



CNS

OCCASIONAL PAPER

#36 · MAY 2018

The Shadow Sector: North Korea's Information Technology Networks

Andrea Berger, Cameron Trainer, Shea Cotton, and Catherine Dill



Middlebury Institute of
International Studies at Monterey

James Martin Center for Nonproliferation Studies

James Martin Center for Nonproliferation Studies
nonproliferation.org

The James Martin Center for Nonproliferation Studies (CNS) strives to combat the spread of weapons of mass destruction by training the next generation of nonproliferation specialists and disseminating timely information and analysis. CNS at the Middlebury Institute of International Studies at Monterey is the largest nongovernmental organization in the United States devoted exclusively to research and training on nonproliferation issues.

Middlebury Institute for International Studies at Monterey
www.miis.edu

The Middlebury Institute for International Studies at Monterey provides international professional education in areas of critical importance to a rapidly changing global community, including international policy and management, translation and interpretation, language teaching, sustainable development, and nonproliferation. We prepare students from all over the world to make a meaningful impact in their chosen fields through degree programs characterized by immersive and collaborative learning, and opportunities to acquire and apply practical professional skills. Our students are emerging leaders capable of bridging cultural, organizational, and language divides to produce sustainable, equitable solutions to a variety of global challenges.

James Martin Center for Nonproliferation Studies
Monterey Institute of International Studies
460 Pierce Street
Monterey, CA 93940, USA
Tel: +1 (831) 647-4154
Fax: +1 (831) 647-3519

Disclaimer

The James Martin Center for Nonproliferation Studies (CNS) has relied exclusively upon open-source intelligence for the research underpinning this report. These sources, like all forms of intelligence, have their limitations. As a result, the mention of any individual, company, organization, or other entity in this report does not imply the violation of any law or agreement, in the United States or elsewhere. The views, judgments, and conclusions in this report are the sole representations of the author and do not necessarily represent either the official position or policy or bear the endorsement CNS or the Middlebury Institute of International Studies at Monterey.

© The President and Trustees of Middlebury College, December 2017

Cover image: Shutterstock. Editing and production: Rhianna Tyson Kreger

The Shadow Sector: North Korea's Information Technology Networks

By Andrea Berger, Cameron Trainer, Shea Cotton, and Catherine Dill

Executive Summary

North Korea's commercial information technology (IT) industry has operated overseas, largely unnoticed, for decades. It sells a range of products and services including website and app development, administrative and business management software, IT security software, and biometric identification software for law enforcement applications. Its global network includes a myriad of front companies, intermediaries, and foreign partnerships. Yet despite the attention currently paid to North Korea's overseas revenue streams and its offensive activities in cyberspace, the spotlight has yet to illuminate the money-spinning North Korean IT firms whose offerings seem to have found their way into corporate supply chains and potentially even Western-allied law enforcement agencies. Drawing upon extensive open-source investigations by the authors, this paper examines several nodes in North Korea-linked IT networks and considers the implications for current and future policy efforts to stem North Korean revenue and mitigate the cyber-security threats the country poses.

Introduction

A common assumption about North Korean export activity is that, as former Secretary of Defense Robert Gates once said, the Democratic Republic of North Korea (DPRK) will “sell anything they have to anybody who has the cash to buy it.” Pyongyang’s information technology (IT) sector bears out this view. Gaining steam in the 1990s, the North Korean IT sector has expanded to include a significant network overseas in locations such as China, Russia, Southeast Asia, the Middle East, and Africa. Today, the country’s firms generate foreign revenue from the sale of a wide range of related goods and services, including website and app development, administrative and business management software, radio and mobile communications platforms, IT security software, and biometric identification software for law enforcement applications. North Koreans appear to have marketed virtual private networks (VPNs) and encryption software in Malaysia, sold fingerprint-scanning technology to large Chinese companies and parts of the Nigerian government, produced facial recognition software for law enforcement agencies via front operations, and built websites for myriad individual and corporate clients.

North Korea’s activities in the IT sector pose three main challenges for international efforts to curb threats emanating from the country. First, revenue accrued through the sale of IT goods and services likely blunts the impact of sanctions imposed by the United Nations and individual countries. Those sanctions focus primarily on the North Korean export of tangible commodities. Generally, services are considered only when they relate to military contracts, or more recently, to migrant labor. As a result, it is possible that North Korea may more actively seek to generate funds through intangible or less-tangible offerings, including those in the IT sector. Indeed, one specialist has recognized the DPRK as a source of affordable IT talent.¹ Cultivating IT expertise on activities such as software development not only provides revenue for the country, but also sidesteps the need to export migrant laborers in contravention of UN sanctions.²

Moreover, some of the revenue earned through the IT sector may directly or indirectly benefit individuals or companies linked to North Korea’s nuclear and missile programs. The network of companies linked to Glacom—a company recognized by the United Nations for both its links to the UN-

¹ Paul Tija, “Inside the Hermit Kingdom: IT and Outsourcing in North Korea,” *Communications of the ACM* 55, no. 8 (2012), pp. 22–25, [http://www.gpic.nl/outsourcingInNorthKorea\(CACM\).pdf](http://www.gpic.nl/outsourcingInNorthKorea(CACM).pdf).

