

ISS GLOBAL / COMPARATIVE INCIDENT ASSESSMENT



UK infrastructure outages

Air traffic control, banking and Google Cloud — testing the links

REPORTING / REVIEW WINDOW

8 September–20 October 2026 · European comparisons

ISSUE DATE

2026-10-21

The reviewed record supports a cloud-dependent banking disruption and separate air traffic control faults. It does not establish a coordinated hostile operation.

This report tests the proposed connection between recent UK aviation failures and the 20 October digital-service disruption. It assesses causal evidence, malicious-activity indicators and European precedents, then sets out proportionate investigative priorities. ^{[1][7][9]}

Evidence cutoff: 21 October 2026, 08:06 BST (07:06 UTC). Public-source assessment; later findings may change the conclusions.

What happened and its threat significance

COUNTRIES / REGION	WHERE	WHEN
United Kingdom; Ireland; Germany; Spain; Portugal	UK air traffic control and London-region cloud services; European banking impacts and historical aviation/power comparisons.	Main incidents: 8 and 21 September; 20 October 2026. Assessment issued 21 October. Historical comparisons are dated separately.

What happened

On 20 October, Google Cloud suffered a London-region outage, and Revolut attributed disruption of its services to that supplier. Recent UK air traffic control failures had separately prompted operational restrictions. This report reconstructs the events, compares their mechanisms and assesses whether the public evidence supports a shared cause or deliberate interference. ^{[4][8][10]}

It also examines an independent German banking outage, a documented European aviation cyber incident and the Iberian electricity blackout to distinguish genuine causal links from similar consequences. ^{[11][12][14]}

Threat significance

ISS Global assessment. The immediate concern is resilience: disruption at one widely used supplier can affect several essential services, while independent faults can create a misleading impression of coordinated attack. Google’s security-monitoring services were also affected, making recovery of monitoring workflows an investigative priority. ^{[2][15]}

EXECUTIVE JUDGEMENT

Prioritise verified dependencies, continuity arrangements and preservation of technical evidence. The strongest supported explanation is a cloud-service cascade alongside distinct aviation faults. Any claim of rogue activity should be tested against evidence of unauthorised action, rather than inferred from the number of affected organisations. ^{[4][7][9]}

Scope, geography and event identity



Map 1. Geographic context only. London marker: 51.5072° N, 0.1275° W; city reference, not a cloud facility. EPSG:3857 display; WGS84 input. Scale applies at the bar latitude. Esri and credited contributors. [16][17]

CASE	DATE OF EVENT	ROLE IN THIS ASSESSMENT
NATS / Swanwick	8 Sep 2026	UK aviation software failure [7]
NATS / Prestwick	21 Sep 2026	Separate UK aviation network failure [9]
Google / Revolut	20 Oct 2026	Cloud incident and customer impact [1][4]
ING Germany	20 Oct 2026	Contemporaneous negative comparison [11]
Collins Aerospace	Reported 19 Sep 2025	Historical cyber comparator [12]
Iberian blackout	28 Apr 2025	Historical technical-cascade comparator [14]

The map is an orientation aid, not evidence of shared power, communications or hosting. A cloud region’s commercial label does not identify a single building. No local facility point or connection line is plotted without evidence.

Scope rule. “Yesterday” means 20 October 2026. Recent ATC events are resolved to the two September incidents above. This is a selected comparison, not a statistical survey of all European outages.

20 October: the documented cloud link

Google attributes the London-region outage to a power event affecting zone europe-west2-b. Its incident analysis remains pending. ^[1]

MILESTONE	EUROPE/LONDON — BST
Recorded start	20 Oct, 07:08
Most workloads recovering	13:10
Recorded incident end	15:00
Final displayed notice	15:03; most customers mitigated, a small residual group still affected ^[1]

Conversion uses PDT +8 hours = BST. The supplier’s 19 October 23:08 start is therefore 20 October in the UK. The recorded interval is 7 hours 52 minutes. The administrative end time should not be read as simultaneous recovery for every customer. ^[1]

Why Revolut is a supported connection

The Journal obtained a Revolut spokesperson’s attribution to Google Cloud and reported restoration for Irish users. Revolut said customer money and data remained safe. Its live status page showed all systems operational when checked on 21 October, but does not preserve the exact customer recovery time. ^{[4][5]}

Google’s customer case study documents Revolut’s use of Compute Engine. This supports the existence of a supplier relationship; the incident-specific statement supplies the causal attribution. A marketing case study alone would not prove that yesterday’s failed service depended on the affected zone. ^[6]

Banking impact is not one uniform event

Reuters reported Revolut card and ATM problems, Lloyds recovery expectations and HSBC customer-access difficulties. Its broader list also included user-report aggregation. Those observations do not establish an identical technical cause at every named organisation. ^[3]

Assessment. Record the Revolut dependency as supported. Keep other customer-level dependency claims separately qualified until operator records identify the failed service and its relationship to the cloud incident.

