The Rise of the Fake Tech Workforce: State-Sponsored Infiltration of U.S. Technical Supply Chains

warontherocks.com/2025/02/the-rise-of-the-fake-tech-workforce-state-sponsored-infiltration-of-u-s-technical-supply-chains/

February 27, 2025

Nathaniel Davis and Nina Kollars

February 27, 2025

Commentary

If the cornerstone of America’s competitive advantage is its domestic workforce’s capacity to drive technological innovation, then how do we respond if members of that workforce are not who they say they are?

On Dec. 12, 2024, the Department of Justice released an indictment against 14 North Korean nationals for involvement in a fake IT worker scheme impacting hundreds of U.S. firms and funneling millions of dollars to the ballistic missile program in the Democratic People’s Republic of Korea.

“Fake technology work” is conventionally associated with the techniques individuals use in attempting to appear productive, taking wages for work they did not do themselves. This type of fraud is not necessarily a threat to national security. However, cyber security researchers have grown concerned with employment fraud schemes that could be used by state-backed threat actors to gain access to sensitive systems inside firms and government agencies. Certainly, not all cyber threats are necessarily direct threats to the Department of Defense and its industrial base, but the rising trend of employment identity fraud merits more careful attention above the usual noise of conventional cybercrime.

This article is intended to introduce lawmakers and defense planners to the broader threat, but as is always the case with cyber threats, decision-makers need to read more deeply as befits their organization’s responsibilities and threat profile. Hereafter is a brief overview of what the national security policymaker needs to know about this trend, what resources firms and agencies need to manage their risk, and perhaps most importantly what not to do.

Become a Member

The Trend

For most working in cyber security, the weaponization of fake technology worker fraud as part of international statecraft is unsurprising. The U.S. technology sector has been publicly battling advanced persistent threat teams sponsored by North Korea for nearly 15 years. Regardless of the method (e.g., ransomware, spyware, etc.), North Korea has been leveraging the asymmetric features of attacks in cyberspace to bypass sanctions and fund its regime. It is only recently that industry has associated identity fraud with threats to national security.

The December indictment is part of a year-long series of revelations. The initial indictment unsealed in May 2024 named Arizona resident Christina Marie Chapman and three foreign nationals for their part in the theft of over 60 identities that they then used to obtain employment from U.S. firms. They infiltrated over 300 companies, which permitted agents to extort and funnel wages back to North Korean coffers. Chapman plead guilty to running a laptop farm in her home using equipment and login access obtained from the unwitting employers, obfuscating the true locations of the North Korean IT workers based internationally throughout Southeast Asia, Africa, China, and Russia.

These cases mark what FBI Special Agent Ashley Johnson characterizes as "the tip of the iceberg." Johnson warned back in May 2024 that "North Korea has trained and deployed thousands of IT workers to perpetrate this same scheme against U.S. companies every day."

There has been clear coordination of efforts to channel funds to North Korea at scale by North Korea's "IT Warriors," with assistance from Russian and Chinese firms. Yanbian Silverstar of China and Volasys Silverstar of Russia have been named as facilitating the fraud via replication of websites posing as fake U.S. IT firms offering workers for consulting and contract labor.

Estimating the scale of the broader problem and rooting it out will inevitably be done in back-channel conversations across affected firms, with help from federal and international crime agencies. As is the case with most cyber incidents, firms are reluctant to publicly disclose what transpired. The incentives for transparency are still outweighed by the headaches disclosure can cause like damage to reputation, risk of litigation, and loss of revenue. The potential impact is significant enough that the Securities and Exchange Commission released a Final Rule regarding incident disclosure.

Among the leaders in breaking this story was Palo Alto Networks' Unit 42, which documented a case they refer to as Wagemole in November 2023. Thereafter, in July 2024, KnowBe4 publicly disclosed they were a victim of this fraud.

The ongoing shortage of technical expertise for the Department of Defense exacerbates the potential for fraud. For over a decade now, the cyber workforce problem has continued to outrun solutions with no end in sight. Our adversaries have taken notice of our struggles with hiring and retaining a technology and cyber workforce. It will simply be a matter of time before our adversaries leverage access gained through identity fraud to directly manipulate software and networks. It would be a small step for a fake technology worker to move from sanctions evasion to sabotage of software and hardware supply chains, or to theft of critical and sensitive data like the cyber espionage activities of Onyx Sleet.

These risks demonstrate the need for integration of the defense industrial base with the wider U.S. private sector technology and service base. The innovation and production capacity needed to realize the Department of Defense's vision for military victory requires close, if not fully overlapping, relationships with private sector firms outside the traditional defense industrial base. While conventional defense industry firms are accustomed to protocols to ensure thorough vetting of their labor force, the opposite is true of more innovative small and medium-sized technology sector firms that rely upon international and remote talent. These firms must now worry about how much of their workforces are and will be affected by this rising trend.

Adjustments, Not Massive Overhaul

Rising threats are not necessarily a reason for massive changes in policy. Instead, we contend that somewhat simple adjustments are likely sufficient. Specifically, we propose more robust identity verification, streamlined internal information sharing, and greater external collaboration as starting points for changes that offer defensive improvements.

Identity verification is one pressure point that we can leverage. An overarching issue is the delay between the initial background check (i.e., Does this identity have a history and is this identity real?) and identity verification (i.e., Is the human in front of me the same as that of the identity we just checked?). Currently, most employers conduct these two activities at separate times, often through separate offices. The separation of these two activities is a weakness fraudsters rely upon. The gap is even more pronounced when an organization is leveraging a contracted workforce to supplement their full-time employees with limited access to background checks or identity verification information obtained by the vendor.

