TREADSTONE 71® · ADVERSARY BRIEFINGS · OCTOBER 29, 2026 · TLP:CLEAR

Four Adversaries, Four Decisions

Threat intelligence for critical infrastructure operators: who is coming, what they want from you, how likely they are to try, and what to decide before they arrive.

Bottom line. Each state runs one operation against infrastructure operators that matters more than the rest. China holds quiet access for a future crisis. Russia destroys, and its targets have moved west into NATO. North Korea gets hired. Iran-affiliated operators rewrite logic in small water plants; personas then claim and deny. All four use AI the same way: the old attack, faster, cheaper and with fewer people. None needed AI to invent a new one.

China · Volt Typhoon

Holds access in power, water, telecoms and transport for a Taiwan crisis. **Decide:** close the management-platform doors now.

Russia · Sandworm

Wipes systems and cuts power; aimed a wiper at a Polish energy firm in December 2025 (ESET, medium confidence). **Decide:** fund recovery time.

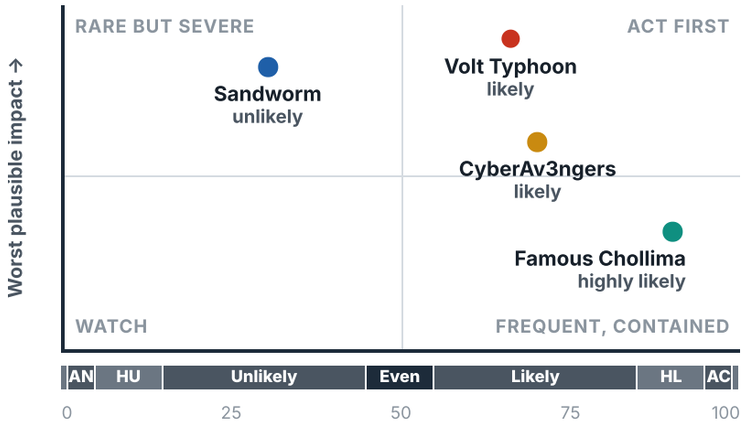
North Korea · Famous Chollima

Wins remote IT jobs behind deepfake faces; pays Pyongyang. **Decide:** verify identity at payroll and the laptop.

Iran · CyberAv3ngers

Defaced screens in 2023; rewrote safety logic in 2026 (IRGC role: likely). **Decide:** no controller on the open internet.

WHERE EACH ACTOR SITS FOR AN INFRASTRUCTURE OPERATOR



Treadstone 71 analytic placement; each dot sits mid-band. Conditions: China, a US or allied lifeline operator; Russia, an operator in NATO Europe sits higher; North Korea, a firm hiring remote IT staff; Iran, controllers reachable from the internet. AN almost no chance, HU highly unlikely, HL highly likely, AC almost certain.

WHO IN YOUR COMPANY OWNS THE RESPONSE

Owner	China	Russia	DPRK	Iran
Board	●	●	○	●
CISO and SOC	●	●	●	○
OT and plant engineering	●	●		●
HR and recruiting			●	
Finance and payroll		●	●	
Legal and compliance	○	●	●	○
Communications	○	●		●
Procurement and vendors	●	○	●	○

● primary owner ○ supporting role

AI IN EVERY PLAYBOOK: WHERE EACH STATE USES IT, BY PUBLIC RECORD

Use of AI	China	Russia	N. Korea	Iran
Reconnaissance	●	◐	◐	●
Personas and phishing	●	●	●	●
Influence content	●	●	◐	●
Malware and code	●	●	●	●
Identity fraud and deepfakes			●	◐
Autonomous AI agents	●			

● documented in government or AI-company reporting, 2024 to 2026 ◐ one vendor report, or unattributed blank: no public record. Covers each state's operators beyond the cluster briefed.

HOW EACH BRIEFING READS

Each adversary gets three pages: the picture first (bottom line, decision, judgments, who they are, what they want, how they operate), then how they get in, where you stop them, how they use AI and who owns the response. The plan closes each briefing: dated actions with owners, signposts to watch, and the evidence behind the calls.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

CHINA

Volt Typhoon

Also tracked as Vanguard Panda (CrowdStrike) and Bronze Silhouette (Secureworks) · Sponsor: People's Liberation Army, possible MSS overlay · China composite in The Adversary Index: 89 (Q3 2026) · Briefing date: October 29, 2026

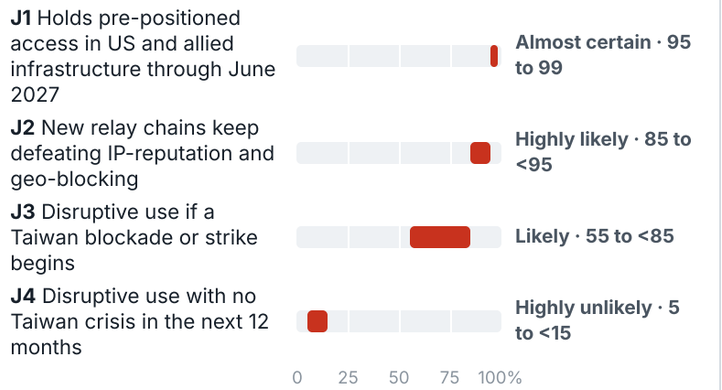
Bottom line. Volt Typhoon sits inside the plant and waits. Beijing picks the day. A Taiwan crisis is the trigger to watch. Lumen's Black Lotus Labs reported on October 29 that the group survived takedowns of its router network and rebuilt its relay chains in under two minutes. Four confirmed zero-days in network management products fell along the way. Treadstone 71 assesses it almost certain that the group holds access inside US and allied infrastructure through mid-2027, and highly unlikely that it switches anything off before a crisis gives it a reason.

The decision. Close the doors into your management and SD-WAN platforms now, before a crisis, and prove from your own logs that nobody already walked through them.

WHO

A PLA-run cluster. Treadstone 71 places it under the Cyberspace Force, formed when the PLA broke up its Strategic Support Force in April 2024, and holds a possible MSS overlay at a roughly even chance. Microsoft disclosed the group in May 2023. A Five Eyes advisory of February 2024 found access held at some victims for at least five years, which puts first entry in 2019 or earlier.

JUDGMENTS, AS SHERMAN KENT BANDS (BAR = THE BAND'S RANGE)



WHAT THEY WANT FROM YOU

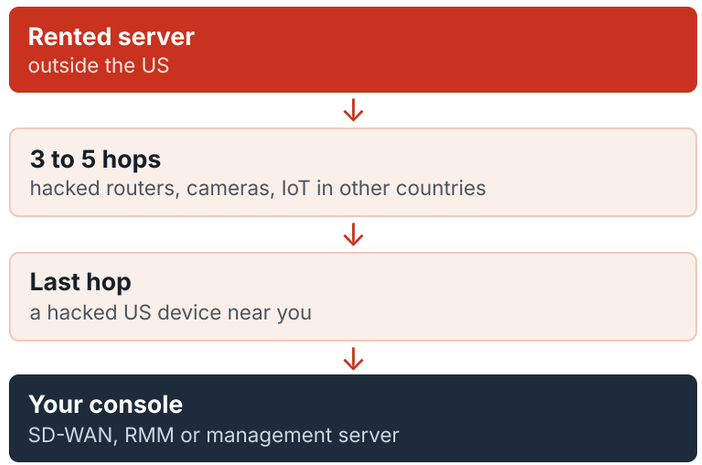
Access, held until a crisis makes it worth using: credentials and a quiet route into the systems that run power, water, telecoms, ports and transport. Lumen found the most victims in Hawaii, California and Texas. That map fits preparation for a fight in the Pacific.

SEVEN YEARS OF QUIET ACCESS

2019	Earliest access, per a February 2024 advisory
Mid-2021	Earliest activity Microsoft observed
May 2023	Microsoft and US agencies disclose the group
Nov 2023	Silent Train relay network appears
Jan 2024	FBI takes down the KV-botnet routers
Aug 2024	Versa Director zero-day exploited
Feb 2026	Cisco SD-WAN flaw (CVSS 10) exploited
Oct 2026	Lumen: 4 zero-days, hundreds of victims warned

Sources: US and Five Eyes advisories; Lumen via Security Affairs.