² UN Security Council Resolution 2397, S/Res/2397, November 15, 2017.

sanctioned North Korean intelligence agency and its role financing the country's nuclear programs—includes at least two IT companies, examined below.³

The Korea Computer Center (KCC)—established in North Korea in 1990 to expand the country's IT capabilities and, according to the United States Treasury, operating overseas in Germany, China, Syria, India, and the Middle East—is another interesting case. It was designated by the US Treasury June 1, 2017⁴ for generating revenue for the North Korean regime, including the UN-sanctioned Munitions Industry Department.⁵ North Korea's continued revenue generation through IT thus seems to be a possible lifeline for at least some sanctioned entities, dulling the effect of efforts to exert particularly pointed pressure on those parts of the North Korean system.

It is possible that North Korea's IT sector may yet become a more focused target of the “maximum pressure” campaign championed by the United States. Though IT exports writ large have yet to be subject to international sanctions, President of the United States Donald J. Trump signed, in September 2017, Executive Order 13810, which specifically includes North Korea's IT sector under the new sanctions authority.⁶ Taken together with the sanctions on KCC in 2017, this indicates that the US Treasury may be paying greater attention to North Korean IT activities. Given Washington's leading role in designing sanctions at the UN level, this interest could translate into multilateral measures in future as well. Focus of that kind would help raise attention to North Korean activity in the sector and provide a relatively straightforward basis for countries interested in taking action to curb it.

Restricting North Korea's activity in the IT sector will nevertheless involve a second challenge. Less tangible technology transfers of the kind sold by North Korea are intrinsically difficult for countries to detect and prevent, but they present an even greater problem when layered with North Korea's evasive practices. North Korean networks active overseas have become increasingly adept at “hiding in plain sight” and concealing visible links to Pyongyang. Front companies and aliases help North Korean firms blend into the Asian marketplace, allowing them to market their goods as being from China or Southeast Asia, for example. This approach means North Korean individuals and entities can often convince unwitting clients to use them as a supplier without raising any alarm bells that something is amiss. This applies to the IT sector as well. Investigations indicate that North Korea may be using freelancing websites—such as Freelancer.com and Guru.com—to further enhance their anonymity and generate new business from customers unaware that their business is going to Pyongyang.

Third, the export of IT goods—particularly software—heightens the risk of cyber insecurity. Attention to North Korean offensive activity in cyberspace is mounting, following the attempted theft of nearly

³ United Nations, “The List established and maintained pursuant to Security Council res. 1718,” generated April 25, 2018, <https://sancs.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/dprk-r.xsl>.

⁴ US Department of the Treasury, “Treasury Sanctions Suppliers of North Korea's Nuclear and Weapons Proliferation Programs,” Press release, June 1, 2017, <https://www.treasury.gov/press-center/press-releases/Pages/sm0099.aspx>.

⁵ The Munitions Industry Department was sanctioned by the United Nations on March 2, 2016, for its role overseeing the DPRK's ballistic-missile program.

⁶ Executive Office of the President, “Imposing Additional Sanctions with Respect to North Korea,” Executive Order 13810, September 20, 2017, <https://www.federalregister.gov/documents/2017/09/25/2017-20647/imposing-additional-sanctions-with-respect-to-north-korea>.

one billion dollars from Bangladesh's account at the Federal Reserve Bank of New York⁷ and the worldwide WannaCry malware attacks,⁸ both of which have been attributed to the DPRK. Analysis conducted by Kaspersky Lab, an internationally recognized cybersecurity firm, purports to reveal the modus operandi for North Korean hackers. According to their analysis, North Korean hackers initially compromise a victim's network using remotely accessible vulnerable code or an exploit planted on a benign website.⁹ The former method is of particular interest as North Korean-developed software could be an ideal delivery mechanism for remotely accessible code. Though individual cases of vulnerabilities created by use of North Korean IT security products have yet to be publicly reported, the potential for such vulnerabilities undeniably exists. North Korea has repeatedly shown that it is willing to exploit its cyber capabilities for commercial and financial gain.

This report highlights these challenges using two case studies, focusing on nodes in North Korea-linked IT networks. The cases outlined are based purely on open-source information, and therefore tell an incomplete story. They also represent both a fraction of the authors' wider research on this subject, and a fraction of North Korean IT networks themselves. As a result, this report is merely a starting point for a necessarily larger conversation over the threats and risks posed by North Korean involvement in the commercial IT industry, and how best to address them.

The Korea Aprokgang Technology Company Network

Investigations into North Korean IT companies overseas reveal the key role played by the Korea Aprokgang Technology Company, whose business is known to span Russia, China, Southeast Asia, and Africa.¹⁰ According to a 2002 business publication, the company has "led the IT industry in North Korea since the 1990s," with a specialization in biometric information technology products and software for security applications.¹¹ The same publication claimed the company then had 400 IT workers, and that it had "shipped security products based on its fingerprint authentication technology and personal authentication system to China, Thailand, Japan and Nigeria."¹² Aprokgang claims to have won two gold prizes for its fingerprint recognition and scanning software at the International Exhibition of Inventions in Geneva during the 1990s.¹³ Other North Korean companies have made similar claims.¹⁴

⁷ Aruna Viswanatha, and Nicole Hong, "U.S. Preparing Cases Linking North Korea to Theft at N.Y. Fed," *Wall Street Journal*, March 22, 2017, <https://www.wsj.com/articles/u-s-preparing-cases-linking-north-korea-to-theft-at-n-y-fed-1490215094>.