Currently, most businesses contract out for services to conduct criminal and lifestyle checks on a given identity. This normally occurs before onboarding and permits the fraudsters to input their own supporting background information, which may differ from the information initially provided to the recruiter. The identity verification process is often a perfunctory part of completing the Employment Eligibility Verification (Form I-9) during onboarding. It doesn't require a government photo ID or a Social Security number, just a List B identity document and a List C employment authorization document. Tools like E-Verify can add a layer of robustness to the process but are often not leveraged sufficiently against tight hiring deadlines and pressure to move the person along into their role.

At the firm and organizational level, the necessary elements needed to defend against the external threat and mitigate the internal threat likely already exist inside the company but are often divided across multiple groups: direct managers, cyber security teams, and human resources departments and their recruitment teams. Oftentimes, these teams operate in silos with limited interaction. Security offices should have the most up-to-date information on current tactics, but that information is of little benefit if the other teams are never told what to look for. Similarly, if a recruiter identifies a suspicious candidate but has no process for logging these personas, there is nothing to prevent the applicant from trying for a different position under another recruiter.

Going forward, human resources and recruitment offices must be aligned with security offices. Recruiting offices are often viewed as simply a resource for filling employment gaps, but they are usually the first touchpoint with the external candidates. They should be trained to recognize the signs of a potential fraudulent technology worker. Similarly, the broader human resources offices need to improve how they leverage the records of employees and candidates. Cross-referencing the candidate-supplied information (e.g., photos, phone numbers, and email addresses) against existing records can identify suspicious applicants much earlier in the hiring process. In real terms, the security office (or provider of those services) should have open lines of communication with the human resources and recruiting offices. This close alignment means that the risks and protections needed can be understood and managed holistically.

The problem isn't fully solved once a person is checked and verified. That outsider is now a new insider in the company. Again, no major policy adjustments are necessary, just a greater focus on access to resources based on performance and time. Once hired, employees should be put on probationary periods of limited access and greeted with a healthy dose of required face-to-face engagement on camera or in person. Over time, as trust builds the newly hired employe can transition to more consequential projects.

Effective retention and development of a trusted workforce is also essential to insider threat reduction and identification of fake technology workers. Those office holiday parties, recognition events, and employee development programs are not just niceties. Disgruntled employees are risky and more likely to engage in illegal subcontracting, sell their electronic identities, and trade in stolen data.

At the federal and international level, it is no secret there are significant growing pains when it comes to cyber security maturity and the defense industrial base. More checkboxes and training are not only unwelcome but further complicate a process that is already painful to small and medium-sized businesses — not to mention the international science and technology firms of our most trusted allies. A more effective mitigation would be to leverage preexisting informal sharing relationships and create a formal information-sharing program that facilitates passing threat intelligence across firms and trusted international organizations. A less-restricted sharing capability would allow more consistent linking of the individual cases at a firm with larger organizationally backed enterprise fraud efforts. These alignments between firm hiring and security offices and national and international law enforcement agencies are key to managing the threat and taking down the larger operations.

Potential Pitfalls

It may be tempting to hope that AI will help filter out the internal and external threats, but it won't. In fact, generative AI appears to have only exacerbated the sheer noisiness of hiring processes as applicants both malevolent and sincere use generative AI to try to bypass screening filters in applicant tracking systems. Threat intelligence should be leveraged to flag candidates for further review. Human-centered tool adoption is always better than blind faith in mindless automation.

Additionally, it is likely that firms and government agencies will want to reverse their expansion of remote work policies to blunt this threat. It is the wrong answer. Turning back, no matter how tempting, will not make the problem disappear. Given the ease with which North Korea has convinced people to serve as laptop farm facilitators, it is not outside the realm of possibility to see them recruit proxies to go into the office for them. The fundamental fact is that we are in a condition of scarcity for qualified labor — full stop. Backing away from remote work will further exacerbate and weaken our competitive global position by closing off access to an already highly sought-after workforce. It is more about managing the risk of access to resources and sensitive work in firms and organizations. Aligning human resource offices, hiring teams, and security offices will help mitigate these risks.

Way Forward

This is not a situation that can be resolved quickly. It is not solely a technical, a human resource, or even a single organization's problem. Mitigating the threat requires a collaborative solution.

The focus for firms and organizations should be to update their understanding of the threat patterns and build in careful checks against those behaviors. There is no substitute for having knowledgeable people well-armed with effective tools in the hiring and employment retention process.

What is most important is that we make these adjustments now. These fraud efforts are low risk with a high reward. They are not going to stop. It is on us, as defenders, to find a solution that balances the invasive requirements of a more robust identity verification system and the demand for a more open threat-sharing method against the need to maintain organizational reputation and candidate privacy. Only by collaborating, both across internal teams and between organizations, will we be able to stand against the rising fake technology workforce.

Nathaniel Davis has spent more than a decade defending government and private sector systems from both internal and external compromise. He is currently a member of the Paranoids at Yahoo, serving as a senior security systems engineer on the Cyber Defense team. He has presented his original research hunting fake technology workers in numerous off-the-record events within the security community. This is his first time on the record.

Nina Kollars, PhD is an associate professor in the Cyber and Innovation Policy Institute of the U.S. Naval War College and director/co-founder of the Maritime Hacking Village, a non-profit education and research maritime vulnerability initiative. She has had the honor of serving as a DefCon speaker on internet fraud and as a DefCon goon. She is also a certified executive bourbon steward and fan of cigars on occasion.

Image: Midjourney

Commentary