STRIDER

INSIDE THE SHADOW NETWORK

North Korean IT Workers and Their PRC Backers

TABLE OF CONTENTS

Page 3 > Executive Summary

Page 4 > Introduction

Page 6 > Tactics, Techniques, and Procedures

Page 8 > Risks to Western Businesses

Page 10 > North Korean IT Workers Abroad

Page 12 > The Role of PRC-Based Entities

Page 14 > Conclusion

EXECUTIVE SUMMARY

Using Strider's proprietary risk methodology and open-source data collection, this report details the tactics, techniques, and procedures (TTPs) used by DPRK actors, including the use of fake identities, front companies, and exploitation of global freelancing platforms. This report also maps the geographic spread of North Korean IT workers across China, Russia, Southeast Asia, Africa, and the Middle East, and highlights the role of PRC-based entities like Liaoning China Trade Industry Co., Ltd., which was recently sanctioned for materially supporting DPRK cyber operations.

Using Checkpoint, Strider's proprietary third-party due diligence tool, Strider identified 35 affiliated organizations tied to a sanctioned entity—information that can help companies avoid unwittingly enabling DPRK-linked activity. To mitigate risk, businesses should adopt stronger due diligence processes, enforce compliance with sanctions, and remain vigilant against increasingly sophisticated threats emerging from global talent pipelines.

INTRODUCTION

Amid the growing demand for technical talent and the rise of remote work, a less visible threat has emerged within global hiring networks. North Korean IT professionals, operating under false or stolen identities, have successfully secured work with companies across the U.S. and other Western nations. These individuals, often posing as freelance developers or engineers, **are part of a strategic state-directed effort to access sensitive information, advance geopolitical goals, and generate revenue for the Democratic People's Republic of Korea (DPRK)**—funds that are then used to support prohibited weapons programs and evade international sanctions. Western businesses risk financial losses, intellectual property theft, data breaches, and reputational damages should they hire any fraudulent worker—but the risk is especially great should they hire an individual from the DPRK.

On December 12, 2024, the U.S. Department of Justice unveiled indictments against **14 North Korean nationals for orchestrating an expansive fraud campaign that spanned years and continents.** The individuals, posing as remote contractors, infiltrated hundreds of businesses by disguising their true identities—sometimes even impersonating real people—to secure employment, steal funds, and funnel revenues directly to Pyongyang. According to the U.S. Department of the Treasury, up to 90 percent of their earnings were used by the DPRK government to bankroll its weapons of mass destruction (WMD) and ballistic missile programs.

By January 2025, the U.S. government intensified its crackdown. The Treasury Department's Office of Foreign Assets Control (OFAC) issued sanctions targeting multiple individuals and entities involved in this scheme, further highlighting the extent to which Western companies have unknowingly become conduits for DPRK state-sponsored activities. Just days later, the FBI and Department of Justice reinforced the gravity of the threat with another round of indictments and public service announcements, warning that hiring North Korean IT workers could result in stolen intellectual property, data breaches, and direct violations of U.S. and UN sanctions.

These schemes are not carried out in isolation. Many of the operations detailed in U.S. government indictments and sanctions involve facilitators and front companies based in the People's Republic of China (PRC), where North Korean operatives often reside and access the global internet. Chinese-based intermediaries have played a crucial role in enabling the DPRK's use of digital platforms, payment systems, and employment marketplaces—creating a cross-border infrastructure that helps obscure the origins of the workers and facilitates the laundering of illicit proceeds.

In a world increasingly reliant on remote work and globalized talent pools, the line between innovation and infiltration has never been thinner.

This report explores how North Korean IT operatives penetrate digital workforces, the systemic vulnerabilities they exploit, and the strategic, legal, and reputational risks Western businesses now face.

TACTICS, TECHNIQUES, AND PROCEDURES

North Korean IT workers use a variety of tactics, techniques, and procedures (TTPs) to achieve their objectives. These TTPs are sophisticated and designed to obfuscate their true origins and intentions, making them difficult to detect and mitigate.