⁸ "Cyber-attack: US and UK blame North Korea for WannaCry," BBC, December 19, 2017. <http://www.bbc.com/news/world-us-canada-42407488>.

⁹ "Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies," Kaspersky Lab, April 3, 2017, https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies.

¹⁰ A.k.a. Korea Aprokgang Technology Development Company (KATDC).

¹¹ *North Korea: Investment & Business Guide* (Washington, DC: USA International Business Publications, 2002), p. 100.

¹² Ibid.

¹³ Ibid. The Exhibition did not respond to repeated requests for information.

¹⁴ Chosun Technology Company supposedly won a prize for a fingerprint device at the same exhibition, albeit in 1996. See *North Korea: Investment & Business Guide*, p. 257. CNS has been unable to independently confirm such claims, although the Korea Central News Agency has referenced those made by Aprokgang. See "Korea Amnokgang Technology Development Corporation," KCNA, September 25, 2002. Accessed via www.KCNAWatch.co. It is possible that these companies won their prizes under different names. There is precedent: the KCC supposedly participated in the 1999 China World Computer Fair under the name of an

Aprokgang has continued to be active since the 1990s. In or around 2006, it appears to have outfitted the civil service in Rivers State in Nigeria with fingerprint and card scanners. The Nigerian team that set out to find appropriate contractors reportedly searched “all over the place, until their ship berthed at the shores of KATCO Limited [the Korea Aprokgang Technology Corporation].” The company is registered in Nigeria as “Katrad Aprokgyang Technologies Company,” and remains a live entity.¹⁵ It is unclear how precisely the Nigerian officials tasked with procuring new security systems for River State arrived at Korea Aprokgang’s “shores.”

There is evidence that Nigerian contracts may have run through China. The press release regarding the River State deal mentions that those responsible for procurement made “the ultimate discovery of PEFIS,” a brand trademarked by the Katrad Aprokgang Technology Co in Lagos, Nigeria, that features a fingerprint as its logo.¹⁶ Web searches for PEFIS reveal that it is a Beijing-registered firm formally incorporated as PEFIS Electronic Technology (Beijing) Co. offering a range of biometric security products, from fingerprint scanners to facial recognition software and card readers.¹⁷ Some of these products are displayed on a corresponding Chinese Ministry of Commerce page for the company.¹⁸ PEFIS also purports to be the “first developer of a fingerprint lock in China,” and to have received four gold prizes at the International Exhibition of Inventions—a claim that corresponds with that made by Korea Aprokgang.¹⁹ This link is borne out by corporate registry documents, which show that PEFIS was a live company, through January 2018, with the Korea Yalu River Technology Development Association as a primary shareholder.²⁰ “Aprokgang,” or its alternate romanization “Amrokgang,” is the Korean name for “Yalu River.”

PEFIS was first registered in China in 1996, using a 45 million yuan initial investment from the Korea Yalu River Technology Development Association.²¹ According to its latest corporate filings, the company has 14 staff, including its directors Han Zhihu (韩治虎), Li Wenshan (李文山), and Yin Yongjun (尹勇俊). Its

undisclosed Chinese company. See: Woo-Suk Nam, “North Korea’s IT Industry,” Korea Trade-Investment Promotion Agency, January 3, 2001, <http://www.kotra.or.kr:80/main/info/nk/eng/main.php3>, online via Wayback Machine at www.web.archive.org. According to the Korea Trade-Investment Promotion Agency, KCC also produced a fingerprint lock at one point. It is unclear whether this was among the products it presented in 1999. It is also unclear whether these entities developed their technologies in parallel, or if such development was a shared enterprise.

¹⁵ Information from the Nigerian Corporate Affairs Commission, company number 424297. See <http://new.cac.gov.ng/home/>. The use of alternate romanisations of Korean names is a common challenge when conducting due diligence on North Korean corporate networks.

¹⁶ Trademark number TP. 73709/03.

¹⁷ Chinese name: 培富士电子技术 (北京) 有限公司, with Registration number 110000410111651. Some English translations of the name on official documentation use “Pei Fuji Electronic Technology (Beijing) Co Ltd.”

¹⁸ “Pefis Electronic Technology (beijing) Co., Ltd,” Ministry of Commerce of the People’s Republic of China, Accessed April 25, 2018, <http://ccne.mofcom.gov.cn/5159>.

¹⁹ Note the discrepancy between Aprokgang’s claim (gold prizes in 1990 and 1994) and that of PEFIS (four gold prizes between 1990 and 1996). The reason for this discrepancy is unclear.

²⁰ 朝鲜鸭绿江技术开发总会社. While a company number is provided for this shareholder, they do not appear to be separately registered as a legal entity in China. Official corporate registry document also suggests that in 2015, the shareholder was listed with a slightly different name (鲜鸭绿江技术开发总会社) compared to the one usually offered (朝鲜鸭绿江技术开发总会社). It is unclear whether this represents a significant change.