SILENT TRAIN: HOW THE TRAFFIC REACHES YOU



Chains average about four devices; a new chain takes under two minutes to build. The final address looks local, so IP reputation and geo-blocking miss it.

QUIET ACCESS UNTIL A TRIGGER



© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

CHINA · VOLT TYPHOON · HOW THEY GET IN, AND WHO CARES

HOW THEY GET IN, AND WHERE YOU STOP THEM

	THEIR MOVE	WHERE YOU STOP IT
1	Rents a server outside the US, then hops through hacked routers, cameras and IoT gear in other countries, about four devices per chain.	**Stop:** Do not trust IP reputation alone. Alert on admin logins from residential addresses, even local ones.
2	Exits through a compromised US device close to you, so the traffic looks local.	**Stop:** Allowlist the few addresses allowed to reach management consoles.
3	Exploits the management layer: Versa Director, N-able N-central, Cisco Catalyst SD-WAN, VeloCloud Orchestrator, Quest KACE.	**Stop:** Take every management console off the open internet. Patch those five first.
4	Steals admin credentials and copies the Active Directory database with ntdsutil.	**Stop:** Phishing-resistant MFA for every admin. Alert on ntdsutil and volume shadow copies on domain controllers.
5	Lives off the land with netsh, wmic and PowerShell, and leaves no malware behind.	**Stop:** Hunt admin-tool misuse across 12 months of logs. File hashes will not find it.
6	Waits for months or years, active mostly during China business hours.	**Stop:** Keep 12 months of telemetry. Check login times against China Standard Time.

WHERE CHINA'S OPERATORS USE AI, BY PUBLIC RECORD

Reconnaissance DOCUMENTED	**Personas and phishing** DOCUMENTED
Influence content DOCUMENTED	**Malware and code** DOCUMENTED
Identity fraud and deepfakes NO PUBLIC RECORD	**Autonomous AI agents** DOCUMENTED

State-level view from the overview matrix, wider than the cluster briefed.

AI IN THEIR PLAYBOOK

No public record ties Volt Typhoon itself to AI tools. Automation shows plainly. Lumen counted more than 27 device types in the relay chains. Nobody builds that by hand. Other Chinese operators already run AI end to end. In July, suspected Chinese hackers ran up to eight AI agents built from open-source frameworks against a government network the Financial Times identified as Taiwan's, mapped 21 systems and took at least 85 accounts. Expect the pre-positioning mission to adopt the same agents.

So what. Indicator feeds miss Volt Typhoon. No malware. Local-looking addresses. Legitimate admin tools. Your own log history is the only proof the group is absent, read by someone who knows what normal looks like.

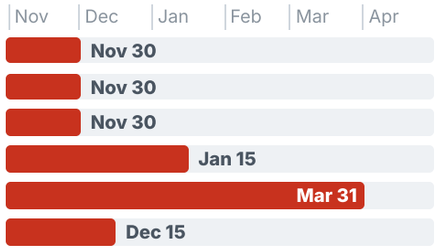
WHO CARES, AND THE DECISION EACH OWES

Owner	Why it matters	Decision they owe
Board	A crisis across the Pacific cuts your service with no warning.	Set the tolerance for a crisis-day outage and fund the fixes below.
CISO and SOC	Detection rests on behavior. Signatures miss it.	Approve the hunt and the 12-month log retention.
OT and plant engineering	The target is the ability to stop operations.	How many hours do we run with IT down or untrusted?
Procurement and IT vendors	Managed service providers and management platforms are the doors.	Require patch times and MFA in vendor contracts.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

CHINA · VOLT TYPHOON · WHAT TO DO, AND WHAT TO WATCH

THE PLAN ON ONE LINE: EACH ACTION, ITS OWNER, ITS DEADLINE



Bars run from today, October 29, 2026, to each deadline. Year-one cost, mid-size operator: $122K to $330K; Fortune tiers on page 15.

SIGNPOSTS TO WATCH

Signpost	Most likely meaning
PLA drills around Taiwan turn into a declared exclusion zone or blockade	Judgment three's trigger is met. Start the manual-operations plan and staff it around the clock.
A new joint advisory names fresh Volt Typhoon zero-days	Your patch window shrinks from weeks to days.
Admin logins to management consoles from local residential addresses at odd hours	A relay chain likely ends on your doorstep. Investigate before you block.
A vendor reports a successor to Silent Train	The group adapted again; expect new device types in the chains.

WHAT TO DO, BY WHEN, AND WHAT IT COSTS

#	Action	Owner	By; mid-size cost
1	List every internet-facing management, RMM and SD-WAN console. Pull it off the internet or put it behind VPN with phishing-resistant MFA.	**CIO**	**Nov 30, 2026** **$20-55K**
2	Patch Versa Director, N-able N-central, Cisco Catalyst SD-WAN (CVE-2026-20127), VeloCloud Orchestrator and Quest KACE.	**IT operations**	**Nov 30, 2026** **$5-15K**
3	Extend log retention to at least 12 months for edge devices and management systems.	**CISO**	**Nov 30, 2026** **$20-65K/yr**
4	Hunt up to 12 months of held logs for ntdsutil, netsh portproxy and remote wmic on domain controllers and jump hosts.	**SOC**	**Jan 15, 2027** **$25-90K**
5	Run a 72-hour manual-operations drill that assumes IT is compromised.	**OT engineering**	**Mar 31, 2027** **$50-100K**
6	Brief the board on crisis-triggered disruption; ask it to set the outage tolerance.	**CISO**	**Dec 15, 2026** **$2-5K**

WHICH EVIDENCE CARRIES WHICH JUDGMENT

	E1 A1	E2 B2	E3 B3	E4 B2	Direct
J1	●	●		○	2
J2	○	●		○	1
J3	●			●	2
J4	●	●		○	2

● direct support ○ indirect or partial blank: not relevant. Grades under each source: reliability and credibility. E3: AI section. J3 and J4 lean on the advisories' finding that the access serves disruption in a conflict; no disruptive use has been observed.

EVIDENCE BEHIND THE JUDGMENTS

#	Source	Rel.	Cred.
E1	NSA, CISA, FBI and Five Eyes advisories, 2023 to 2024	A	1
E2	Lumen Black Lotus Labs, via Security Affairs, Oct 29, 2026	B	2
E3	Dream and Financial Times on AI agents, via Security Affairs, Aug 12, 2026	B	3
E4	Treadstone 71 Volt Typhoon annex, May 2026	B	2

METHODS APPLIED

Indicators and warnings tied to a single trigger, a Taiwan crisis. **Key assumptions check:** activation needs a political trigger; if that assumption fails, judgment four rises. **Cone of plausibility:** baseline quiet access; crisis activation; exposure by a vendor that forces a rebuild. Reliability and credibility are graded apart under the ASA Evidence Standard.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

RUSSIA

Sandworm

Also tracked as APT44, Seashell Blizzard (Microsoft), Voodoo Bear (CrowdStrike) and ELECTRUM (Dragos) · Sponsor: GRU Unit 74455 · Russia composite in The Adversary Index: 85 (Q3 2026) · Briefing date: October 29, 2026

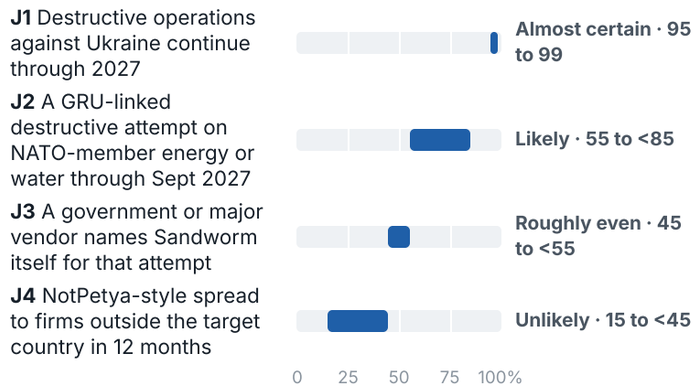
Bottom line. Sandworm turns the lights off. The unit holds the clearest public record of cutting power by cyberattack, in Ukraine in 2015 and 2016. NotPetya was its work too, the costliest cyberattack on record at roughly $10 billion. ESET ties it, at medium confidence, to DynoWiper, a new wiper aimed at a Polish energy company in late December 2025. The attack failed. ESET still calls it a rare destructive strike on a NATO member's infrastructure. Treadstone 71 assesses it likely that GRU units or their hacktivist fronts attempt another destructive attack on NATO-member energy or water through September 2027.

