areas.
- **Days 14–15.** Some water companies issue precautionary boil-water notices or pressure warnings in affected areas, delivered by leaflet and loudhailer where digital channels are down.

- **Days 16–18.** Fake "government" messages spread on whatever channels still work, giving wrong locations for help points and false advice about water.



Illustration: AI-generated, fictional. *A family checking saved guidance on a laptop by lantern light during a power cut.*

Vignette (fictional): *Day 12, 9 p.m. The Morgans have had no power since early afternoon, and their phones show "No Service". The grandmother's care line is silent. Their son plugs the family's drive into the laptop, which has a two-thirds charge. They search the offline guidance for "boil water notice what to do". It brings up the published guidance, and they follow the steps: fill containers, how long to boil, who to check on. They walk next door to check on their elderly neighbour and give her the printed checklist from the drive.*

What fails	Power (regional), mobile data and voice, digital landlines, card payments, fuel distribution, some cloud-hosted public services, water in places.
What the public sees	Darkness, no signal, cash-only or no payments, queues, worry about water and medicines, rumours.
What officials need	Keep official guidance reachable without networks. Run rest centres and community hubs. Counter disinformation. Avoid overwhelming responders.
How offline information helps	Published guidance stays readable with no signal, and an offline search tool finds the right page. Hubs can act as information points, and a dated copy of published guidance helps people check rumours. Devices need charge, so power banks or small generators at hubs matter.

Phase 4: Mobilisation and rising tension (Days 19–24)

- **Day 19.** After further attributed attacks on allies, NATO raises readiness. UK reservists are called up (fictional).
- **Days 20–21.** Government sets out civil-protection arrangements and updates public guidance. Networks are partly restored, so saved guidance can be refreshed.
- **Day 22.** Local authorities and LRFs open more community hubs and rest centres. Schools and libraries become information points.
- **Days 23–24.** Air travel is curtailed. Some transport is prioritised for military movement. Shortages persist.



Illustration: AI-generated, fictional. *A village hall community hub run by volunteers, lit by battery lanterns.*

Vignette (fictional): *Gareth, the (fictional) chair of a Local Resilience Forum, chairs a call on Day 20 while power is back. His priority list: refresh the guidance on every drive held in hubs while the network is up; get drives into the remaining care homes; brief hub volunteers on how to help people search offline. "Assume we lose comms again tomorrow," he says. "What do people have in their hands when we do?"*

What fails	Networks are intermittent rather than down. Supply chains are strained. Public anxiety is high.
What the public sees	Partial normality with visible military activity. Uncertainty, and a hunger for trusted information.
What officials need	Mass distribution of current guidance. Prepared hubs. Coordination with the voluntary sector. Calm, consistent messaging.
How offline information helps	When networks are partly restored, saved guidance picks up the latest published advice. Hub volunteers can be shown how to help people search offline.

Phase 5: Outbreak of hostilities (Days 25–28)

- **Day 25.** Armed conflict begins between NATO and Russia (fictional). Strikes and cyber-attacks affect infrastructure categories such as energy, telecoms, data centres and transport.
- **Days 25–26.** Longer outages of power and communications in affected regions. Many online services are unavailable.
- **Days 26–28.** Civil-protection guidance (sheltering, water, heat and light, looking after vulnerable people) becomes the most-needed information. It is also the hardest to reach.

What fails	Large-scale power and telecoms failure in places. Internet broadly degraded. Emergency services stretched and phone lines congested or unavailable.
What the public sees	Fear, isolation, need for practical instructions, concern for vulnerable relatives.
What officials need	Keep people informed and acting sensibly without networks. Reduce avoidable demand on responders. Maintain trust.
How offline information helps	Homes and hubs keep a readable, searchable copy of published guidance. People look it up and act for themselves, and hub volunteers can answer common questions from it.

Phase 6: Sustained conflict (Day 29 and beyond)

- **Days 29–30+.** Intermittent restoration and repeated disruption. Communities organise around hubs. Guidance is revised as the situation evolves.

What fails	Recurring and unpredictable failures. Supply rationing.
What the public sees	Fatigue, adapting to routines, reliance on local networks of neighbours and hubs.
What officials need	A way to refresh guidance across the country despite unreliable networks. Countering disinformation. Supporting volunteers.
How offline information helps	Updated copies can reach hubs by local transport and be shared with residents, and saved guidance refreshes whenever any link returns. Dated, versioned copies help people tell current guidance from old or fake messages.