²¹ In 2018 valuation, this equates to approximately 62 million yuan, or USD \$9.7 million (Annex 1). Beijing Administration for Industry and Commerce, National Enterprise Credit Information Publicity System.

annual return figures are not disclosed on official paperwork, but are available via third-party sites.²² Annual sales for 2016 reportedly amount to 274 million yuan (USD \$42 million), though recorded profit is only 205,000 yuan or USD \$34,000 (Annex 2). It is unclear whether these figures are accurate, as amounts recorded for tax paid by the company would be equivalent to a 0.05% tax rate. The company filed annual reports through 2016, demonstrating its recent activity in the Chinese IT sector.

Pefis' business license was revoked by the Beijing Administration for Industry and Commerce on January 22, 2018, ostensibly for violating UN resolution 2375 (2017). That resolution—adopted 11 September 2017—required countries to prohibit joint ventures and cooperative entities with DPRK entities or individuals, mandating the closure of existing joint ventures by 9 January 2018. Despite China's administrative action against Pefis, a welcome example of sanctions enforcement, the company's website and page with the Ministry of Commerce both remain active at time of writing.²³

Further research indicates that one of PEFIS' sources of profit may be the sale of its software and algorithms to other major biometric security firms. The PEFIS home page features a set of links to other Chinese companies producing fingerprint scanning products (Annex 3). One is for a company that appears to be Chinese owned and operated, though there are indications that its products may use North Korean software. Several separate business-to-business websites marketing the company's products claim that its products use North Korean algorithms (Annex 4). Some of the advertisements state that the product is a "new version of North Korean algorithms with dependability and accuracy...[and] identification speed obviously improved." In fact, as demonstrated in Annex 4, a search for the same phrase reveals many more potential suppliers of products claiming to integrate North Korean algorithms. This software may be supplied by PEFIS or its parent firm, though CNS cannot confirm this. If accurate, through the Chinese company's distributors and partners, the products and their integrated North Korean software is on sale in every continent.

Another Chinese manufacturer identified on the PEFIS site is also active in the biometric security arena. They, too, describe their fingerprint scanners as having a "world-class algorithm," though with no mention of North Korea or any foreign provider of it. However, their product interface bears striking resemblance to one advertised by a Malaysian company, which states that it uses algorithms that won gold prizes at the International Exhibition of Inventions in Geneva during the 1990s. Though it cannot be confirmed, the similarity in claims suggests it could be a reference to the same prizes won by Korea Aprokgang. Furthermore, the screen on the Malaysian product fingerprint time recorder is almost identical to that of a fingerprint time recorder sold by one of the PEFIS-linked Chinese companies. Both show a time around 10am, a date stamp of 2015, and a backdrop of a desert and blue sky (Annex 5). It is unclear whether these similarities exist because they use the same underlying software, or whether there are other explanations.

Further research links PEFIS to an Aprokgang-affiliate in Russia. The affiliate—EMA, LLC—is 49 percent owned by Korea Aprokgang.²⁴ Since its incorporation in 2008, EMA has engaged in behaviors similar to other Aprokgang companies selling biometric security devices. This includes the manufacture of computers and peripheral equipment, electrical installation, and joinery installation. EMA possesses a

²² From 2014, Chinese authorities no longer publish certain types of financial information, including shareholding contributions.

²³ National Enterprise Credit Information Publicity System, accessed May 8, 2018. See Annex 1.

²⁴ Russian name: ООО ЭМА, with Tax Identification Number (ИНН) 6501196130. Its full name in Russian is ООО ЭлектроМонтаж Амноккань. The remainder of the shares are held by a Russian company.

2009 consignment certificate for biometric locks model FOC568 manufactured by PEFIS, which corresponds to an entry on the PEFIS website.²⁵ A matching lock²⁶ is advertised by a Russian security company as the Aprokgang-568 (Апроккан-568).²⁷ That company shares its registered address and phone number with EMA. Its owner is also the general director and majority shareholder via another Russian security company of EMA. Korea Aprokgang also has an active representative²⁸ in Vladivostok, though it is unclear whether this “Aprokgang” is the same entity as the Korea Aprokgang Technology Development Company in Pyongyang, or whether it is affiliated with a parent company or other firm in the corporate group.

These activities suggest that, despite the sanctions regime, Korea Aprokgang and its affiliate companies (including PEFIS) are able to successfully form diverse corporate partnerships and develop business in the global market for biometric security products and software. Crucially, it appears that a key part of their business is not the sale of physical devices, but of intangible technology transfer. This shift will only make it harder for investigators to uncover the activities of this network and others involved in the North Korean IT sector. Furthermore, the sale of software could pose a cyber-security risk for clients.

The GLOCOM Network

Global Communications Co, or “Glocom,” a defense firm operating from Malaysia that sold “radios and communications equipment, navigation equipment, Battle Management System (BMS), Command & Control System (C2S), and other customized equipment for [sic] military and para-military organizations, secret service and security organizations, and specially authorized civilian governments at home and abroad.”²⁹ In February 2017, the United Nations Panel of Experts established pursuant to resolution 1874 exposed Glocom as a North Korean front controlled by the country’s intelligence agency, the Reconnaissance General Bureau.³⁰ A Reuters special investigation published shortly thereafter revealed a web of Glocom-linked individuals and benignly named front companies operating in Malaysia, Singapore, and further afield.³¹ Together, they showed how key North Korean individuals based in Pyongyang and Kuala Lumpur were able to establish this network and facilitate years of illegal arms-related sales, gaining access to local bank accounts and major defense trade fairs.