The aviation failures are distinct cases

Swanwick — 8 September 2026

NATS’ preliminary report identifies a previously unknown legacy software defect affecting flight data. It states that radar monitoring and aircraft communications continued, while reduced capacity and manual coordination preserved safety. Its security conclusion was preliminary: no evidence at that stage of malicious or cyber-related causation. ^[7]

The 18 September release describes a timing interaction during aircraft-code allocation: a higher-priority task interrupted processing, and incorrect resumption corrupted output. NATS described this as unrelated to the 2023 failure and rejected suggestions of incorrect military intervention. ^[8]

Prestwick — 21 September 2026

The subsequently published report identifies a site-network fault producing excessive network load and disrupted data exchange. It explicitly separates this event from 8 September and earlier NATS technical events. NATS security specialists reported no evidence of malicious cyber activity, unauthorised access or hostile intervention. ^[9]

PRESTWICK CHRONOLOGY	LOCAL TIME — BST
Initial network errors	02:32
Source confirmed / isolated	09:15–09:50
Normal operations; restrictions removed	14:00 ^[9]

What the comparison permits

ISS Global assessment. Shared ownership and similar travel disruption justify comparing resilience and recovery practices. They do not establish a common failing component. The public accounts identify different mechanisms, and neither supplies a causal path to the October cloud outage. ^{[7][9]}

A safety-driven reduction in capacity is an operational response. Treating that response as evidence of a hostile shutdown reverses the causal chain. The relevant comparison is what failed, which safeguards remained available and how workload was controlled.

Finding. Keep the two aviation events and the cloud incident as separate case records. Add an evidential link only if a common dependency or action is documented; do not connect them merely because their effects reached UK transport or banking.

05 / ANALYSIS

Which links survive examination?

PROPOSED CONNECTION	EVIDENCE ASSESSMENT	INVESTIGATIVE TREATMENT
Cloud → Revolut	Supported operator attribution; established supplier relationship. ^{[4][6]}	Dependency link with source and date.
Cloud → every named bank	Not demonstrated for each bank by the reviewed reporting. ^[3]	Separate service-impact evidence from root cause.
Cloud → Google SecOps	Same supplier records a related power-event outage. ^[2]	Linked service impact; not a second independent attack.
Cloud → ING Germany	ING reported no indication of external/provider connection. ^[3]	Keep separate unless new technical evidence changes this.
Swanwick → Prestwick	NATS expressly identifies unrelated faults. ^[9]	Comparison relationship, not established causation.
September ATC → October cloud	No shared component, malicious action or infrastructure path disclosed in these records. ^{[1][7][9]}	Unsubstantiated common-cause hypothesis.

ING is an important control case

German-language reporting describes disruption to ING's app and online banking and attributes a rejection of a cyber cause to the bank. That is a bank statement, not an externally audited finding. It nevertheless weighs against automatically merging all same-day incidents into the Google event. ^[11]

A useful analytical test asks what should be seen if the events really share a cause: a common supplier dependency, matching failure signatures, or a documented initiating action. Calendar coincidence alone is compatible with both shared and independent causes; it has little discriminating value.

A link must state its meaning

"Same day", "same supplier", "similar impact" and "same perpetrator" are different relationships. Only the first three can be created from scheduling, dependency or impact records. Attribution requires additional evidence. A single catch-all "linked" label would obscure the key judgement in this case.

Does the evidence support rogue activity?

Definition. Here, rogue activity means deliberate unauthorised interference: external compromise, insider sabotage or physical interference. It does not mean any serious malfunction, poor design or inadequate resilience. Operational negligence and intentional disruption are separate propositions.

HYPOTHESIS	FIT WITH REVIEWED EVIDENCE	WHAT WOULD MATERIALLY CHANGE IT
Distinct technical failures plus a cloud cascade	Best-supported explanation. Matches operator mechanisms and customer attribution. ^{[4][7][9]}	A contradiction in engineering evidence or a verified shared dependency.
Common non-malicious external dependency	Possible in principle, not evidenced across ATC and cloud here.	A common upstream provider, facility or change with a matching causal chronology.
Malicious action in one incident	Not established for October cloud; NATS publishes adverse findings against this explanation. ^{[7][9]}	Verified unauthorised access/ action causally tied to failure.
Coordinated hostile campaign	Unsupported by this selected public record.	Cross-case forensic links and actor evidence, beyond repeated headlines.