5. Timeline: from normal to sustained disruption (hypothetical)

When	Phase	Events (hypothetical)	Public impacts	How offline information helps
Day 0	**Normal**	Background hybrid activity; guidance mostly online	None visible; latent dependencies	Guidance saved offline in homes and hubs; offline exercises
Days 1–5	**Grey-zone provocation**	Diplomatic incident; drone sightings; DDoS on councils; fake notices; GNSS interference	Brief website outages; rumours	Refresh while networks are up; dated copy to check fake notices against
Days 6–10	**Escalating hybrid**	Cable/interconnector damage; arson; NHS supplier ransomware; warnings; panic buying	Slower internet, prices up, paper fallback, shortages	Hubs, schools, care homes and libraries check saved guidance is current
Days 11–18	**Systemic disruption**	Regional power cuts; masts fail; payments and fuel disrupted; cloud outage; water notices; disinformation	No power/signal; cash-only; queues; boil-water; confusion	Offline guidance and search; hubs as information points; power banks at hubs
Days 19–24	**Mobilisation, rising tension**	Raised readiness; reservists; civil-protection guidance; more hubs; travel curtailed	Intermittent networks; high anxiety	Refresh saved guidance while networks are up; brief hub volunteers
Days 25–28	**Outbreak of hostilities**	Strikes and cyber-attacks on infrastructure categories; long outages	Widespread loss of services; responders stretched	Saved guidance in homes and hubs; volunteers answer common questions
Days 29–30+	**Sustained conflict**	Cycles of restoration and disruption; revised guidance	Fatigue; local self-reliance	Updated copies via hubs and local transport; dated, versioned guidance

Colour band runs from green (normal) to red (sustained conflict). All events in this table are fictional.

6. How offline preparedness information helps at each stage

Government, LRFs, councils, emergency services, broadcasters and the voluntary sector lead the response. Offline preparedness information is a modest, complementary layer. It holds content government and partners have already published, alongside Emergency Alerts, broadcast and leaflets, and helps people find it when web and mobile channels are degraded. People then decide and act for themselves.

Before disruption

- **Guidance in place early.** Community hubs, rest centres, libraries, schools, care homes, GP surgeries, village halls and households can keep published guidance saved offline, refreshed whenever they reconnect.
- **Refreshing while networks work.** While networks are healthy, newly published guidance reaches every connected copy, so the latest version is already in people's hands before any disruption.
- **Practising without networks.** Exercises can include an "offline phase", testing whether responders and volunteers can find and use published guidance with no connectivity.
- **Language.** Welsh and Gaelic editions support bilingual communities in Wales and the Highlands and Islands.

During disruption

- **Guidance without networks.** Homes and hubs keep a readable, searchable library of published GOV.UK, NHS and LRF guidance, plus general offline reference. It works for as long as a device can be charged.
- **Hubs as information points.** Volunteers can answer common questions such as water safety, keeping warm, food storage and looking after vulnerable people. The offline search helps them find the relevant published page quickly.
- **Less avoidable demand.** Routine questions answered from saved guidance can mean fewer calls to stretched services, and people can find published guidance without needing a phone line.
- **A steady reference.** Dated, versioned copies of guidance as published let hubs and households check a viral "official" message against what was actually published.

Over a longer period

- **Refreshing through hubs.** When guidance changes, updated copies can be taken to hubs by local transport. A hub with an intermittent link can refresh its own copies and then residents' copies locally.

About Preptorum

Preptorum Ltd makes offline drives built from published GOV.UK, NHS and LRF guidance, with an on-device search tool (GPT4All) and offline general reference material, in English, Welsh and Gaelic. Drives refresh when they reconnect. Preptorum Ltd is independent and is not affiliated with, or endorsed by, any government department, LRF or council. The search tool helps people find published guidance; it does not give medical advice.

Sources

[1] MI5, "MI5 Director General Delivers Annual Threat Update", 13 Oct 2026. https://www.mi5.gov.uk/mi5-director-general-delivers-annual-threat-update

[2] BBC News, "Man 'planned to torch drone factory in Russian sabotage plot', court told", 2026. https://www.bbc.co.uk/news/articles/c74e0ml3y8go

[3] The Independent, "Drones targeting UK military sites nearly every day…", 2026. https://www.independent.co.uk/news/uk/home-news/drones-uk-military-bases-russia-putin-iran-b3051804.html

[4] Reuters, "Germany says Russia responsible for drone attack at Leipzig airport", 1 Sep 2026. https://www.reuters.com/world/europe/germany-says-russia-responsible-drone-attack-leipzig-airport-2026-09-01/