WCW Resources and Adnet International

Little-noticed at the time of the investigation were the two IT companies within the Glocom network.³² WCW Resources Sdn Bhd, registered in Malaysia in November 2015, remains active at the time of writing.

²⁵ Registry number POCC CN.AB71.A00442, issued October 23, 2009.

²⁶ Referred to in the consignment certificate as the FOC568, sold by PEFIS as the FOC568PET and by FinEko-Rosa-1 as the Aprokgang-568 (Апроккан-568).

²⁷ Russian: ООО ЧОП “ФИНЭКО-РОСА-1,” Tax Identification Number (ИНН) 6501146700. See www.fineco-rosa.snc.ru, and specifically the Aprokgang-linked products page www.fineco-rosa.snc.ru/teh6.html.

²⁸ Russian: Пред ОТЗ “Апроккань,” Tax Identification Number (ИНН) 9909344990.

²⁹ “About Glocom” section, www.glocom-corp.com.

³⁰ United Nations Security Council, “Note by the President of the Security Council,” S/2017/150, February 27, 2017.

³¹ James Pearson and Rozanna Latiff, “North Korea spy agency runs arms operation out of Malaysia, U.N. says,” Reuters, February 26, 2017, <https://www.reuters.com/article/us-northkorea-malaysia-arms-insight/north-korea-spy-agency-runs-arms-operation-out-of-malaysia-u-n-says-idUSKBN1650YE>.

³² James Pearson of Reuters discussed the firm in a March 2017 episode of the Arms Control Wonk podcast. See: “Glocom and DPRK Fronts,” Arms Control Wonk Podcast, March 10, 2017, <http://armscontrolwonk.libsyn.com/glocom-and-dprk-fronts>. Thereafter, CyberScoop also reported on the activities of these companies, further detailing Adnet International’s purported operations. See Patrick Howell

Though no North Koreans appear as directors,³³ WCW's majority shareholder is Kim Chang Hyok, the North Korean at the center of the Glocom network in Malaysia.³⁴ The firm offers a range of "computer consultancy" services spanning web and software development.

Similarly, Adnet International Sdn Bhd, registered in 2015 by a group of Malaysian nationals and only recently dissolved, also lists Kim Chang Hyok as a shareholder.³⁵ Several of its Malaysian directors also appear on the paperwork of other Glocom-linked front companies.

Adnet's website was removed shortly after the UN named Glocom, but archived versions are available online.³⁶ It advertised a range of IT products and services, from virtual private network clients and encryption services, to USB security keys, apps, and website development. The Adnet site further claims that its core technology includes "biometrics identification techniques based on fingerprint, palm-print or face identification skills, artificial intelligence techniques" and that "the fingerprint products based on self-developed fingerprint identification technique were awarded four golden prizes at Geneva International Invention Exhibitions held in Switzerland (1990~1996)."³⁷ The assertion mirrors that made by PEFIS and Aprokang. Furthermore, Adnet states that it has "old cooperative partners of tens of years in China, Russia, Japan, Nigeria and [elsewhere]" and that its products were on sale in "China, Japan, Malaysia, India, Pakistan, Thailand, UAE, UK, Germany, France, Russia, Canada, Argentina, Nigeria and other countries."³⁸

The company's declared employee details also merit further scrutiny. Adnet's website stated that it had "over 500 talented technicians"; however, given the other available details about the company's operations, it is unlikely that it would have had this number of employees in Malaysia alone. Instead, it is more likely that the firm was also drawing upon technicians—possibly North Korean—located elsewhere. Adnet's phone number is used on social media accounts for "Zhu Taihu," a Korean-speaking IT developer at Adnet International, according to his LinkedIn page. On the page, he notes that he is establishing a "promising IT company in Malaysia" and "can provide a lot of IT technicians as many as you want if you want... If you hire them, you'll never be disappointed and you'll become a millionaire."³⁹ His LinkedIn profile photo appears to have borrowed from an unrelated Indonesian man, suggesting that the profile may be fake and "Zhu Taihu" may be an alias.

Investigations also revealed Freelancer profiles for Malaysian software developers claiming to have worked at Adnet International in Malaysia (Annex 6). One states under their Adnet experience that "hiring me is hiring my members," and purports to have been involved in the development of a vehicle recognition system, an area in which North Korean firms elsewhere also claim to specialize, as outlined

O'Neill, "Why was North Korea running a phantom cybersecurity startup in Malaysia?" *CyberScoop*, March 27, 2017, <https://www.cyberscoop.com/north-korea-cybersecurity-United-nations-adnet-international/>.

³³ North Korea increasingly relies on foreign nationals to complete corporate paperwork for its networks overseas, particularly in jurisdictions where corporate records contain details of director/shareholder nationalities.

³⁴ Information from the SSM Companies Commission of Malaysia, company number 1166441-K.

³⁵ Information from the SSM Companies Commission of Malaysia, company number 1145090-U.

³⁶ Website of Adnet International, www.adnet.com.my, accessed via Wayback Machine at www.web.archive.org.

³⁷ "About Us," Adnet International, www.adnet.com.my/adnet/aboutus, accessed via Wayback Machine at www.web.archive.org.

