INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 07:14 UTC

UK Cyber Chief: Nation-States Now Drive 75% of Critical Infrastructure Attacks, AI Will Accelerate Exploitation by 2028

SECURITY ANALYSIS | CRITICAL | CVSS 9.5

SCC Item ID	SCC-STY-2026-0220
Type	Security Analysis
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	UK Critical National Infrastructure broadly (no specific products or vendors identified)
Published	2026-06-17T12:00:00+00:00
Discovery Source	Rss:T2 Gov

Executive Summary

NCSC CEO Richard Horne disclosed on June 17, 2026, that nation-state actors, primarily Russia, China, and Iran, were responsible for approximately 75% of more than 200 cyber incidents targeting UK critical national infrastructure in the twelve months ending May 2026. Horne explicitly reframed the threat as a continuous adversarial contest, signaling that the UK government no longer treats CNI cyber risk as a manageable, episodic problem. The NCSC's assessment that AI-enabled exploitation of legacy CNI vulnerabilities is highly likely by 2028 sets a hard planning horizon for security leaders across Five Eyes nations and allied partners.

Technical Analysis

Richard Horne's June 17, 2026 remarks at RUSI, corroborated by NCSC's Annual Review 2025 CNI chapter, represent the most explicit public attribution of UK CNI attacks to a state-actor majority to date. The 75% figure covers more than 150 of 200-plus incidents across a twelve-month window, a volume and attribution density that suggests sustained, coordinated campaigns rather than opportunistic intrusions.

The MITRE techniques embedded in the source data sketch the operational playbook these adversaries are running: initial reconnaissance via active scanning (T1595) and exploitation of public-facing applications (T1190), followed by access through valid accounts and external remote services (T1078, T1133), supply chain compromise for initial footholds in interconnected CNI environments (T1195), and tool and exploit acquisition outside the target network (T1588, T1588.006). Post-access activity patterns include defense evasion through indicator removal (T1070) and impairment of defensive tools (T1562), persistence via system service creation

(T1543), and, in the most severe cases, ransomware-style data encryption (T1486).

The CWE profile is equally telling. CWE-1104 (use of unmaintained third-party components) and CWE-1035 (use of components with known vulnerabilities) dominate, reflecting CNI's well-documented reliance on operational technology and industrial control systems built on decades-old software stacks with no vendor support path. CWE-119 (memory safety violations in legacy codebases) and CWE-200 (information exposure) round out a vulnerability surface that was never designed to withstand Internet-era adversaries, let alone AI-assisted reconnaissance.

Horne's 2028 AI exploitation warning is grounded in a specific threat logic: adversaries are using AI to automate reconnaissance against legacy attack surfaces, lower the skill floor for exploit development against unpatched CVEs embedded in OT systems, and accelerate the time-to-exploit window. The implication for CNI operators is that the current window, 2026 to 2028, is the remediation window. Organizations that have deferred legacy modernization will find their deferral decision transformed from a financial risk into an active exploitation vector.

The advisory carries direct relevance beyond UK borders. Five Eyes intelligence-sharing architecture means that techniques refined against UK CNI are operationally transferable to equivalent infrastructure in the US, Canada, Australia, and New Zealand. The NCSC's public disclosure at this specificity level is itself a threat intelligence artifact, a signal to allied defenders that the attribution confidence is high enough to discuss publicly.