[5] eBuilder Security, "Finnish Appeals Court Revives Eagle S Prosecution…", Aug 2026. https://ebuildersecurity.se/en/cyber-news/finland-appeals-court-eagle-s-baltic-cable-jurisdiction/

[6] Reuters, "Russia can falsify GPS signals deep into Europe, Lithuania says", 26 May 2026. https://www.reuters.com/business/aerospace-defense/russia-can-falsify-gps-signals-deep-into-europe-lithuania-says-2026-05-26/

[7] BBC News, "Yandex: Ukraine strikes data centre in third attack on Russian tech giant", Oct 2026. https://www.bbc.com/news/articles/cw0k0g57mk3zo

[8] The Record (Recorded Future News), "Ukraine strikes third Yandex data center…", 12 Oct 2026. https://therecord.media/ukraine-strikes-third-yandex-data-center

[9] POLITICO, "Ukrainian drones strike data center of Russia's biggest bank", 14 Oct 2026. https://www.politico.com/news/2026/10/14/ukrainian-drones-struck-russian-sberbank-data-center

[10] Reuters via Devdiscourse, "Ukrainian drones hit Russia's biggest data centre", 14 Oct 2026. https://www.devdiscourse.com/article/international/3992081-ukrainian-drones-hit-russias-biggest-data-centre

[11] ENTSO-E, "28 April 2025 Blackout" (incl. Final Report, 20 Mar 2026). https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/

[12] ENTSO-E news, "Expert Panel Final Report on 28 April 2025 Blackout", 20 Mar 2026. https://www.entsoe.eu/news/2026/03/20/entso-e-publishes-expert-panel-final-report-on-28-april-2025-blackout-in-spain-and-portugal/

[13] NESO, "Final report from the review into the North Hyde Substation outage". https://www.neso.energy/news/final-report-review-north-hyde-substation-outage

[14] BBC News, "CrowdStrike IT outage affected 8.5 million Windows devices"; Guardian on GP impact, 19 Jul 2024. https://www.bbc.com/news/articles/cpe3zgznwjno

[15] Cabinet Office, "UK Government Resilience Action Plan", 8 Jul 2025. https://www.gov.uk/government/publications/uk-government-resilience-action-plan/uk-government-resilience-action-plan-html

[16] MoD, "The Strategic Defence Review 2025 – Making Britain Safer", 2 Jun 2025. https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad

[17] Home Office, "National Security (State Threats) Act 2026: factsheet", updated 6 Oct 2026. https://www.gov.uk/government/publications/national-security-state-threats-act-2026-factsheet/national-security-state-threats-act-2026-factsheet

[18] Ofcom, "Your landline is going digital: what you need to know". https://www.ofcom.org.uk/phones-and-broadband/landline-phones/future-of-landline-calls

[19] BBC News, "Copenhagen and Oslo airports forced to close temporarily over drones", Sep 2025. https://www.bbc.com/news/articles/cn4lj1yvgvgo

[20] Reuters, "Poland downs drones in its airspace…", 10 Sep 2025. https://www.reuters.com/business/aerospace-defense/poland-downs-drones-its-airspace-becoming-first-nato-member-fire-during-war-2025-09-10/

[21] CERT Polska, "Energy Sector Incident Report – 29 December 2025". https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

[22] The Register, "UK, EU officially pin Poland energy cyberattack on Russia", 13 Jul 2026. https://www.theregister.com/security/2026/07/13/uk-eu-officially-pin-poland-energy-cyberattack-on-russia/5270458

[23] NCSC, "Pro-Russia hacktivist activity continues to target UK organisations". https://www.ncsc.gov.uk/news/pro-russia-hacktivist-activity-continues-to-target-uk-organisations

[24] BBC News, "Pro-Russia hackers claim Greater Manchester council cyber attacks". https://www.bbc.co.uk/news/articles/c36p063jz7do

[25] Finnish Police (NBI), "Investigation into Fitburg cable damage concluded", 2026. https://poliisi.fi/en/-/investigation-into-fitburg-cable-damage-concluded

[26] Congressional Research Service, "Russian Hybrid Warfare Activities in Europe" (R49134), incl. Baltic Sentry. https://www.congress.gov/crs-product/R49134

[27] Cabinet Office, "National Risk Register 2025 edition". https://assets.publishing.service.gov.uk/media/67b5f85732b2aab18314bbe4/National_Risk_Register_2025.pdf

[28] GOV.UK, "National Emergency Alert test to be held on 7th September" (2025). https://www.gov.uk/government/news/national-emergency-alert-test-to-be-held-on-7th-september

Illustrations: AI-generated, fictional. They do not depict real people, places or events.

All sources accessed 15 October 2026.