Disguised Identities and Front Companies

One of the primary tactics employed by North Korean IT workers is the use of fake identities and front companies. These individuals often operate under aliases and use forged documents to gain employment in foreign firms. In many cases, they establish front companies that appear to be legitimate IT services firms. These companies serve as a cover for their operations, allowing them to interact with global clients without raising suspicion.

One reported example is Danish electric car company Fisker, who unknowingly hired a North Korean IT worker in 2022. The remote worker, Kou Thao, listed his address as a house in Arizona. However, that house actually belonged to a woman named Christina Chapman, who had been running a laptop farm in service of and funneling paychecks back to the DPRK. Fisker terminated the employee after being notified by the FBI in 2023.

In another example, crypto company Kraken identified a North Korean operative who had applied for a remote IT job using the same email address that had been flagged by the FBI as being a suspected DPRK operative.

Exploitation of Freelancing Platforms

North Korean IT workers sometimes use online freelancing platforms such as Upwork, Freelancer, and Fiverr. These platforms provide an anonymous way to offer IT services to global clients. By bidding on projects from Western companies, these workers can earn hard currency for the DPRK regime while gaining access to potentially sensitive information. The anonymity of these platforms makes it challenging to trace the true identity of the workers.

Cybercrime and Ransomware

Some North Korean workers are involved in cybercrime activities. This includes the deployment of ransomware, phishing attacks, and hacking. These operations are often coordinated with DPRK state-sponsored hacking groups like the Lazarus Group. The proceeds from these cybercrimes are funneled back to the DPRK regime, helping to fund its nuclear and missile programs.

Software and App Development

A significant portion of North Korean IT workers abroad are engaged in software and app development. They create applications that are marketed to global audiences, often under the banner of foreign companies. These apps can sometimes include malicious code that allows North Korean operatives to conduct surveillance or steal data from users. The revenue generated from these apps also contributes to the regime's coffers.

Manipulation of Cryptocurrency Markets

The DPRK has shown a growing interest in cryptocurrencies to evade international sanctions. IT workers are involved in the manipulation of cryptocurrency markets, including the use of malware to mine cryptocurrencies, hacking of exchanges, and participation in initial coin offerings under false pretenses.

RISKS TO WESTERN BUSINESSES

The activities of North Korean IT workers pose several significant risks to Western businesses. These risks are not limited to direct financial losses but extend to broader issues such as intellectual property theft, data breaches, and reputational damage.

01 Regulatory and Legal Risks

Western businesses that unknowingly engage with North Korean IT workers may find themselves in violation of international sanctions. These sanctions are designed to isolate the DPRK regime and cut off its access to global financial systems. Companies found to be in violation of these sanctions can face hefty fines, legal action, and restrictions on their ability to operate internationally.

02 Reputational Damage

The association with North Korean IT workers can lead to reputational damage for Western businesses. If it is discovered that a company has inadvertently hired North Korean operatives, even through legitimate channels like freelancing platforms, the company could face public backlash and potential legal consequences. This risk is particularly acute for firms operating in sensitive industries such as defense, finance, and technology.

03 Intellectual Property Theft

By embedding themselves in legitimate IT projects, these workers can gain access to proprietary software, trade secrets, and other forms of intellectual property. This stolen intellectual property can be used to advance the DPRK's technological capabilities or sold to third parties, including hostile nation states and criminal organizations.

04 Data Breaches and Espionage

North Korean IT workers are often involved in projects that provide access to sensitive data. This data can include personal information, financial records, and corporate secrets. The workers can exfiltrate this data and transmit it back to the DPRK, where it can be used for espionage purposes. The data can also be sold on the dark web, leading to significant financial and reputational damage for the affected companies.

05 Financial Losses from Cybercrime

Western businesses are increasingly targeted by cybercrime activities linked to North Korean IT workers. Ransomware attacks, in particular, have become a significant threat. These attacks can result in substantial financial losses, both from the ransom payments and the costs associated with recovering from the attack. The involvement of North Korean IT workers in these activities adds an additional layer of complexity, as the proceeds are used to fund a hostile regime.