The decision. Treat Russia as a sabotage threat to your own infrastructure and measure readiness in hours to recover.

WHO

GRU Unit 74455, run from a building in Khimki outside Moscow, with six officers indicted by Washington in October 2020. Eighteen years in, the unit hides behind Telegram "hacktivist" fronts that claim its work: CyberArmyofRussia_Reborn, XakNet and Solntsepek, per Mandiant; a separate GRU-backed front, Z-Pentest, burst water pipes in Denmark in 2024, and Copenhagen blamed Russia in December 2025.

JUDGMENTS, AS SHERMAN KENT BANDS (BAR = THE BAND'S RANGE)



WHAT THEY WANT FROM YOU

Pressure on governments that back Ukraine, with your outage as the message to your government. Poland helps stabilize Ukraine's grid; ESET suggests the December strike aimed to stress that support in winter.

THE TARGET SET MOVES WEST

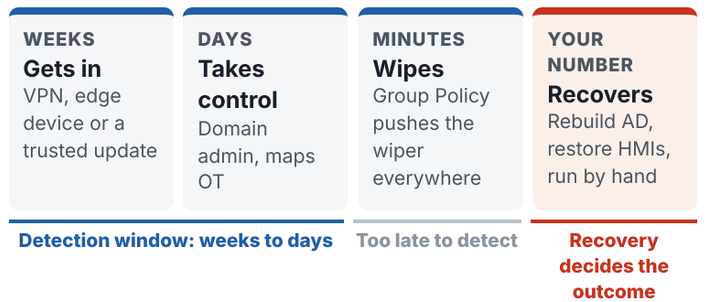
Dec 2015	Ukraine grid: 225,000 customers lose power
Dec 2016	Kyiv substation hit with Industroyer
Jun 2017	NotPetya: about $10 billion in damage worldwide
Feb 2022	Viasat satellite modems knocked out across Europe
Jan 2024	Telegram fronts tamper with Texas water utilities
2024	GRU-backed Z-Pentest bursts water pipes in Denmark
Dec 2025	Polish energy company: DynoWiper attack fails

Sources: DOJ, Mandiant, Danish government, ESET. Z-Pentest is a GRU-backed front, not Sandworm by name.

THE ESCALATION LADDER, TOP RUNG WORST



A WIPER ATTACK: WHERE TIME FAVORS YOU, AND WHERE IT RUNS OUT



© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

RUSSIA · SANDWORM · HOW THEY GET IN, AND WHO CARES

HOW THEY GET IN, AND WHERE YOU STOP THEM

	THEIR MOVE	WHERE YOU STOP IT
1	Gets in through VPNs and edge devices, or through a trusted software update, as with the Ukrainian accounting software behind NotPetya.	**Stop:** Patch edge devices first. Watch what your software updates change.
2	Takes domain admin and maps the OT network.	**Stop:** Separate IT and OT admin accounts. One controlled jump path into OT.
3	Pushes a wiper to every machine at once through Group Policy or scheduled tasks.	**Stop:** Alert on new or edited Group Policy objects and domain-wide scheduled tasks.
4	Hits the plant: protection relays, HMIs and SCADA servers.	**Stop:** Offline gold images of HMIs and SCADA servers; tested manual operation.
5	A Telegram front claims the attack before you understand it.	**Stop:** Verify through your ISAC before you confirm or deny anything.

WHERE RUSSIA'S OPERATORS USE AI, BY PUBLIC RECORD

Reconnaissance ONE REPORT	**Personas and phishing** DOCUMENTED
Influence content DOCUMENTED	**Malware and code** DOCUMENTED
Identity fraud and deepfakes NO PUBLIC RECORD	Autonomous AI agents NO PUBLIC RECORD

State-level view from the overview matrix, wider than the cluster briefed.

AI IN THEIR PLAYBOOK

No public report ties Sandworm itself to AI tools. Its sister GRU unit, APT28, fielded LameHug in July 2025: malware that asks an open-source model, Qwen 2.5-Coder, to write its commands in real time (CERT-UA, medium confidence). GRU units share tools. Expect AI to speed Sandworm's reconnaissance and wiper development before it shows up in a public report.

So what. A wiper runs in minutes, so one number decides the outcome: the hours you need to rebuild Active Directory and restart the plant from clean images.

WHO CARES, AND THE DECISION EACH OWES

Owner	Why it matters	Decision they owe
Board	An outage brings regulators (NIS2 in Europe) and lost revenue.	Set the recovery-time target and fund it.
CISO and SOC	The wiper arrives through domain admin.	Monitor Group Policy and admin accounts around the clock.
OT engineering	The physical process is the target.	Keep manual operation drilled and offline images current.
CFO and legal	NotPetya victims fought insurers over war exclusions.	Check the policy's war and state-actor exclusions now.
Communications	Fronts claim first and exaggerate.	Hold a verified statement ready.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

RUSSIA · SANDWORM · WHAT TO DO, AND WHAT TO WATCH

THE PLAN ON ONE LINE: EACH ACTION, ITS OWNER, ITS DEADLINE



Bars run from today, October 29, 2026, to each deadline. Year-one cost, mid-size operator: $95K to $337K; Fortune tiers on page 15.

SIGNPOSTS TO WATCH

Signpost	Most likely meaning
Peace talks collapse, or allies approve a major new arms package for Ukraine	Raise the watch on allied energy and water for the following 90 days.
Telegram fronts post video of HMI screens from your country	Likely reconnaissance or a prelude to a claimed attack. Check exposed HMIs that day.
ESET or CERT-UA names a new wiper family	Pull the indicators and check Group Policy changes the same week.
Winter energy stress, December to February	Peak risk window; the Poland attack fell in late December. Finish the restore and rebuild tests before it opens.

WHAT TO DO, BY WHEN, AND WHAT IT COSTS

#	Action	Owner	By; mid-size cost
1	Keep offline, tested backups of domain controllers, HMIs and SCADA servers; run a full restore.	**IT and OT**	**Dec 15, 2026** **$40-140K**
2	Time a bare-metal rebuild of domain controllers and core OT servers. Target under 72 hours.	**CISO**	**Dec 31, 2026** **$15-45K**
3	Send the SOC an alert on any new or changed GPO and any domain-wide scheduled task.	**SOC**	**Nov 30, 2026** **$3-30K**
4	Remove internet exposure of HMIs and remote OT access; one controlled jump path.	**OT engineering**	**Dec 31, 2026** **$30-100K**
5	Review war and state-actor exclusions in the cyber insurance policy with the broker.	**CFO and legal**	**Jan 15, 2027** **$5-18K**
6	Draft a holding statement for a hacktivist claim; check with your ISAC first.	**Communications**	**Nov 30, 2026** **$2-4K**

WHICH EVIDENCE CARRIES WHICH JUDGMENT

	E1 A1	E2 B2	E3 A2	E4 B2	E5 A2	Direct
J1		●			○	1
J2		●	●	●		3
J3		○	○			0
J4	○	○				0

● direct support ○ indirect or partial blank: not relevant. Grades under each source: reliability and credibility. E5: also the AI section. J3 and J4 rest on indirect sources only: ESET's medium-confidence call, Denmark naming Russia but not the unit, and history.