Cause, intent and attribution are separate tests

A reported power event describes an immediate mechanism. By itself it neither proves deliberate interference nor conclusively excludes it. The final engineering explanation, security review and change history are the appropriate evidence for that distinction. ^[1]

The absence of published indicators is weaker evidence than a competent examination finding none. NATS provides attributed security findings; Google’s displayed incident notice does not provide an equivalent detailed hostile-activity assessment. This difference should remain visible in the judgement. ^{[1][7][9]}

Current assessment

There is no affirmative evidence in the reviewed material sufficient to label this cluster sabotage, a state operation or a coordinated criminal campaign. That is a bounded assessment of the accessible record, not proof that every possible malicious explanation has been eliminated. Confidence is stronger in the documented Revolut dependency than in any comprehensive exclusion of hostile involvement.

European precedents: different evidential tests

Collins Aerospace — a documented cyber comparator

The NCA said the aerospace cyber incident was reported on 19 September 2025 and affected Heathrow and other European airports. Its 24 September statement announced an arrest the previous day on suspicion of Computer Misuse Act offences, with conditional bail. That procedural event is not a conviction. ^[12]

The NCA’s 2026 strategic assessment subsequently lists Collins among successful 2025 ransomware attacks. Together these records support a cyber classification of that historical incident; they do not establish who caused the current outages. ^[13]

Comparative lesson. Supplier dependence can transmit both accidental failures and malicious disruption. The downstream airport effects do not decide between those causes; the investigation and technical findings do. Similar inconvenience is not an attribution indicator.

Spain and Portugal — a technical cascade comparator

ENTSO-E’s 20 March 2026 announcement concerns the blackout of 28 April 2025. Its expert-panel findings describe interacting oscillations, voltage and reactive-power control problems, generation reductions and generator disconnections culminating in a cascade. It is a historical event with later investigative reporting. ^[14]

The engineering explanation illustrates why extensive disruption need not imply coordinated intervention. This report uses the published summary for that positive mechanism, not as a blanket claim that all conceivable security issues were excluded.

COMPARISON	RELEVANT SIMILARITY	DO NOT INFER
Collins, 2025	Supplier incident reaches multiple customers.	Same attacker or technique in 2026.
Iberia, 2025 / findings 2026	Technical propagation creates extensive impact.	Shared electricity failure with London.
ING, 20 Oct 2026	Same-day customer-access disruption.	Common provider merely from timing. ^[11]

Selection limit. These are contrasting examples, chosen to test reasoning. They are not a representative sample from which to calculate an increase in attacks or an elevated probability of sabotage.

Reporting chronology and evidence audit

PUBLICATION / OBSERVATION	WHAT BECAME PUBLIC	EVENT DATE DISTINGUISHED
16 / 18 Sep 2026	NATS preliminary report dated 16 Sep; release 18 Sep. ^{[7][8]}	8 Sep 2026
16 Oct 2026	Prestwick findings published. ^[10]	21 Sep 2026
20 Oct 2026	Google operational updates; Revolut impact and recovery reporting. ^{[1][4]}	20 Oct in UK time
20 Oct 2026	ING disruption and bank statements reported. ^{[3][11]}	20 Oct 2026
21 Oct 2026	Live Revolut status checked as operational. ^[5]	Observation date, not failure date

Source independence

Google’s cloud and security dashboards are complementary records from one supplier. NATS’ releases and reports likewise form one operator family per investigation. Reuters reproductions count as one reporting family. The Journal’s direct spokesperson comment supports Revolut’s stated attribution; it is not a second forensic examination. Counting URLs would overstate corroboration.

Conflicts and precision

The residual-impact qualification on page 4 takes precedence over Reuters’ broader restoration wording. All explicit dashboard times are converted from Pacific time. ^{[1][3]}

No transaction-loss totals, verified victim count, intrusion indicators, shared infrastructure inventory or cross-case forensic artefacts were available in the material reviewed. It cannot support a quantified trend, actor attribution or a claim that the whole UK payment system failed.

Imagery decision

Reviewed coverage offered a Reuters file photograph of a Google logo in Paris and an Alamy stock illustration for Revolut. Neither depicts the failed infrastructure or demonstrates its cause, so both were excluded. The real basemap supplies geographic context; no generated incident imagery or decorative “hacker” photograph is used. ^{[3][4]}

The linked NATS PDFs in the source register are public documents for examination. Their statements are attributed to the operator; ISS Global has not inspected the underlying systems or original technical logs.