To mitigate these risks, Western businesses must be vigilant in their hiring practices, particularly when engaging with freelancers or third-party IT service providers. Enhanced due diligence, robust cybersecurity measures, and adherence to international sanctions are crucial in protecting against the threats posed by North Korean IT workers.

NORTH KOREAN IT WORKERS ABROAD

Many North Korean IT workers are dispatched abroad—particularly to countries like the PRC, Russia, parts of Southeast Asia, Africa, and the Middle East—where they work under front companies or use aliases. By understanding where these hubs are located, organizations can prioritize deeper vetting for vendors, freelancers, or subcontractors operating from these regions.

People's Republic of China

The PRC's vast digital economy and close geographical proximity to the DPRK make it an ideal base of operations for North Korean IT workers. They often operate in major cities like Dalian, Shenyang, and Beijing. They are typically employed by PRC firms or joint ventures, sometimes even setting up front companies. These IT workers exploit the relatively lax regulatory environment to engage in cyber activities, often targeting Western companies.

Russian Federation

Russia, particularly the Far Eastern regions, hosts a substantial number of North Korean IT professionals. Russia's complex relationship with the West and its challenges with international sanctions make it a conducive environment for North Korean operatives. These workers often secure employment in Russian tech firms or collaborate with Russian cybercriminal networks. The Russian government's increasingly close relationship with the DPRK provides a degree of protection and operational freedom for these workers.

Africa and the Middle East

North Korean IT workers also operate in countries like Nigeria, Kenya, and the United Arab Emirates. In these regions, they often engage in activities ranging from software development to more nefarious cyber activities like hacking and ransomware deployment. These workers take advantage of the limited cybersecurity infrastructure in these regions to operate with relative impunity.

Southeast Asia

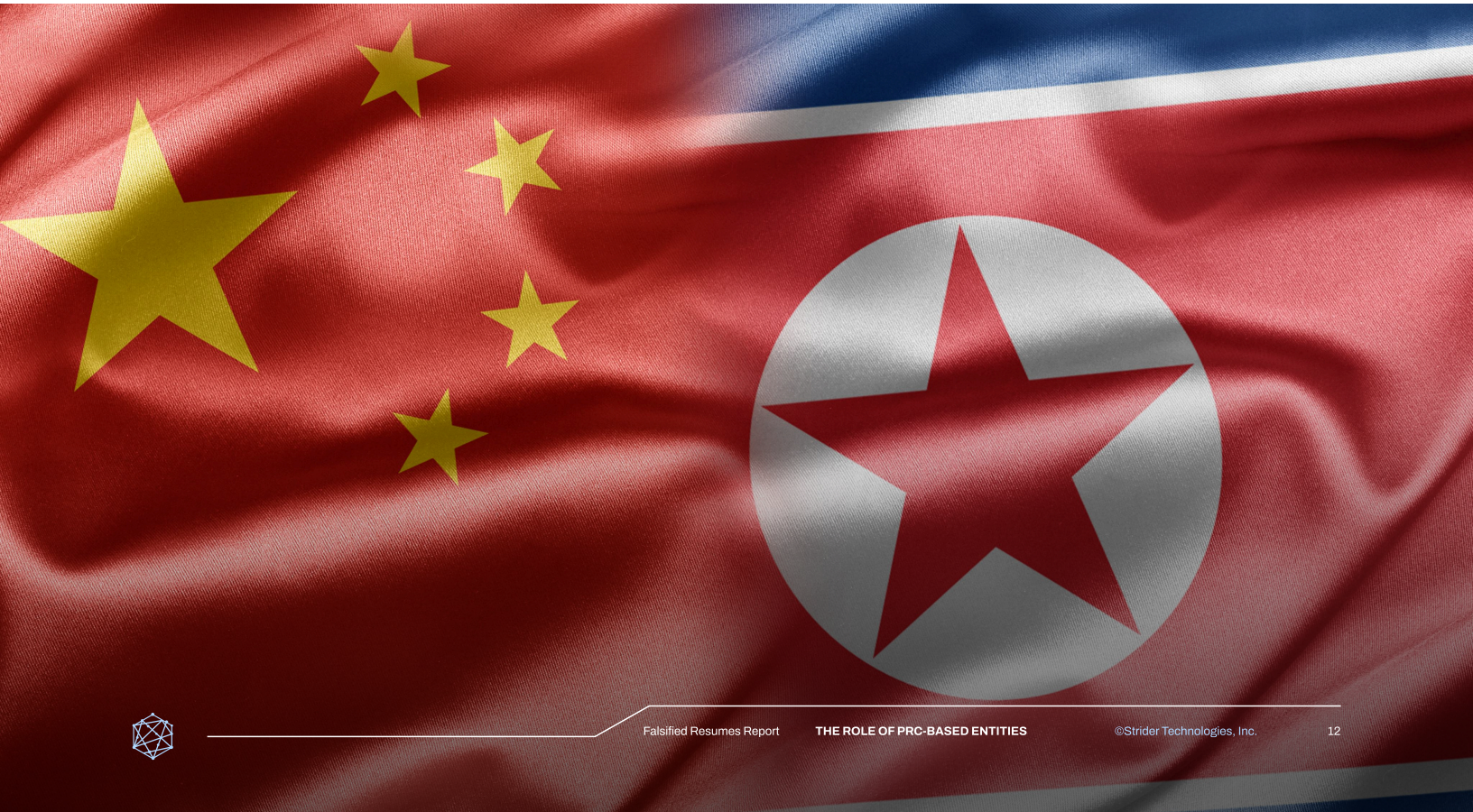
Malaysia, Vietnam, and Cambodia are known to host North Korean IT workers who exploit the burgeoning tech industries and the relatively loose regulatory environments to conduct their operations. They often work in IT outsourcing firms, sometimes even setting up their own businesses. The focus in these countries is typically on software development, website design, and other IT services that can be easily exported to global markets.