EVIDENCE BEHIND THE JUDGMENTS

#	Source	Rel.	Cred.
E1	US indictment of six GRU officers, Oct 2020	**A**	**1**
E2	ESET on DynoWiper (attribution medium confidence) and APT Activity Report, Jan and May 2026	**B**	**2**
E3	Danish government attribution, Dec 18, 2025, via Euronews	**A**	**2**
E4	Mandiant on Telegram fronts and US water, via SC Media	**B**	**2**
E5	CERT-UA on LameHug, via BleepingComputer, Jul 2025	**A**	**2**

METHODS APPLIED

Analysis of competing hypotheses on the Poland attack: Sandworm, another GRU unit, or a criminal wiper; the malware overlap favors Sandworm, as ESET found. **Escalation ladder** from Ukraine to NATO soil. **Red team:** what does the GRU gain from a winter outage in an ally? Grades follow the ASA Evidence Standard, axes kept apart.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

NORTH KOREA

Famous Chollima: the IT worker scheme

Also tracked as Jasper Sleet (Microsoft), UNC5267 (Mandiant) and WageMole · Sponsor: DPRK state, under Reconnaissance General Bureau oversight · North Korea composite in The Adversary Index: 79 (Q3 2026) · Briefing date: October 29, 2026

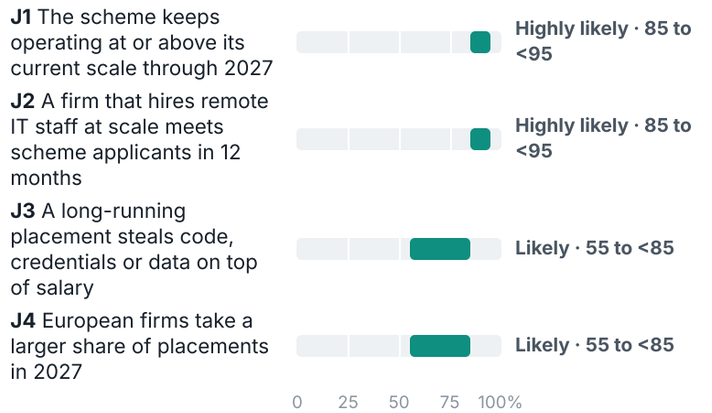
Bottom line. North Korea walks in through HR. Its operatives apply for jobs. They use stolen identities, AI-built résumés and real-time deepfake video to win remote IT jobs. Pay goes home. Access stays. Eleven governments warned on July 31, 2026 that deepfakes now beat live video interviews. UN monitors put the scheme's revenue at $250 million to $600 million a year, and the FBI disclosed in July that one operative had worked inside a US federal agency. Treadstone 71 assesses it highly likely that any organization hiring remote IT staff at scale meets scheme applicants in the next 12 months.

The decision. Move identity checks beyond the interview, which deepfakes now beat, and into the paycheck and the laptop, where a fake face buys nothing.

WHO

Thousands of IT workers posing as Americans and Europeans from China, Russia, Southeast Asia and Africa, run for the North Korean state and helped by "laptop farm" hosts in the US and elsewhere; France, Germany, Italy and the Netherlands joined the warning against them for the first time in July. CrowdStrike credits Famous Chollima with nearly half the state hands-on-keyboard intrusions it tracked at American technology companies in the year to March 2026.

JUDGMENTS, AS SHERMAN KENT BANDS (BAR = THE BAND'S RANGE)



WHAT THEY WANT FROM YOU

Salary first, as hard currency for weapons programs, then access: source code, credentials, crypto wallets, and data to sell or ransom. Researchers watching three hires inside a fake startup saw them run reconnaissance commands within hours of their first login.

$250-600M
Yearly IT worker revenue for Pyongyang (UN Panel of Experts and MSMT estimates)

47%
Share of state-sponsored hands-on intrusions against US tech firms, 12 months to March 2026 (CrowdStrike)

11
Governments behind the July 31, 2026 alert, four of them European newcomers

THE HIRING PIPELINE, AND WHO OWNS EACH GATE

1. Identity AI
stolen or synthetic; AI-edited ID
Gate: HR

2. Résumé AI
AI-written, AI-coached
Gate: HR

3. Interview AI
live deepfake face
Gate: HR

4. Laptop
shipped to a laptop farm
Gate: IT

5. Payroll
crypto or third-party account
Gate: Payroll

6. Access
code, credentials, data
Gate: SOC

Read left to right, top to bottom. The first three stages carry the AI. The last three, laptop, pay and access, are where checks bite; once hired, operatives still lean on chatbots for the job itself.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

NORTH KOREA · FAMOUS CHOLLIMA · HOW THEY GET IN, AND WHO CARES

HOW THEY GET IN, AND WHERE YOU STOP THEM

	THEIR MOVE	WHERE YOU STOP IT
1	Builds an identity from stolen or synthetic documents; AI edits the photos (one license carried Google's AI watermark).	**Stop:** Check IDs against independent records. Ignore candidate-supplied references.
2	Writes an AI-tailored résumé and rehearses with AI interview coaching.	**Stop:** Expect polished applicants. Polish proves nothing.
3	Passes the video interview behind a real-time deepfake face.	**Stop:** Add an unscheduled live call with a physical action: hand across the face, move rooms.
4	Has the laptop shipped to a US "laptop farm" and works through AnyDesk or an IP-KVM box.	**Stop:** Ship only to a verified home address. Alert on IP-KVM and remote-access tools.
5	Asks to be paid in crypto, by money transfer, or to a third-party account.	**Stop:** Match the bank account name to the ID before the first paycheck.
6	Uses the job to collect code, credentials and data.	**Stop:** Watch first-week behavior: system fingerprinting, location checks, personal account syncing.

WHERE NORTH KOREA'S OPERATORS USE AI, BY PUBLIC RECORD

Reconnaissance ONE REPORT	**Personas and phishing** DOCUMENTED
Influence content ONE REPORT	**Malware and code** DOCUMENTED
Identity fraud and deepfakes DOCUMENTED	**Autonomous AI agents** NO PUBLIC RECORD

State-level view from the overview matrix, wider than the cluster briefed.

AI IN THEIR PLAYBOOK

AI does most of its work at the front door: operatives use generative tools to forge and edit ID images, write résumés, coach interviews and, now, wear another face live on camera. Once hired, they use chatbots to do the actual coding job. Treadstone 71's May 2026 baseline placed North Korea last among the four in AI adoption, at 48 of 100; the July alert shows that adoption is concentrated in hiring fraud, where it works.

So what. Hiring is now an attack surface. HR and payroll hold the first line of defense. The SOC stands behind them. A firm that pays a scheme worker also risks a sanctions problem: US civil sanctions penalties apply on strict liability, so an unknowing hirer still carries exposure.

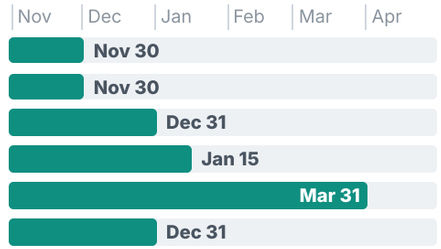
WHO CARES, AND THE DECISION EACH OWES

Owner	Why it matters	Decision they owe
HR and recruiting	The interview is where the deepfake works.	Add live, unscripted identity steps for remote IT roles.
Payroll and finance	The money trail is the scheme's purpose.	Verify account ownership before the first payment.
Legal and compliance	Paying a North Korean worker breaches sanctions.	Name the lawyer who takes the call on a suspected hire.
SOC	New hires act like intruders in week one.	Monitor new remote hires as closely as contractors.
Procurement	Staffing agencies and subcontractors hide the worker.	Write the same checks into agency contracts.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

NORTH KOREA · FAMOUS CHOLLIMA · WHAT TO DO, AND WHAT TO WATCH

THE PLAN ON ONE LINE: EACH ACTION, ITS OWNER, ITS DEADLINE



Bars run from today, October 29, 2026, to each deadline. Year-one cost, mid-size operator: $47K to $114K; Fortune tiers on page 15.

SIGNPOSTS TO WATCH

Signpost	Most likely meaning
A new hire logs in from two locations at once, or from an unexpected network	Possible relay through a laptop farm. Check before the next payroll run.
A candidate avoids unscheduled camera time or asks to change the delivery address	Classic scheme behavior. Pause the offer and verify in person.
A request to switch pay to crypto or a third-party account	The money leg of the scheme. Freeze the change and escalate to legal.
A new advisory or indictment names laptop-farm hosts in your country	Local infrastructure sits near you. Recheck the delivery address of every remote hire's laptop.