Action Checklist

1. Step 1: Inventory legacy OT and ICS components, identify systems running unsupported third-party software (CWE-1104) or components with known unpatched CVEs (CWE-1035); prioritize any CNI-adjacent systems with external network exposure.
2. Step 2: Audit external remote access and valid account controls, verify MFA enforcement on all external remote services (NIST AC-17, CIS 6.4) and review account inventories for dormant or over-privileged accounts (NIST AC-2, CIS 5.3, CIS 5.4) consistent with T1133 and T1078 exploitation patterns.
3. Step 3: Review supply chain risk posture, map third-party software and service dependencies in CNI-adjacent systems against the T1195 supply chain compromise vector; apply NIST AC-20 (Use of External Systems) controls and verify vendor security assurance documentation.
4. Step 4: Validate detection coverage against the disclosed TTP set, confirm SIEM and EDR rules cover active scanning (T1595), public-facing application exploitation (T1190), defense impairment (T1562), and indicator removal (T1070); audit log completeness per NIST AU-2 and CIS 8.2.
5. Step 5: Update threat model and risk register, formally incorporate Russia, China, and Iran state-sponsored actor profiles targeting CNI; document AI-accelerated exploitation as an emerging risk with a 2028 planning horizon per the NCSC assessment.
6. Step 6: Brief leadership and board, present the NCSC's 75% attribution figure and 2028 AI exploitation warning as a strategic planning input, not a compliance checkbox; frame legacy modernization investment in terms of the closing remediation window.
7. Step 7: Monitor NCSC and Five Eyes follow-on disclosures, track NCSC advisories, CISA joint advisories, and ASD/ACSC publications for updated IOCs, actor TTPs, and sector-specific CNI guidance tied to this campaign context.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO, CNI sector regulator, and NCSC if any detection output from Step 4 confirms active scanning, unauthorized remote access, or log tampering on CNI-adjacent systems, or if supply chain review in Step 3 identifies a backdoored or compromised vendor component with active network connectivity — any of these conditions indicates the organization has moved from preparation posture into an active incident requiring declaration under NIST 800-61r3 §3.2 incident criteria and applicable UK NIS Regulations notification obligations.
Recovery Notes	Following containment of any confirmed nation-state intrusion into CNI-adjacent systems, verify eradication completeness by re-imaging affected hosts from known-good golden images and validating firmware integrity on OT/ICS components against vendor-supplied checksums before restoring network connectivity — do not rely solely on AV or EDR clean bills of health given the sophistication of the Russia, China, and Iran actor set disclosed by NCSC. Maintain enhanced monitoring for at least 90 days post-recovery, specifically watching for reinfection via the original access vector and any signs of secondary persistence (scheduled tasks, WMI subscriptions, firmware implants) that survived the eradication phase. Coordinate with NCSC's CISP (Cyber Security Information Sharing Partnership) during the recovery window to receive any updated IOCs tied to the specific actor campaign before declaring recovery complete.
Forensic Artifacts	Windows Security Event Log — Event ID 4624 (Logon Type 10/3), 4648, 4672, and 4625 filtered for remote access sessions and failed logon spikes consistent with nation-state valid account (T1078) and external remote service (T1133) abuse against CNI operator identity infrastructure | OT/ICS network protocol logs (Modbus, DNP3, IEC 61850) captured via passive tap or industrial historian — anomalous read/write commands or engineering workstation polling patterns consistent with pre-positioning reconnaissance by Russian or Chinese APT groups targeting operational technology | Web server and application gateway access logs (IIS W3C logs or Apache/nginx access.log) — URI patterns, user-agent strings, and HTTP response codes indicative of automated exploitation scanning (T1595) and public-facing application exploitation (T1190) targeting internet-exposed CNI management interfaces | Windows Security Event Log and Sysmon Event ID 23 (FileDelete) and Event ID 26 (FileDeleteDetected) combined with audit log for Security event log clearing (Event ID 1102) and System log clearing (Event ID 104) — direct forensic evidence of indicator removal (T1070) activity consistent with nation-state operational security tradecraft | Third-party vendor remote access session logs (jump server logs, privileged access workstation audit trails, vendor VPN authentication records) — timestamps, source IPs, and commands executed during vendor maintenance windows, relevant to supply chain compromise (T1195) forensic reconstruction of how a trusted vendor channel may have been leveraged for initial access into CNI systems

Per-Action IR Details

Step 1: Inventory legacy OT and ICS components — identify systems running unsupported third-party software (CWE-1104) or components with known unpatched CVEs (CWE-1035); prioritize any CNI-adjacent systems with external network exposure.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing and maintaining IR capability, asset visibility, and baseline posture before incidents occur

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a

Vulnerability Management Process), NIST AC-20 (Use Of External Systems)

Compensating: Run a passive network scan of the OT/ICS network segment using nmap with the -sn flag to avoid disrupting industrial protocols, combined with osquery's 'SELECT * FROM programs' and 'SELECT * FROM kernel_modules' to enumerate installed software versions without an enterprise asset manager. Cross-reference output against CISA's Known Exploited Vulnerabilities catalog (catalog.cisa.gov/api/1.0/vulnerabilities.json) using a simple Python script to flag unpatched components. Maintain a shared spreadsheet with columns for asset, firmware/OS version, last patch date, and external exposure status — this is achievable by two analysts in a single sprint.

Evidence: This is a preparation-phase inventory step and does not alter live system state, so no volatile capture precedes it. However, document the current asset and patch state as a baseline snapshot — export osquery results, nmap output, and any firmware version strings to immutable storage before any patching begins, so the pre-remediation exposure surface is preserved for later post-incident comparison against NCSC's disclosed CNI targeting patterns from Russia, China, and Iran actors.