THE ROLE OF PRC-BASED ENTITIES

Strider's research is powered by our unmatched global data. Using advanced AI technology, Strider collects and processes open-source data in more than 100 languages from 65,000 unique sources worldwide—totaling more than 16 billion documents. This breadth and depth of data enables Strider to uncover complex global threat networks. Using our global organization data, Strider identified potential PRC intermediaries who may be using fraudulent identities to ship equipment for DPRK remote workers.

Strider identified a PRC-affiliated organization referenced in a U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) Sanctions notice issued on January 16, 2025.

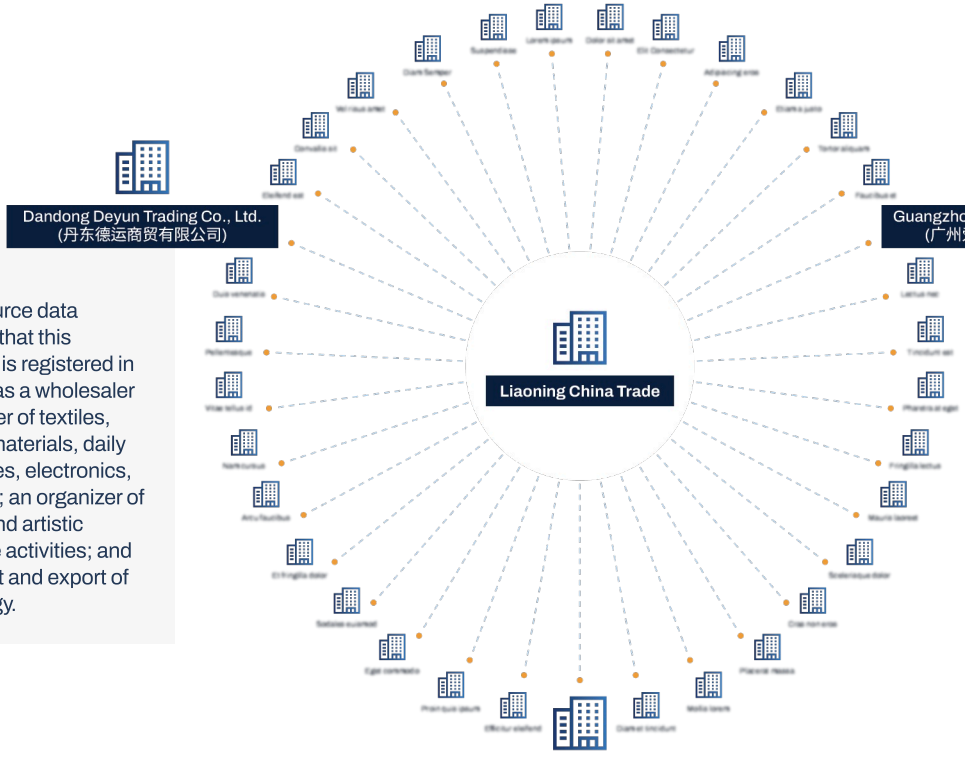
Liaoning China Trade Industry Co., Ltd (Liaoning China Trade) is a PRC-based company that has shipped equipment to Department 53 of The Ministry of The People's Armed Forces (Department 53), enabling it to conduct its IT worker activities abroad. These shipments include computers, graphics cards, HDMI cables, and network equipment. Department 53 is an entity subordinate to the DPRK Ministry of National Defense that is known for generating revenue through front companies in various sectors, including information technology (IT) and software development.