³⁸ *Ibid.*

³⁹ LinkedIn page for "Taihu Zhu," <https://my.linkedin.com/in/taihu-zhu-97851412a>.

below.⁴⁰ While it cannot be confirmed that this is the same Adnet as the Glocom-linked company in question, it is possible that Glocom-linked IT firms are using Freelancer profiles to conceal the North Korean origin of the services offered.

Future TechGroup

Glocom shares its current web infrastructure with a company called Future TechGroup,⁴¹ whose expired SSL certificate is self-signed by Glocom. Future Techgroup's website, the landing page of which now only says "coming soon," previously advertised a "powerful and experienced info-tech community."⁴² It made no mention of its physical location or who is part of this "community." However, the previous website analyzed by CNS bears distinct hallmarks of a North Korean firm. Cached versions of the site show it advertises sophisticated technology for mushroom growing—an industry that, while out of place in their software-focused business, is distinctly popular in North Korea. The company also advertised Korean-language translation software, another red flag. In addition, the marketing video on the site featured a cover of the Rocky theme song performed by the Moranbong Band, a North Korean pop group, for Kim Jong Un.⁴³

The firm claimed to have recently won a prestigious award for its facial recognition software at an international competition in Switzerland.⁴⁴ Further investigations into the competition supported this claim in part. The software in question, however, had been entered by a seemingly reputable not-for-profit entity in a US-allied country, not by a North Korean firm.⁴⁵ The authors have refrained from publishing full details of this partner company, as our research suggests that it was probably genuinely unaware of their software supplier's connection to North Korea—a link effectively obscured by the evasive tactics adopted by Future TechGroup-linked individuals and entities. It is the opinion of the authors that even reasonable due diligence performed by the company may not have sent up red flags.

In addition to its claims to major international prizes, Future TechGroup advertises past website development projects—including one for a US primary school—and purports to have sold their facial recognition software to Turkish and other law enforcement agencies. CNS could not verify these claims.

If true, how could a seemingly North Korea-linked IT firm manage to successfully permeate the global security marketplace in this way without being detected? One possibility is that individuals linked to

⁴⁰ "Sosit Sdn Bhd," a firm within the MKP Group—a North Korean-Malaysian joint venture—boasts having developed a vehicle tracking software which uses GPS. See

<http://sosit.mkpholdings.com.my/product/index.php?part=vehicle>. As with other North Korean-linked IT firms, SOSIT and individuals affiliated with it make use of freelancer websites to develop new business.

⁴¹ It is possible that Future TechGroup has a North Korean analogue, Miraetech Company. *Mirae* is Korean for future. That company's areas of work correspond to those of Future TechGroup. Miraetech has produced devices in the fields of IT, machine-building, and geological prospecting.⁴¹ This last field is of particular note: Future TechGroup also, in addition to its IT services, sells geomagnetic prospecting technologies. "Miraetech Company". *KCNA*. 30 September 2009. Accessed via www.KCNAWatch.co.

⁴² Content was removed from the website <future-techgroup.com> in August 2017.

⁴³ The authors are grateful to the devoted Moranbong Band fan who pointed out this detail. A video of the Rocky theme song as performed by the Moranbong Band is available at: <https://www.youtube.com/watch?v=aIYZMkkzNzk>.

⁴⁴ The competition is not related to the International Exhibition of Inventions in Geneva. <https://web.archive.org/web/20170220014915/http://future-techgroup.com/>.

⁴⁵ In line with the apparent North Korean signatures on the Future TechGroup website, a video held by the authors that demonstrates the software appears to feature Korean individuals.

Future TechGroup formed business links in the way that many programmers do: freelancing websites. Further research into information presented on the Future TechGroup site revealed freelance profiles on Freelancer.com and Guru.com for a Vietnam-based facial and object recognition software specialist called “Richard Minh.”⁴⁶ Product images on those Freelancer pages are identical to the product videos and images on the previous Future TechGroup site (see Annex 7).

Richard Minh’s Freelancer profile is under the username “kjg197318,” suggesting that “Richard Minh” could be an alias and his username corresponds to his true initials and possibly birthdate. Freelancer pages show that “kjg197318” has won a number of contracts around the world, including for license plate recognition software for a customer in Turkey and a range of clients in North America and Europe.⁴⁷ According to the parallel Guru.com profile, Richard Minh preferred to take payment for work by PayPal.

The Vietnamese connection is further strengthened by one of the pages from the Future TechGroup website. In demonstrating the vehicle recognition software, the example used appears to be a Vietnamese license plate (see Annex 8). Vietnam recently announced that it had denied visas for more than twenty North Korean IT workers, though it is unclear whether they were connected to this case.⁴⁸

North Korean evasion cases like this prove the effectiveness of Pyongyang’s approach: use simple obfuscation methods and replicate them on a large scale. Basic tactics like hiding in the volume of foreign Asian business, creating front companies with non-descript web footprints, and using aliases are often enough for North Korea to convince outside eyes that nothing is amiss. In addition, North Korean individuals using freelancing websites can often act with even greater levels of anonymity. These tactics seem to have fooled both major international competition and at least one reputable defense firm in a US-allied country. The outcome is that foreign governments and law enforcement agencies may have inadvertently and indirectly paid North Korea to develop software they currently use.