Step 2: Audit external remote access and valid account controls — verify MFA enforcement on all external remote services (NIST AC-17, CIS 6.4) and review account inventories for dormant or over-privileged accounts (NIST AC-2, CIS 5.3, CIS 5.4) consistent with T1133 and T1078 exploitation patterns.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: hardening identity and access controls as a prerequisite to incident detection and response capability

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AC-17 (Remote Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For VPN/RDP services without a commercial MFA layer, deploy Duo Security free tier or configure Windows NPS with Azure AD MFA (free for up to 50 users) as an authentication proxy. Enumerate all Active Directory accounts inactive for 45+ days using: 'Search-ADAccount -AccountInactive -TimeSpan 45.00:00:00 | Select-Object Name,LastLogonDate,Enabled | Export-Csv dormant_accounts.csv'. For over-privileged accounts, run 'Get-ADGroupMember -Identity "Domain Admins" -Recursive' and compare against a manually maintained least-privilege role matrix. This two-step PowerShell audit is achievable in under two hours by one analyst.

Evidence: BEFORE revoking any dormant or over-privileged accounts or disabling remote access services, capture the following volatile and log evidence specific to state-actor valid-account abuse patterns: export Windows Security Event Log Event ID 4624 (successful logon) and 4648 (explicit credential logon) for the past 90 days filtering on Logon Type 10 (RemoteInteractive) and Type 3 (Network); export VPN authentication logs showing source IPs and session durations; capture 'Get-NetTCPConnection' output on remote access hosts to document any currently active inbound sessions. Nation-state actors abusing valid accounts frequently maintain persistent access through secondary implants before defensive review triggers account action — these logs preserve the evidence of that access pattern before revocation destroys session context.

Step 3: Review supply chain risk posture — map third-party software and service dependencies in CNI-adjacent systems against the T1195 supply chain compromise vector; apply NIST AC-20 (Use of External Systems) controls and verify vendor security assurance documentation.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: identifying and managing external dependencies that expand the attack surface available to nation-state supply chain operators

Controls: NIST AC-20 (Use Of External Systems), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Use the free Syft CLI tool (anchore/syft) to generate a Software Bill of Materials (SBOM) in CycloneDX format for each CNI-adjacent server, then cross-reference component hashes against the OSV vulnerability database (osv.dev API) to identify compromised or backdoored third-party libraries consistent with the

nation-state supply chain tradecraft highlighted in the NCSC assessment. Manually review vendor security assurance documentation against the NCSC's published supply chain security guidance and log the review date, vendor name, and assurance status in a two-column tracker. Two analysts can cover the highest-criticality systems in a single working day using this approach.

Evidence: This step is a preparatory review and does not directly alter live system state. However, before any vendor software is disabled or removed based on findings, capture installed package metadata and running process lists: run 'Get-WmiObject Win32_Product | Select Name,Version,Vendor | Export-Csv installed_sw_baseline.csv' and 'ps aux' or 'Get-Process | Select-Object Name,Id,Path' on Linux and Windows hosts respectively. Preserve integrity hashes (SHA-256) of all third-party binaries flagged during the review using 'Get-FileHash -Algorithm SHA256' so that any subsequent supply chain implant analysis has a clean pre-remediation binary baseline to compare against. Nation-state supply chain implants targeting CNI (consistent with patterns attributed to Russia and China actors in the NCSC assessment) frequently persist in signed vendor update packages or legitimate remote management agents.

Step 4: Validate detection coverage against the disclosed TTP set — confirm SIEM and EDR rules cover active scanning (T1595), public-facing application exploitation (T1190), defense impairment (T1562), and indicator removal (T1070); audit log completeness per NIST AU-2 and CIS 8.2.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: validating that monitoring capabilities can identify the specific TTP set disclosed by the NCSC for CNI-targeting nation-state campaigns

Controls: NIST AU-2 (Event Logging), NIST AU-3 (Content Of Audit Records), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with the SwiftOnSecurity or olafhartong modular config to cover process creation (Event ID 1), network connections (Event ID 3), and file deletion (Event ID 23 — relevant to T1070 indicator removal) on all CNI-adjacent Windows hosts without requiring a commercial EDR. Apply the public Sigma rules for T1595 (repo: SigmaHQ/sigma, tags: attack.reconnaissance) and T1562 (tags: attack.defense_evasion) against Windows Event Logs using chainsaw (WithSecureLabs/chainsaw) for free batch log hunting. For Linux CNI hosts, enable auditd with rules targeting execve syscalls and deletion of log files in /var/log to detect indicator removal. Validate coverage gaps by running ATT&CK Navigator (free, MITRE-hosted) against the NCSC-disclosed TTP set and coloring uncovered techniques red.