OFAC's sanctions terms state that "all property and interests in property of the designated persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, individually or in the aggregate, 50 percent or more by one or more blocked persons are also blocked." OFAC designates Liaoning China Trade for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, Department 53, a person whose property and interests in property are blocked pursuant to E.O. 13687.

Further investigation into Liaoning China Trade using Checkpoint, Strider's proprietary third-party due diligence platform, identified 35 additional organizations linked to the company through organizational and personal connections. Strider's data strongly indicates that these 35 organizations are affiliated with Liaoning China Trade and therefore could be materially supporting Department 53. This network presents a significant risk to Western businesses, which may unknowingly engage with or rely on entities connected to North Korean operations, exposing them to potential sanctions violations and serious reputational harm.

Three of the identified 35 organizations are:



01

Open-source data indicates that this company is registered in the PRC as a wholesaler and retailer of textiles, building materials, daily necessities, electronics, and more; an organizer of cultural and artistic exchange activities; and the import and export of technology.

02

Open-source data indicates that this company is registered in the PRC as a wholesaler of mineral products, building materials, and chemical products.

03

Open-source data indicates that this company is registered in the PRC as a wholesaler of cosmetics, personal hygiene products, clothing, and daily necessities. However, this differs slightly from how the company is advertised online—as a producer and wholesaler of commercial induction cookers, bathroom mirror cabinets, and backpacks.

Image 1: Screenshot of organizations with affiliation to Liaoning China Trade in Strider's Checkpoint tool.

CONCLUSION

This investigation underscores how PRC-based front companies are facilitating the global operations of fraudulent North Korean IT workers. By providing false business affiliations, laundering earnings, and securing access to international platforms, these entities serve as critical enablers of a broader illicit ecosystem. The scope and scale of this network is far greater than most Western companies realize, exposing them to heightened security, compliance, and reputational risks. Addressing this network requires coordinated vigilance across public and private sectors.

While the DPRK's use of this tactic has been highly publicized, the threat of fraudulently identified workers is far more widespread and systemic. Strider has also uncovered cases of remote workers from the PRC, India, and Pakistan using fake identities, fabricated work histories, and falsified credentials to secure employment within Western businesses, often gaining access to sensitive systems and data. In response to this growing threat, Strider will be launching a new tool designed to help organizations detect and flag falsified resumes during the hiring process, strengthening workforce integrity and reducing the risk of state-sponsored threats.

For access to the list of these organizations affiliated with Liaoning China Trade, or for more insight into information detailed in this report and future Strider tools, reach out to our team via email at info@striderintel.com.