Conclusion

The case studies included in this report provide merely a small window into the front companies, intermediaries, and foreign partnerships that have allowed North Korean IT offerings to find their way into public- and private-sector supply chains worldwide. Pyongyang’s activities in this sector are far larger than detailed in this report, and larger still than what is appreciated in the public conversation over North Korea’s overseas footprint.

The challenges this activity creates for policy and cyber security could be comparatively substantial. The continued sale of North Korean IT goods and services undercuts the UN sanctions regime in several ways. Generally speaking, it represents a continued source of revenue for North Korea, albeit one that is difficult to quantify given the approach to contracting and lead generation that appears to occur. Commercial freelancing profiles, and North Korea’s general commercial networks, seem to be increasingly used to produce new contracts that can be filled by the country’s IT developers, wherever they may reside. More specifically, as the companies linked to the Glocom network demonstrate, IT

⁴⁶ See Richard Minh’s Guru.com active profile at <https://www.guru.com/freelancers/richard-minh>. The Freelancer.com profile for Richard Minh (<https://www.freelancer.com/u/kjg197318>) has been closed since commencing this investigation.

⁴⁷ See, for example: <https://www.freelancer.com/projects/android/project-for-kjg-14117250/>

⁴⁸ Shim, Elizabeth. “Vietnam expels North Korea shipping chief,” UPI, October 20, 2017, <https://www.upi.com/Vietnam-expels-North-Korea-shipping-chief/3621508509635/>.

services seem to be benefitting parts of the North Korean system that have a role in the country's military programs.

The result is that IT products and services sold overseas by the North Koreans may be blunting both the effect of targeted sanctions on certain entities of concern, as well as on the regime more broadly. A more general treatment of the IT sector within multilateral and unilateral sanctions regimes could help. At present, these IT-related sales are sanctionable only if they violate bans on joint ventures, designations of individuals or entities, or migrant labor restrictions. While parts of Korea Aprokgang's Nigerian and Russian networks appeared to be structured as joint ventures, and while the Glocom network has confirmed ties to the sanctioned Reconnaissance General Bureau, ascertaining and substantiating linkages between IT companies and existing sanctions is likely to require more effort than most countries are willing to exert.⁴⁹ It is also unclear precisely how much of North Korea's IT activity the current sanctions net would catch.

Even with changes to the sanctions regime, restricting North Korea's activity in the global IT sector will pose an operational challenge. North Korean networks continue to create elaborate guises to fool their interlocutors into thinking they are of another nationality. Intangible forms of revenue generation, like North Korea's sale of algorithms or any software development offshoring, are also intrinsically harder to stem than tangible ones. Governments lack opportunities to physically interdict such exports, and even countries with comparatively sophisticated export-control arrangements struggle to develop feasible approaches to managing intangible technology transfers.

Perhaps the best chance of disrupting this activity rests on disrupting the networks involved. In contemplating the shape of any sanctions that cover North Korean IT, governments should seek to create sector-wide authorities to take aim at major players in North Korea's IT industry. As indicated above, this has yet to occur at the UN level, and the Korea Computer Center is, at the time of writing, the only IT company sanctioned by the United States.

Government guidance to the private sector—particularly those operating in industries in which the North Koreans specialize, such as biometric identification—would also be useful. Such action would clearly demonstrate to the private sector the need to be alert to DPRK IT services and to take this problem seriously. It could also provide specific examples of DPRK action they could look to and guard against. Companies and other actors outsourcing IT goods and services—especially those in high-risk industries—should augment and expand their due diligence practices when contracting using freelancer websites or providers in Asia.

Without such steps, North Korea's activity in the IT sector is likely to continue to pose an underappreciated cybersecurity threat. At present, it seems that many affected clients have unwittingly engaged North Koreans. While the level of access Pyongyang may have into their customers' systems and data depends upon the services rendered, there is demonstrated potential for North Korea to exploit these relationships for its cyber activities. As long as North Korea's IT sector remains in the shadows, Pyongyang's concerning sale of such goods and services will likely continue unabated.

⁴⁹ Similarly, according to the US Treasury, the KCC "generates money for the North Korean regime through software development and programming," including for the sanctioned Munitions Industry Department, and "is reported to have overseas locations in Germany, China, Syria, India and the Middle East." Department of Treasury, "Treasury Sanctions Suppliers of North Korea's Nuclear and Weapons Proliferation Programs."

About the Authors

Andrea Berger is a Senior Research Associate at the James Martin Center for Nonproliferation Studies (CNS), where her current research focuses on East Asian nuclear issues, proliferation networks, and export controls and sanctions. Andrea is also an associate fellow at King's College London and at the Royal United Services Institute for Defence and Security Studies (RUSI). Prior to joining CNS, she was the Deputy Director of the Nuclear Policy team at the RUSI, and an analyst in the Government of Canada.

Cameron Trainer is a Research Associate at CNS. He is a graduate of the University of St. Andrews, where he studied International Relations and Russian.

Shea Cotton is a Research Associate at CNS in Monterey. He supports the Export Control and Nonproliferation Program (XNP) at the James Martin Center for Nonproliferation Studies at the Monterey Institute of International Studies. His primary area of study is on US export controls and their effects on industry compliance. Shea built and manages the North Korea Missile Test Database that tracks North Korea's missile-testing activity. He earned his BA and MA from the University of Georgia.