Threat significance and investigation priorities

The operational risk is concrete

Google’s separate security record identifies disruption to SecOps SIEM and SOAR, including access, normalisation and detection workflows. Its recorded interval converts to 07:08–12:50 BST on 20 October; the 13:11 BST notice reports mitigation for affected customers. This supports monitoring interruption, not evidence that an attacker exploited it. ^[2]

ISS Global assessment. Availability and assurance can degrade together. A restored customer-facing service should not automatically close the investigation if monitoring, reconciliation or recovery records still need review. Check whether delayed events were recovered before drawing conclusions from apparent quiet periods.

PRIORITY	EVIDENCE TO REQUEST THROUGH AUTHORISED CHANNELS	DECISION SUPPORTED
Preserve chronology	Timestamped notices, internal incident logs and change records; retain original timezone.	Establish onset and causal order.
Validate dependencies	Affected service/zone records and supplier incident references.	Confirm or reject customer-level links.
Test hostile action	Competent security findings; access and change audit; relevant physical-event records.	Separate malfunction, error and deliberate action.
Reconcile monitoring	Ingestion gaps, delayed detections and recovery/backlog confirmation.	Evaluate assurance during the outage.
Measure consequence	Validated customer impact, recovery milestones and transaction reconciliation.	Separate access loss from financial/data loss.

COBR-style brief and Dfuze case support

Maintain one factual situation statement, affected-service list, consequence assessment and decision log. In Dfuze, retain separate event records with source snapshots and dated claims; label dependency links distinctly from comparisons or proposed attribution. Record the analyst’s reasoning as assessment, not as an exhibit finding.

Update threshold

Reassess when Google publishes its root-cause analysis, NATS releases later findings, a bank confirms a dependency, or an investigator discloses causally relevant hostile-activity evidence. The July UK designation of four cloud providers as critical third parties predates these events and supports scrutiny of systemic resilience; it is not a misconduct finding. ^[15]

Present judgement. Address the evidenced resilience risks now. Keep the hostile-activity hypothesis open to evidence, but do not promote it to an incident finding on temporal coincidence alone.

SOURCE REGISTER

Sources 01–06

Source families and access limits are recorded below. Repetition of a statement is not independent proof.

-
- 01 **Multiple services: europe-west2 incident Xs2XTHzAVC9YnafnPyzj**
Google Cloud · 20 October 2026; final displayed update 07:03 PDT
 Family: Google operator incident record · Full public text reviewed 21 October 2026; English. Operator statements are attributed, not independent forensic verification.
<https://status.cloud.google.com/incidents/Xs2XTHzAVC9YnafnPyzj>
-
- 02 **Google SecOps / SOAR incident TbiK9xsCcj7rkBCdGwD2**
Google Security Products · 20 October 2026; final displayed update 05:11 PDT
 Family: Google operator incident record; same supplier as [1] · Full public text reviewed 21 October 2026; English. Operator statements are attributed, not independent forensic verification.
<https://status.cloud.google.com/security/incidents/TbiK9xsCcj7rkBCdGwD2>
-
- 03 **Google Cloud outage in UK eases after impacting digital banks, public sector websites**
Reuters, republished by KSL · 20 October 2026
 Family: Reuters reporting · Full wire reproduction reviewed 21 October. Reuters original could not be opened. Named company comments distinguished from Downdetector reports; syndicated copies count once. Displayed KSL times not converted because timezone is unspecified.
<https://www.ksl.com/article/51638545/google-cloud-servicesface-outage-in-london-revolut-services-down-too>
-
- 04 **Revolut services restored as Google Cloud outage blamed for disruption**
The Journal / Andrew Walsh; with AFP · 20 October 2026
 Family: The Journal spokesperson reporting; AFP contribution · Full text reviewed 21 October. Direct Revolut spokesperson account; cloud details overlap Google/AFP. Relative update label; dated incident and embedded statement establish 20 October coverage.
<https://www.thejournal.ie/revolut-outage-customers-card-payments-app-7198815-Oct2026/>
-
- 05 **System status — Ireland**
Revolut · Live page accessed 21 October 2026
 Family: Revolut operator · Current status reviewed: all systems operational. Dynamic page is not a preserved incident chronology and cannot establish the precise recovery time.
<https://www.revolut.com/en-IE/system-status/>
-
- 06 **Revolut: Building the first global financial super app with Google Cloud**
Google Cloud · Undated customer case study
 Family: Google supplier / Revolut customer case · Full public case study reviewed 21 October. Supports an established supplier relationship, not a complete current dependency map or incident root cause.
<https://cloud.google.com/customers/revolut>
-

SOURCE REGISTER

Sources 07–12

Source families and access limits are recorded below. Repetition of a statement is not independent proof.