WHAT TO DO, BY WHEN, AND WHAT IT COSTS

#	Action	Owner	By; mid-size cost
1	Add an unscheduled live video step with a physical action, plus one in-person or notarized ID check, for remote IT hires.	**HR**	**Nov 30, 2026** **$10-20K/yr**
2	Match bank account names to IDs before first payroll; block crypto and third-party payment requests.	**Payroll**	**Nov 30, 2026** **$3-8K**
3	Ship laptops only to verified addresses; alert on IP-KVM, AnyDesk and Chrome Remote Desktop installs.	**IT and SOC**	**Dec 31, 2026** **$3-8K**
4	Review every remote IT hire of the past 24 months against the red flags here.	**HR and SOC**	**Jan 15, 2027** **$22-45K**
5	Put the same checks into staffing-agency and contractor agreements.	**Procurement**	**Mar 31, 2027** **$6-24K**
6	Agree an escalation path to sanctions counsel for a suspected hire.	**Legal**	**Dec 31, 2026** **$3-9K**

WHICH EVIDENCE CARRIES WHICH JUDGMENT

	E1 A2	E2 A2	E3 A2	E4 B2	E5 B2	E6 B2	Direct
J1	●	●	●		●		4
J2	●			○	●		2
J3	○		○	●			1
J4	●					○	1

● direct support ○ indirect or partial blank: not relevant. Grades under each source: reliability and credibility. E6: also the AI section. J4 rests on one direct source, the July alert.

EVIDENCE BEHIND THE JUDGMENTS

#	Source	Rel.	Cred.
E1	Eleven-nation joint alert, Jul 31, 2026, via TechTimes and CSA	**A**	**2**
E2	UN Panel of Experts and MSMT revenue estimates	**A**	**2**
E3	FBI disclosure of a federal-agency placement, Jul 2026, via CSA	**A**	**2**
E4	CSA research note on the honeypot startup, Aug 15, 2026	**B**	**2**
E5	CrowdStrike 47 percent figure, via TechTimes	**B**	**2**
E6	Treadstone 71 DPRK AI tradecraft baseline, May 2026	**B**	**2**

METHODS APPLIED

Chokepoint analysis of the hiring pipeline: each stage the operative must pass, and the cheapest control at each. **Red team:** how do we get one of our own people hired here under a false name? **Signposts** for HR, payroll and the SOC. Grades follow the ASA Evidence Standard, axes kept apart.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

IRAN

CyberAv3ngers

IRGC Cyber Electronic Command; US advisory aliases include Storm-0784, Bauxite, UNC5691, Hydro Kitten, APT Iran, Mr. Soul, Soldiers of Solomon and Shahid Kaveh Group · Iran composite in The Adversary Index: 77 (Q3 2026, up one) · Briefing date: October 29, 2026

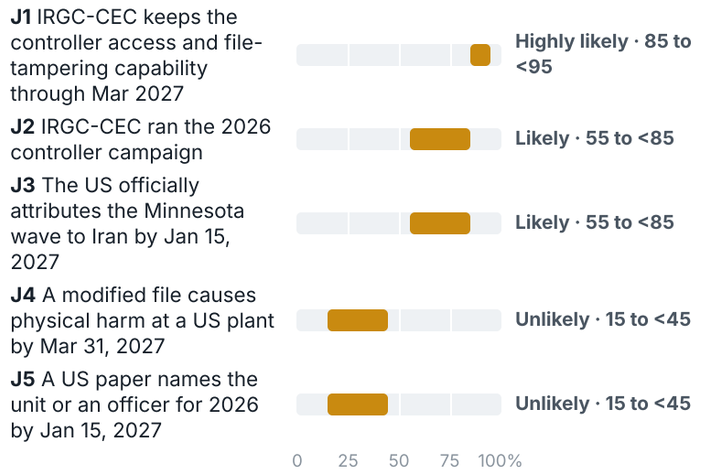
Bottom line. CyberAv3ngers defaced screens on water-plant controllers in 2023. In 2026, operators the US calls "Iranian-affiliated" rewrote the logic inside them. A US advisory describes a modified file at one victim that overrode safe limits and switched off alarms while the operator's screen read normal. Separately, Minnesota confirmed a coordinated attack on more than 30 water systems on July 26 and 27; the state fusion center found it aligned with the campaign, short of attribution. Washington has not named the unit for 2026. Persona claims, state-media relays and expert denials filled that gap all summer. Treadstone 71 assesses it highly likely that the IRGC keeps the capability through March 2027, and unlikely that it causes physical harm at a US plant in that window.

The decision. Take every controller off the open internet by mid-November, and check the logic inside your PLCs against a known-good copy before you trust the screen.

WHO

A state organ, run by the IRGC. Treasury designated six IRGC-CEC officers on February 2, 2024. On September 3, 2026, the State Department offered up to $10 million for Amir Yaryab, named as head of the Cyber Operations Command over CyberAv3ngers. The persona name itself changed hands in 2024 (likely), so a claim made under the name proves nothing. IRGC-run outlets never use the unit's name next to a US target.

JUDGMENTS, AS SHERMAN KENT BANDS (BAR = THE BAND'S RANGE)



WHAT THEY WANT FROM YOU

Retaliation and pressure in a war with the United States now in its eighth month, cheap and deniable: a boil-water notice in a US town is the effect, and fear and confusion are the point.

2023
Unitronics controllers in US water. At least 75 devices hit, 34 in water. Screens defaced. Treasury: no services disrupted.

→

2026
Rockwell, Schneider and Siemens controllers. Project files pulled and replaced. Safety logic overridden at one victim, alarms off, displays normal. Separately, Minnesota: 30+ systems; fusion center says aligned, not attributed.

CLAIM, FRAME, EFFECT, DENY: THE SUMMER 2026 SEQUENCE

JUN 12
Claim
Handala claims access to California water, says it held back

JUL 23
Frame
Tasnim calls the campaign a national achievement

JUL 26-27
Effect
30+ Minnesota water systems hit

JUL 28
Claim
Persona under the hijacked name claims Minnesota

JUL 29
Deny
Expert on Tasnim: water attacks break doctrine

AUG 1
Deny and threaten
Listed alias: reports are fake; threatens planted bombs

Claims run before and after the effect; denials and a threat follow; no official signs any of it. Verified fact (dark) and persona or state claims (light) never share a box.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

IRAN · CYBERAV3NGERS · HOW THEY GET IN, AND WHO CARES

HOW THEY GET IN, AND WHERE YOU STOP THEM

	THEIR MOVE	WHERE YOU STOP IT
1	Finds controllers and HMIs open to the internet; an AI agent turns intent into a target list in minutes (CloudSEK).	**Stop:** Find and disconnect every exposed PLC and HMI. Ask CISA for free scanning.
2	Connects with the vendor's own engineering software from rented foreign servers.	**Stop:** Block engineering-software ports from outside; allowlist integrator addresses.
3	Downloads the project file, adds instructions that override safe limits, and uploads it back.	**Stop:** Lock PLCs against program changes in RUN. Compare files to a known-good copy monthly.
4	Disables shutdown and alarm logic; the operator display reads normal.	**Stop:** Check safety-critical readings against field gauges by hand.
5	A persona claims or denies; state outlets relay; officials stay silent.	**Stop:** Do not amplify claims. Verify through WaterISAC or your sector ISAC.

WHERE IRAN'S OPERATORS USE AI, BY PUBLIC RECORD

- **Reconnaissance** — DOCUMENTED
- **Personas and phishing** — DOCUMENTED
- **Influence content** — DOCUMENTED
- **Malware and code** — DOCUMENTED
- **Identity fraud and deepfakes** — ONE REPORT
- **Autonomous AI agents** — NO PUBLIC RECORD

State-level view from the overview matrix, wider than the cluster briefed.

AI IN THEIR PLAYBOOK

An August 19 US advisory (AA26-231A) describes AI-generated exploitation scripts for Siemens S7 controllers, disguised as monitoring tools, and names no actor; Treadstone 71 holds the link to the same operators at a roughly even chance. Google reported Iranian groups as the heaviest state users of its Gemini model, for research and phishing content, and Iranian state outlets push AI-made video at scale. AI shortens the research phase most: an agent lists exposed US controllers with default passwords in under five minutes.

So what. Cheap attack. Small utility, thin staff. Physical effect. The fix is configuration: no exposed controllers, no default passwords, and a known-good copy of every program.

WHO CARES, AND THE DECISION EACH OWES

Owner	Why it matters	Decision they owe
Plant managers and operators	The screen lies when the logic is altered.	Add manual checks on safety-critical readings.
Utility board or council	Public safety and liability sit with them.	Fund the exposure fix now.
Communications	Personas claim and deny to sow confusion.	Hold a verified statement; never repeat a persona claim.
Integrators and vendors	Their remote access is a common path.	Require allowlisted, logged access in contracts.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

IRAN · CYBERAV3NGERS · WHAT TO DO, AND WHAT TO WATCH

THE PLAN ON ONE LINE: EACH ACTION, ITS OWNER, ITS DEADLINE



Bars run from today, October 29, 2026, to each deadline. Year-one cost, mid-size operator: $55K to $184K; Fortune tiers on page 15.