Evidence: Detection coverage validation does not directly alter live state, but before making any rule changes or disabling existing detections during tuning, export current SIEM alert rule sets and EDR policy configurations as a point-in-time backup. For CNI environments where nation-state actors are known to perform defense impairment (consistent with T1562 patterns attributed to Russian and Chinese APT groups), also capture current Windows Security Event Log audit policy output via 'auditpol /get /category:*' and Linux auditd rule sets via 'auditctl -l' — these document the detection baseline before any changes and preserve evidence of whether impairment of these controls was attempted prior to detection validation.

Step 5: Update threat model and risk register — formally incorporate Russia, China, and Iran state-sponsored actor profiles targeting CNI; document AI-accelerated exploitation as an emerging risk with a 2028 planning horizon per the NCSC assessment.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: integrating current threat intelligence into organizational risk posture and planning artifacts to ensure IR capability is scoped to the actual adversary set

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: Without a commercial threat intelligence platform, use MITRE ATT&CK Navigator (free) to build dedicated group overlays for APT28, APT29, APT40, and APT34 (the primary CNI-targeting groups attributed to Russia, China, and Iran respectively) and export the TTP heat maps as PDFs for inclusion in the risk register. Document the NCSC's 75% attribution figure and 2028 AI exploitation horizon directly in the risk register entry, citing the NCSC CEO's June 17, 2026 disclosure as the source, and assign a formal risk owner from the CNI operator's leadership team. This can be completed by one analyst in a half-day using free MITRE tooling and a standard risk register template.

Evidence: This is a documentation and planning step that does not alter live system state and does not require volatile evidence capture. However, preserve the source intelligence artifacts — screenshots or archived copies of the NCSC CEO's June 17, 2026 disclosure and any associated NCSC advisory publications — as immutable attachments to the risk register entry, so the evidentiary basis for the threat model update is auditable and cannot be questioned during a post-incident review or regulatory inquiry.

Step 6: Brief leadership and board — present the NCSC's 75% attribution figure and 2028 AI exploitation warning as a strategic planning input, not a compliance checkbox; frame legacy modernization investment in terms of the closing remediation window.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: communicating lessons learned, threat landscape changes, and capability investment needs to organizational leadership to drive sustained improvement

Compensating: Prepare a one-page executive briefing document (no tooling required) structured around three data points: (1) the NCSC's 75% nation-state attribution figure for UK CNI incidents in the twelve months ending May 2026, (2) the NCSC's 2028 AI-accelerated exploitation warning, and (3) the organization's current gap count from Steps 1–4 mapped to estimated remediation cost. Frame the legacy modernization ask in terms of the shrinking window between NCSC's 2028 horizon and current technical debt — this framing is directly supported by NCSC CEO Richard Horne's June 17, 2026 public statement and requires no proprietary tooling to present.

Evidence: This step does not alter live system state and requires no volatile evidence capture. Attach the outputs from Steps 1–4 (asset inventory gaps, dormant account counts, supply chain dependency map, and detection coverage gaps) as supporting annexes to the briefing so leadership decisions are grounded in organization-specific evidence rather than industry statistics alone.

Step 7: Monitor NCSC and Five Eyes follow-on disclosures — track NCSC advisories, CISA joint advisories, and ASD/ACSC publications for updated IOCs, actor TTPs, and sector-specific CNI guidance tied to this campaign context.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: integrating external intelligence updates into organizational detection and response capability as the threat campaign evolves

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Configure free RSS feed monitoring for NCSC (ncsc.gov.uk/api/1/services/alerts.rss), CISA (cisa.gov/news.xml), and ASD/ACSC (cyber.gov.au) advisories using a self-hosted RSS reader (FreshRSS, free and open source) with email alerting for keywords: 'critical national infrastructure', 'Russia', 'China', 'Iran', 'APT', 'OT', 'ICS'. When a new joint advisory drops, immediately extract any STIX/TAXII-formatted IOC packages (CISA routinely publishes these) and import them into a local OpenCTI free instance or manually load indicators into Sysmon network connection rules and YARA signatures for immediate host-level detection coverage without a commercial TIP.

Evidence: This is an ongoing intelligence monitoring step and does not alter live system state, so no volatile evidence capture precedes it. However, each time a new NCSC or Five Eyes advisory is actioned — particularly if it results in blocking an IOC or updating a detection rule — log the advisory reference, date actioned, IOCs added, and detection rules updated in a change log. This creates an auditable record that the organization responded to authoritative CNI threat intelligence in a timely manner, which is critical evidence in the event of a subsequent regulatory inquiry into whether reasonable precautions were taken following the NCSC's public June 2026 disclosures.