-
- 07 Preliminary investigation report: NAS incident 08 September 2026
NATS · Report dated 16 September 2026
 Family: NATS investigation — Swanwick · 18-page public PDF reviewed through web extraction, particularly executive summary, chronology and technical cause. Preliminary; underlying logs and later major report not available in the reviewed record.
<https://www.nats.aero/wp-content/uploads/2026/09/NATS-Preliminary-Investigation-Report-into-NAS-Incident-on-08-Sept-2026-Issued-16-Sept-2026.pdf>
-
- 08 NATS publishes preliminary report on technical incident of 8 September
NATS · 18 September 2026
 Family: NATS investigation — Swanwick; same family as [7] · Full public text reviewed 21 October 2026; English. Operator statements are attributed, not independent forensic verification.
<https://www.nats.aero/news/nats-publishes-preliminary-report-on-technical-incident-of-8-september/>
-
- 09 Prestwick Incident Report — 21 September 2026
NATS · Released 16 October 2026
 Family: NATS investigation — Prestwick · All three public PDF pages reviewed through web extraction. Operator investigation; security findings are attributed to NATS, not independently repeated tests.
<https://www.nats.aero/wp-content/uploads/2026/10/Prestwick-Incident-Report-161026.pdf>
-
- 10 NATS publishes report of Prestwick incident
NATS · 16 October 2026
 Family: NATS investigation — Prestwick; same family as [9] · Full public text reviewed 21 October 2026; English. Operator statements are attributed, not independent forensic verification.
<https://www.nats.aero/statement/nats-publishes-report-of-prestwick-incident/>
-
- 11 ING: Massive IT-Störung legt Onlinebanking und Banking-App stundenlang lahm
IT Finanzmagazin · 20 October 2026
 Family: German financial-technology reporting / ING statements · German public text reviewed 21 October; English paraphrase by ISS Global. Reports attributed ING comments; no underlying diagnostic evidence published.
<https://www.it-finanzmagazin.de/ing-massive-it-stoerung-legt-onlinebanking-und-banking-app-stundenlang-lahm-252589/>
-
- 12 UK arrest following aerospace cyber incident
National Crime Agency · 24 September 2025
 Family: NCA law-enforcement statement · Full public statement reviewed 21 October 2026. Historical comparator; arrest on suspicion is not conviction or proof of attribution to a state.
<https://www.nationalcrimeagency.gov.uk/news/uk-arrest-following-aerospace-cyber-incident>
-

SOURCE REGISTER

Sources 13–17

Source families and access limits are recorded below. Repetition of a statement is not independent proof.

-
- 13 **National Strategic Assessment 2026 — Online harms**
National Crime Agency · 2026 assessment; exact page publication date not displayed
Family: NCA threat assessment · Relevant cybercrime section reviewed 21 October. Describes Collins among 2025 ransomware cases; does not attribute the October 2026 outage cluster.
<https://www.nationalcrimeagency.gov.uk/nsa-domains-2026/nsa-online-harms-2026>
-
- 14 **Expert panel final report on 28 April 2025 blackout in Spain and Portugal**
ENTSO-E · 20 March 2026
Family: European electricity expert-panel findings · Public final-report announcement reviewed 21 October. Engineering summary, not a fresh independent examination by ISS Global; full technical annexes not analysed here.
<https://www.entsoe.eu/news/2026/03/20/entso-e-publishes-expert-panel-final-report-on-28-april-2025-blackout-in-spain-and-portugal/>
-
- 15 **UK financial system strengthened with new safeguards for major technology providers**
HM Treasury · 10 July 2026; designations effective 13 July
Family: UK government policy announcement · Full public text reviewed 21 October. Regulatory context, not evidence of misconduct or a finding about the October incident.
<https://www.gov.uk/government/news/uk-financial-system-strengthened-with-new-safeguards-for-major-technology-providers>
-
- 16 **London (Q84)**
Wikidata · Current entry accessed 21 October 2026
Family: Geographic reference · City reference and UK geography only. Marker at 51.5072° N, 0.1275° W; deliberately not a data-centre coordinate.
<https://www.wikidata.org/wiki/Q84>
-
- 17 **World Topographic Map service and static-map terms**
Esri / ArcGIS · Retrieved 21 October 2026
Family: Basemap provider · Provider attribution retained. Static-map terms: <https://doc.arcgis.com/en/arcgis-online/reference/static-maps.htm>. Context only; no infrastructure topology or attack route implied.
https://services.arcgisonline.com/ArcGIS/rest/services/World_Topo_Map/MapServer
-