SIGNPOSTS TO WATCH

Signpost	Most likely meaning
A US advisory, indictment or Treasury action names IRGC-CEC for 2026 activity	Attribution moves to highly likely; expect sanctions and a tit-for-tat cycle.
A state or federal finding of physical harm from a modified file	Escalation has begun. Treat every unverified program change as an incident.
A listed alias claims a US effect instead of denying one	Tehran has decided to own an effect. Expect a pretext already published.
Renewed large-scale US strikes on Iran (Treadstone 71: roughly even by Nov 30, likely by Jan 15)	The retaliation window opens within days. Expect a Handala claim, then the claim-and-deny cycle. Pull exposure deadlines forward.
A planted-bombs threat or water claim timed to the November 3 midterms	Influence aimed at the vote. Route threats to law enforcement; say nothing until WaterISAC verifies.

WHAT TO DO, BY WHEN, AND WHAT IT COSTS

#	Action	Owner	By; mid-size cost
1	Find every PLC and HMI reachable from the internet and disconnect it or put it behind a gateway.	**OT engineering**	**Nov 15, 2026** **$20-85K**
2	Change default passwords; set PLCs to block program changes while running.	**OT engineering**	**Nov 15, 2026** **$5-15K**
3	Pull current project files and compare them to a known-good copy; repeat monthly.	**OT engineering**	**Dec 15, 2026** **$15-30K/yr**
4	Each week, compare safety-critical readings with local gauges by hand.	**Operators**	**Weekly** **$10-40K/yr**
5	Close engineering-software ports to the internet; permit only known integrator addresses.	**IT and OT**	**Nov 30, 2026** **$3-10K**
6	Prepare statements for a persona claim; verify with WaterISAC before you comment.	**Communications**	**Nov 30, 2026** **$2-4K**

WHICH EVIDENCE CARRIES WHICH JUDGMENT

	E1 A1	E2 A1	E3 B2	E4 B2	E5 F3	Direct
J1	●	○				1
J2	○	○		○		0
J3		○	●			1
J4	●		○			1
J5	●	○				1

● direct support ○ indirect or partial blank: not relevant. Grades under each source: reliability and credibility. E4: AI section · E5: Who section. J2 rests on inference only: no A1 source names the unit for 2026, so the judgment stops at likely.

EVIDENCE BEHIND THE JUDGMENTS

#	Source	Rel.	Cred.
E1	US joint advisories AA26-097A (updated Jul 22) and AA26-231A (Aug 19), 2026	**A**	**1**
E2	Treasury designation, Feb 2, 2024; State reward offer, Sep 3, 2026	**A**	**1**
E3	Minnesota IT Services; WaterISAC memo via Nextgov, Jul 2026	**B**	**2**
E4	Recorded Future Insikt Group, Jul 16, 2026	**B**	**2**
E5	Two Persian exposé channels on the hijacked name	**F**	**3**

METHODS APPLIED

Drawn from Treadstone 71 Public Attribution Series Unit Note 01. **Analysis of competing hypotheses** on who ran 2026. **Adversarial Cognitive Simulator** on the claim-and-deny sequence. **Forensic linguistics** on the persona denials. **Cone of plausibility** through March 31, 2027. Grades follow the ASA Evidence Standard, axes kept apart.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

STRATEGIC FORESIGHT

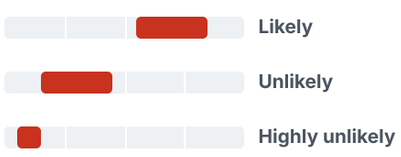
Looking Ahead: Through December 2027

Forecasts extend the judgments in each briefing past the January 15, 2027 refresh of The Adversary Index. Scenario bands per actor are mutually exclusive and run the same Sherman Kent scale.

China · Volt Typhoon stays quiet and stays in.

Treadstone 71 assesses it likely (55 to <85) that pre-positioning and collection continue below the armed-conflict line through 2027. The PLA's 2027 modernization benchmark sets the clock. A visible cyber effect paired with a Taiwan exercise, coercion meant to be seen, is unlikely (15 to <45). Wartime activation against US lifeline sectors is highly unlikely (5 to <15) and turns on a blockade. AI changes the speed. The aim holds. Treadstone 71 judges it likely that Chinese pre-positioning teams adopt agent tooling like the kit used against Taiwan's government network by the end of 2027. Watch for a Taiwan exercise that arrives with an outage.

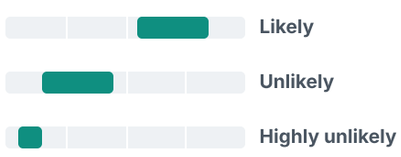
SCENARIOS THROUGH DECEMBER 2027



North Korea · The scheme grows and moves west.

Treadstone 71 holds it highly likely (85 to <95) that the IT worker scheme runs at or above today's scale through 2027, and likely (55 to <85) that Europe's share of placements rises. A pivot from salary to extortion as the main revenue is unlikely (15 to <45). Enforcement that shrinks the scheme is highly unlikely (5 to <15) while laptop-farm hosts keep turning up. AI sets the pace. Real-time deepfakes already beat the interview. A documented hire run end to end by an AI persona, with no operator on camera, stands at a roughly even chance (45 to <55) by the end of 2027. Watch for European indictments of laptop-farm hosts.

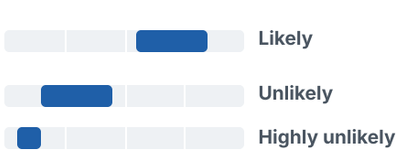
SCENARIOS THROUGH DECEMBER 2027



Russia · Russia keeps testing NATO's lifelines.

Treadstone 71 assesses it likely (55 to <85) that GRU units and their fronts keep probing European energy and water through 2027, most attempts failing or staying small, as in Poland and Denmark. One successful cyber outage on NATO soil is unlikely (15 to <45). A ceasefire that cuts the tempo is highly unlikely (5 to <15); sabotage pressure has outlived every lull since 2014. Winter and arms-package votes set the rhythm. AI arrives through the GRU's shared toolkit. A model-driven wiper or loader in a destructive attack by the end of 2027 stands at a roughly even chance (45 to <55), building on APT28's LameHug. Watch for fronts posting HMI video from a new country.

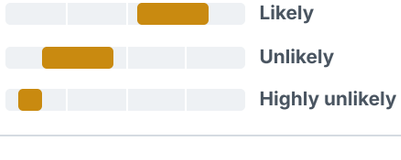
SCENARIOS THROUGH DECEMBER 2027



Iran · Iran's OT campaign rides the war.

Treadstone 71 assesses it likely (55 to <85) that controller intrusions in water, energy and fuel come in bursts that track US strikes through 2027, each wrapped in claims and denials. Renewed large-scale US strikes by January 15 are likely and open the next window. Physical harm at a US plant through 2027 is unlikely (15 to <45). A settlement that halts the campaign is highly unlikely (5 to <15) while the war runs and Mojtaba Khamenei consolidates power. AI lowers the bar. An agent builds a target list in minutes, so more small utilities enter the pool. Watch for the first government paper that names the unit for 2026.

SCENARIOS THROUGH DECEMBER 2027



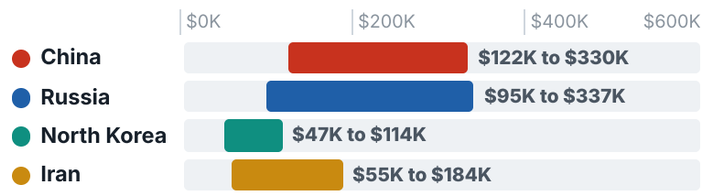
Across the four. Every adversary here uses AI to run an old attack faster. Through 2027 the race that matters is time: how fast an adversary finds exposed equipment against how fast you remove it. The plans in each briefing shorten your side of that race for under a million dollars in year one at a mid-size operator, all four plans together.