Detection Guidance

Detection for the TTP cluster described by the NCSC should focus on four behavioral layers.

Reconnaissance and initial access: Monitor for high-frequency automated scanning activity against externally exposed OT management interfaces, VPN gateways, and remote access portals (T1595, T1190). Log and alert

on authentication attempts against legacy remote services, particularly those that lack MFA, and flag any successful logins from unusual geographies or ASNs associated with state-sponsored infrastructure (T1133, T1078). Per NIST AU-2 and CIS 8.2, ensure authentication logs from network perimeter devices and remote access systems are collected and retained.

Defense evasion and persistence: Hunt for evidence of log clearing or modification (T1070), baseline expected log volume per source and alert on anomalous gaps. Review scheduled tasks, services, and startup items for unauthorized additions (T1543); cross-reference against known-good baselines using D3-SICA (System Init Config Analysis). Alert on termination or configuration changes to EDR agents, firewalls, and audit logging processes (T1562).

Supply chain exposure: Audit software bills of materials for CNI systems; flag any component matching CWE-1104 or CWE-1035 profiles. Monitor for unexpected outbound connections from OT/ICS systems to external infrastructure (T1195 post-compromise behavior).

Legacy vulnerability surface: Prioritize memory-safety CVEs (CWE-119) on systems identified in the asset inventory. Enable file integrity monitoring on configuration files and system executables using D3-SFA (System File Analysis). Review information exposure risks (CWE-200) on systems with external interfaces, banner stripping, error message suppression, and unnecessary service exposure.

NIST SI-4 (system monitoring) and AU-6 (audit record review and analysis) should govern the operational cadence for these detection activities. Organizations should map detection gaps against the full T1595/T1190/T1078/T1133/T1070/T1562 chain rather than addressing techniques in isolation.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to NCSC CNI advisory and NCSC Annual Review 2025 Chapter 02 for published indicators`	The NCSC public disclosure describes campaign TTPs and attribution at a strategic level; specific technical IOCs (C2 infrastructure, payload hashes, tooling signatures) associated with Russian, Chinese, and Iranian CNI intrusion sets are published through NCSC protected channels and coordinated Five Eyes advisories rather than in the public-facing announcement	LOW

Framework Mappings

MITRE-ATTACK

- **T1195** — Supply Chain Compromise
- **T1588** — Obtain Capabilities
- **T1070** — Indicator Removal
- **T1588.006** — Vulnerabilities
- **T1486** — Data Encrypted for Impact
- **T1543** — Create or Modify System Process

- **T1133** — External Remote Services
- **T1595** — Active Scanning
- **T1190** — Exploit Public-Facing Application
- **T1078** — Valid Accounts
- **T1562** — Impair Defenses

NIST-800-53R5

- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **CA-7** — Continuous Monitoring
- **SI-4** — System Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **AU-9** — Protection of Audit Information
- **CM-6** — Configuration Settings
- **SA-4** — Acquisition Process
- **SA-22** — Unsupported System Components
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A06:2021** — Vulnerable and Outdated Components
- **A01:2021** — Broken Access Control
- **A03:2021** — Injection

CIS-V8

- **16.4** — Establish and Manage an Inventory of Third-Party Software Components
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **16.10** — Apply Secure Design Principles in Application Architectures
- **15.1** — Establish and Maintain an Inventory of Service Providers

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1195	Supply Chain Compromise	Initial-Access
T1588	Obtain Capabilities	Resource-Development
T1070	Indicator Removal	Defense-Evasion
T1588.006	Vulnerabilities	Resource-Development
T1486	Data Encrypted for Impact	Impact
T1543	Create or Modify System Process	Persistence
T1133	External Remote Services	Persistence
T1595	Active Scanning	Reconnaissance
T1190	Exploit Public-Facing Application	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1562	Impair Defenses	Defense-Evasion

Sources

Source	URL	Tier
News Feed	https://www.ncsc.gov.uk/news/ncsc-ceo-hostile-states-linked-to-thre...	T1
	https://www.ncsc.gov.uk/news/ncsc-ceo-hostile-states-linked-to-thre...	T1
	https://www.infosecurity-magazine.com/news/hostile-states-cni-75-pe...	T3
	https://therecord.media/britain-nation-state-cyberattacks-richard-h...	T3
Defending the UK's critical national infrastructure	https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025/chapter-...	T1

Generated 2026-06-18 07:14 UTC by TJS Security Command Center