YEAR ONE, ALL FOUR PLANS, BY COMPANY SIZE

Organization	Estimate
Mid-size	**$320K-960K**
Fortune 501-1000	**$990K-6.7M**
Fortune 101-500	**$2.9M-25M**
Fortune 1-100	**$10M-85M**

Treadstone 71 estimates. Per-action figures on page 15; cost of doing nothing on page 16; basis on page 17.

YEAR ONE BY PLAN, MID-SIZE OPERATOR



Bars show the low-to-high range for the six actions in each plan.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

COST MODEL

What the Plans Cost, by Company Size

Year-one estimates for the six actions in each briefing, from a mid-size operator to the Fortune 100. Ranges run low to high; /yr marks a recurring cost. Tier definitions, labor rates, method and exclusions: Cost Model Basis, page 17. The cost of doing nothing: page 16.

CHINA · VOLT TYPHOON

Action	Mid-size	F501-1000	F101-500	F1-100
1 Management consoles off the internet, MFA	$20K-55K	$83K-460K	$260K-1.8M	$1.1M-6.0M
2 Patch the five platforms	$5K-15K	$21K-130K	$65K-490K	$270K-1.6M
3 12-month log retention	$20K-65K/yr	$83K-680K/yr	$330K-2.8M/yr	$1.3M-11M/yr
4 Hunt 12 months of logs	$25K-90K	$78K-560K	$220K-2.0M	$690K-5.9M
5 72-hour manual-operations drill	$50K-100K	$100K-420K	$220K-1.1M	$550K-3.3M
6 Board brief, outage tolerance	$2K-5K	$3K-10K	$4K-16K	$7K-27K
Plan total, year one	**$120K-330K**	**$370K-2.3M**	**$1.1M-8.1M**	**$3.9M-28M**

RUSSIA · SANDWORM

Action	Mid-size	F501-1000	F101-500	F1-100
1 Offline backups, full restore	$40K-140K	$170K-1.2M	$520K-4.6M	$1.8M-15M
2 Timed bare-metal rebuild	$15K-45K	$31K-190K	$65K-490K	$160K-1.5M
3 GPO and task alerting	$3K-30K	$6K-130K	$10K-260K	$20K-490K
4 HMI exposure, one jump path	$30K-100K	$94K-830K	$330K-3.3M	$990K-11M
5 Insurance exclusion review	$5K-18K	$11K-65K	$19K-140K	$37K-260K
6 Holding statement	$2K-4K	$3K-8K	$4K-13K	$7K-22K
Plan total, year one	**$95K-340K**	**$310K-2.4M**	**$940K-8.7M**	**$3.0M-29M**

NORTH KOREA · FAMOUS CHOLLIMA

Action	Mid-size	F501-1000	F101-500	F1-100
1 Live video step and ID check	$10K-20K/yr	$31K-130K/yr	$87K-520K/yr	$440K-2.6M/yr
2 Payroll account matching	$3K-8K	$9K-50K	$26K-210K	$130K-1.1M
3 Laptop shipping, remote-tool alerts	$3K-8K	$6K-33K	$10K-69K	$20K-130K
4 Review 24 months of remote hires	$22K-45K	$69K-280K	$190K-1.2M	$970K-5.9M
5 Agency and contractor clauses	$6K-24K	$13K-87K	$23K-180K	$44K-350K
6 Sanctions escalation path	$3K-9K	$6K-32K	$11K-68K	$22K-130K
Plan total, year one	**$47K-110K**	**$140K-610K**	**$350K-2.2M**	**$1.6M-10M**

IRAN · CYBERAV3NGERS

Action	Mid-size	F501-1000	F101-500	F1-100
1 Exposed PLCs and HMIs off the internet	$20K-85K	$63K-710K	$220K-2.8M	$660K-9.3M
2 Default passwords, run-mode lock	$5K-15K	$16K-130K	$54K-490K	$160K-1.6M
3 Project-file comparison	$15K-30K/yr	$47K-250K/yr	$160K-980K/yr	$490K-3.3M/yr
4 Weekly manual readings	$10K-40K/yr	$31K-330K/yr	$110K-1.3M/yr	$330K-4.4M/yr
5 Engineering ports closed	$3K-10K	$6K-42K	$10K-87K	$20K-160K
6 Persona-claim statements	$2K-4K	$3K-8K	$4K-13K	$7K-22K
Plan total, year one	**$55K-180K**	**$170K-1.5M**	**$560K-5.6M**	**$1.7M-19M**

All four plans, year one	Mid-size	F501-1000	F101-500	F1-100
Combined estimate	**$320K-960K**	**$990K-6.7M**	**$2.9M-25M**	**$10M-85M**

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

COST OF DOING NOTHING

What Inaction Costs, by Company Size

The loss if each adversary's signature event lands, its annual chance with no plan in place, the expected loss a year, and the years of the plan one event pays for.

CHINA · ACCESS FOUND OR USED: FORENSIC EVICTION, REBUILD OF THE MANAGEMENT PLANE, UP TO THREE DAYS OF DEGRADED OPERATIONS.

	Mid-size	F501-1000	F101-500	F1-100
Loss if it lands	$3.0M-12M	$8.0M-30M	$20M-80M	$50M-200M
Annual chance, no plan	Unlikely, 15 to <45 percent, every tier			
Expected loss a year	**$450K-5.4M**	**$1.2M-14M**	**$3.0M-36M**	**$7.5M-90M**
Plan cost, year one	$120K-330K	$370K-2.3M	$1.1M-8.1M	$3.9M-28M
Years of plan, one event	**30 years**	**17 years**	**13 years**	**10 years**

RUSSIA · WIPER ACROSS IT AND OT: ONE TO THREE WEEKS OF REBUILD AND LOST OUTPUT, THE NOTPETYA PATTERN.

	Mid-size	F501-1000	F101-500	F1-100
Loss if it lands	$10M-35M	$30M-120M	$100M-400M	$250M-1.0B
Annual chance, no plan	Highly unlikely, 5 to <15 percent, every tier			
Expected loss a year	**$500K-5.2M**	**$1.5M-18M**	**$5.0M-60M**	**$12M-150M**
Plan cost, year one	$95K-340K	$310K-2.4M	$940K-8.7M	$3.0M-29M
Years of plan, one event	**105 years**	**70 years**	**70 years**	**54 years**

NORTH KOREA · SCHEME WORKER PLACED, THEN FOUND: INVESTIGATION, DATA THEFT OR EXTORTION, SANCTIONS EXPOSURE.

	Mid-size	F501-1000	F101-500	F1-100
Loss if it lands	$1.0M-6.0M	$3.0M-15M	$5.0M-40M	$10M-80M
Annual chance, no plan	Unlikely, 15 to <45 percent, every tier			
Expected loss a year	**$150K-2.7M**	**$450K-6.8M**	**$750K-18M**	**$1.5M-36M**
Plan cost, year one	$47K-110K	$140K-610K	$350K-2.2M	$1.6M-10M
Years of plan, one event	**33 years**	**23 years**	**16 years**	**7 years**

IRAN · ALTERED CONTROLLER LOGIC: PLANT DOWN FOR DAYS, SAFETY RESPONSE, REGULATOR AND PUBLIC SCRUTINY. OT OPERATORS ONLY.

	Mid-size	F501-1000	F101-500	F1-100
Loss if it lands	$1.0M-8.0M	$3.0M-25M	$10M-60M	$20M-150M
Annual chance, no plan	Unlikely, 15 to <45 percent, every tier			
Expected loss a year	**$150K-3.6M**	**$450K-11M**	**$1.5M-27M**	**$3.0M-68M**
Plan cost, year one	$55K-180K	$170K-1.5M	$560K-5.6M	$1.7M-19M
Years of plan, one event	**28 years**	**18 years**	**14 years**	**10 years**

ALL FOUR PLANS AGAINST ALL FOUR THREATS, PER YEAR (LOG SCALE)



Method. Expected annual loss equals the loss if the event lands times its annual chance with no plan in place (annualized loss expectancy). The chance uses the low and high ends of a Sherman Kent band; larger firms present more targets and sit toward the top of each band. Losses scale with each tier's revenue per day and the share of operations a single event reaches. **Anchors.** US average breach cost $10.22 million (IBM, 2025). NotPetya losses in 2017: Maersk $200 to $300 million, Mondelez about $150 million, Reckitt about $130 million, Saint-Gobain about $387 million. Unplanned downtime costs a large automotive plant $2.3 million an hour and the Global 500 about 11 percent of revenue a year (Siemens, 2024). IEEPA civil penalties run to $377,700 per violation or twice the transaction, and every payroll run to a North Korean worker counts. **Left out:** ransom payments, share-price loss, litigation beyond sanctions, and harm to people. Treadstone 71 estimates, built for a board conversation, not an actuarial model.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

ENDNOTE

Cost Model Basis

The reference organizations, rates and method behind every cost figure in the briefings.

REFERENCE ORGANIZATION FOR EACH TIER

Assumption	Mid-size	F501-1000	F101-500	F1-100
Annual revenue	Under $2.5B	About $2.5B to $7.5B	$7.5B to about $45B	About $45B and up
Employees	About 1,000	5,000 to 15,000	15,000 to 60,000	60,000 to 500,000+
Sites; OT sites	3 to 5; 3 to 5	10 to 30; 10 to 30	30 to 150; 30 to 150	150 to 1,000+; 100 to 1,000
Privileged admins	50	150 to 300	400 to 1,200	1,500 to 5,000
Internet-facing assets	About 150	600 to 1,200	1,800 to 4,500	7,500 to 18,000
Remote IT hires a year	About 50	150 to 300	400 to 1,200	2,000 to 6,000
Internal labor, loaded	$110/hr	$125/hr	$140/hr	$150/hr
Outside specialists	$225/hr	$250/hr	$275/hr	$300/hr
Outside counsel	$450/hr	$650/hr	$850/hr	$1,100/hr
Volume discount on technology	None	10%	20%	30%

COST DRIVERS: GROWTH OVER THE MID-SIZE OPERATOR

Cost driver	Actions	F501-1000	F101-500	F1-100
Internet-facing assets	CH1, CH2	x4 to 8	x12 to 30	x50 to 100
Log volume	CH3	x4 to 10	x15 to 40	x60 to 150
Hunt scope	CH4	x3 to 6	x8 to 20	x25 to 60
Sites in a drill	CH5, RU2	x2 to 4	x4 to 10	x10 to 30
Governance hours	CH6, RU6, IR6	x1.5 to 2	x2 to 3	x3 to 5
Servers to back up	RU1	x4 to 8	x12 to 30	x40 to 100
Engineering hours	RU3, NK3, IR5	x2 to 4	x3 to 8	x6 to 15
OT sites	RU4, IR1, IR2, IR3, IR4	x3 to 8	x10 to 30	x30 to 100
Remote IT hires	NK1, NK2, NK4	x3 to 6	x8 to 24	x40 to 120
Counsel hours	RU5, NK5, NK6	x1.5 to 2.5	x2 to 4	x3 to 6

METHOD AND LIMITS

1. Every tier starts with a working SIEM, EDR and identity provider. Costs cover the six actions in each plan and nothing else.
2. Method: each action ties to one cost driver from the table at left, such as internet-facing assets, log volume, OT sites, remote hires or counsel hours. Fortune-tier figures scale the mid-size estimate by that driver's growth, weight labor at 60 percent and technology at 40 percent, then apply the tier's labor rates and volume discount.
3. Technology uses 2026 list-price ranges for hardware security keys, log storage, jump hosts, immutable backup and OT gateways.
4. Excluded: incident response and recovery costs, replacement of legacy controllers, regulatory fines and insurance premiums.
5. OT lines apply only to firms that run plants or field equipment; a bank or software firm in the Fortune 100 drops them. A small water utility, Iran's usual target, needs a fraction of the mid-size Iran figure once it uses CISA's free scanning and WaterISAC guidance.
6. Revenue bands follow the 2026 Fortune 500 cutoff of $7.5 billion; the Fortune 100 and Fortune 1000 boundaries are approximate. Employee and asset counts are Treadstone 71 planning assumptions.
7. Treadstone 71 planning estimates, not vendor quotes. Validate rates and counts against the organization's own contracts before a budget request.
8. The cost of doing nothing, page 16, uses the same tiers; its method and loss anchors sit on that page.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.

Sources

- Lumen Black Lotus Labs on Silent Train, reported by Security Affairs, October 29, 2026: securityaffairs.com/202023
- Dream research on AI agents against a government network, reported by Security Affairs citing the Financial Times, August 12, 2026: securityaffairs.com/197079
- NSA, CISA, FBI and Five Eyes partners, Volt Typhoon advisories AA23-144A, AA24-038A and related fact sheets, 2023 to 2024
- ESET Research, Sandworm and the cyberattack on Poland's power grid, January 23, 2026, updated January 30, 2026; ESET APT Activity Report Q4 2025 to Q1 2026, May 28, 2026
- US Department of Justice, indictment of six GRU Unit 74455 officers, October 19, 2020
- Euronews, Denmark blames Russia for cyberattacks on water utility and election websites, December 19, 2025
- SC Media, US and European water utility attacks linked to Sandworm, citing Mandiant
- BleepingComputer, LameHug malware uses an LLM to write data-theft commands, July 17, 2025, citing CERT-UA
- TechTimes, North Korean IT workers use real-time deepfakes to beat hiring checks, eleven nations warn, August 2, 2026
- Cloud Security Alliance, DPRK IT worker infiltration research note, August 15, 2026
- Joint statement on DPRK IT workers, July 31, 2026, Australian Department of Foreign Affairs and Trade: dfat.gov.au; UN Panel of Experts and Multilateral Sanctions Monitoring Team revenue estimates; OFAC Economic Sanctions Enforcement Guidelines (strict liability)
- CISA and partners, AA26-097A (April 7, 2026, updated July 22, 2026) and AA26-231A (August 19, 2026); US Treasury designation of IRGC-CEC officers, February 2, 2024; State Department Rewards for Justice, September 3, 2026
- Minnesota IT Services statement on community water systems, July 2026; WaterISAC memo carrying the Minnesota Fusion Center finding, reported by Nextgov, July 31, 2026
- CloudSEK, AI, the Iran-US conflict, and the threat to US critical infrastructure, 2026
- Google Threat Intelligence Group, Adversarial misuse of generative AI, January 2025
- Two Persian-language Telegram exposé channels on the CyberAv3ngers name (August 2024; July 2025 to August 2026), graded F3, as cited in Unit Note 01
- Recorded Future Insikt Group, AI has enhanced Iran's asymmetric playbook during the 2026 conflict, July 16, 2026
- Treadstone 71: The Adversary Index Q3 2026 Tier 0 edition (October 5, 2026); Volt Typhoon, Sandworm, Lazarus umbrella and CyberAv3ngers cluster annexes (May 2026); DPRK AI Tradecraft Deep Dive (May 2026); Public Attribution Series Unit Note 01, CyberAv3ngers (October 2026)

Limits of the briefings

Every source is open. No classified or client material appears. Placements on the overview chart are analytic judgments for a generic infrastructure operator in the US or an allied country; a specific organization's exposure depends on its sector, footprint and suppliers. Dates for actions run from October 29, 2026. Iran judgments on physical harm cover US plants only; The Adversary Index rates Gulf hosts of US forces as elevated, and no band here covers European, Gulf or Asia-Pacific operators. Cost estimates on page 15 assume reference organizations at four sizes; a real site needs its own quote. Judgments hold until the signposts in each briefing fire; Treadstone 71 revisits them at the January 15, 2027 refresh of The Adversary Index.

Copyright and trademark

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC. Released TLP:CLEAR: short excerpts are free to quote with attribution to Treadstone 71, LLC. Any other reproduction, distribution or derivative use needs written permission. www.treadstone71.com

How to read the judgments

Probability follows the Sherman Kent spectrum with half-open intervals: almost certain 95 to 99, highly likely 85 to <95, likely 55 to <85, roughly even 45 to <55, unlikely 15 to <45, highly unlikely 5 to <15, almost no chance 1 to <5. Each source carries two grades under the ASA Evidence Standard, Public Edition 1.2: reliability of the source, A to F, and credibility of the information, 1 to 6. The two are never averaged. Verified fact and adversary claim never share a sentence.

© 2026 Treadstone 71, LLC. All rights reserved. TREADSTONE 71® is a registered trademark of Treadstone 71, LLC.