Catherine Dill is a Senior Research Associate in the Export Control and Nonproliferation Program at CNS. She has a broad research portfolio that includes analyzing nuclear and missile programs and nonproliferation and export-control policies in East Asia, illicit procurement networks and nonproliferation sanctions, and the effect of emerging technologies on nonproliferation policy and strategic stability. Catherine helped to establish geo4nonpro.org, a crowdsourcing website dedicated to analyzing satellite and remote sensing imagery of sites of nonproliferation and defense interest. Catherine holds an MA in Nonproliferation and Terrorism Studies from the Middlebury Institute of International Studies at Monterey, and a BS in Foreign Service from Georgetown University's School of Foreign Service. Previously, Catherine worked as a senior consultant at Booz Allen Hamilton in Washington, DC.

Annexes

Annex 1: Corporate Registry Documentation for PEFIS Electronic Technology Co.





培富士电子技术(北京)有限公司 开业

统一社会信用代码: 91110105600060517H

法定代表人: 李文山

登记机关: 北京市工商行政管理局朝阳分局

成立日期: 1996年01月24日

[发送报告](#)

[信息分享](#)

[信息打印](#)

- 基础信息**
- 行政许可信息
- 行政处罚信息
- 列入经营异常名录信息
- 列入严重违法失信企业名单(黑名单)信息

■ 营业执照信息

- 统一社会信用代码: 91110105600060517H
- 企业名称: 培富士电子技术(北京)有限公司
- 类型: 有限责任公司(外国法人独资)
- 法定代表人: 李文山
- 注册资本: 45.000000万美元
- 成立日期: 1996年01月24日
- 营业期限自: 1996年01月24日
- 营业期限至: 2026年01月23日
- 登记机关: 北京市工商行政管理局朝阳分局
- 核准日期: 2017年06月06日
- 登记状态: 开业
- 住所: 北京市朝阳区胜古中路2号院8号楼223-225-227室
- 经营范围: 生产指纹识别系统及民用指纹系统软件;提供技术咨询、技术服务;销售自产产品。(依法须经批准的项目,经相关部门批准后依批准的内容开展经营活动。)

■ 股东及出资信息 股东及出资信息截止2014年2月28日。2014年2月28日之后工商只公示股东姓名,其他出资信息由企业自行公示。

序号	股东名称	股东类型	证照/证件类型	证照/证件号码	详情
1	朝鲜鸭绿江技术开发总会社	企业法人	企业法人营业执照(公司)	ST000008	查看

Source: National Enterprise Credit Information Publicity System, accessed January 2018.



培富士电子技术(北京)有限公司 吊销

统一社会信用代码: 91110105600060517H
 法定代表人: 李文山
 吊销原因:
 吊销日期: 2018年01月22日

发送报告

信息分享

信息打印

基础信息

行政许可信息

行政处罚信息

列入经营异常名录信息

列入严重违法失信企业名单(黑名单)信息

营业执照信息

- 统一社会信用代码: 91110105600060517H
- 类型: 有限责任公司(外国法人独资)
- 注册资本: 45.000000万美元
- 营业期限自: 1996年01月24日
- 登记机关: 北京市工商行政管理局朝阳分局
- 登记状态: 吊销
- 住所: 北京市朝阳区胜古中路2号院8号楼223-225-227室
- 经营范围: 生产指纹识别系统及民用指纹系统软件; 提供技术咨询、技术服务; 销售自产产品。(依法须经批准的项目, 经相关部门批准后依批准的内容开展经营活动。)
- 企业名称: 培富士电子技术(北京)有限公司
- 法定代表人: 李文山
- 成立日期: 1996年01月24日
- 营业期限至: 2026年01月23日
- 核准日期: 2017年06月06日

股东及出资信息

股东及出资信息截止2014年2月28日。2014年2月28日之后工商只公示股东姓名, 其他出资信息由企业自行公示。

序号	股东名称	股东类型	证照/证件类型	证照/证件号码	详情
1	朝鲜鸭绿江技术开发总会社	企业法人	企业法人营业执照(公司)	ST000008	查看

共查询到 1 条记录 共 1 页

首页

« 上一页

1

下一页 »

末页

Source: National Enterprise Credit Information Publicity System, accessed May 8, 2018.

北京市工商行政管理局

行政处罚决定书

京工商朝处字〔2018〕第128号

当事人：培富士电子技术(北京)有限公司

住所：北京市朝阳区胜古中路2号院8号楼223-225-227室

注册号：110000410111651

法定代表人：李文山

经营范围：生产指纹识别系统及民用指纹系统软件；提供技术咨询、技术服务；销售自产产品。（依法须经批准的项目，经相关部门批准后依批准的内容开展经营活动。）

按照2017年9月12日联合国安理会第2375号决议、商务部工商总局关于执行联合国安理会第2375号决议关闭涉朝企业的公告（2017年第55号）的规定要求，朝鲜实体或个人在中国境内设立的中外合资经营企业、中外合作经营企业、外资企业应自联合国安理会第2375号决议通过之日起120天内关闭。截至2018年1月9日，当事人仍未办理注销登记。

上述事实有联合国决议、商务部和工商总局公告、现场检查笔录、北京市企业信用信息网企业信息等证据佐证。

我局于2018年1月16日向当事人送达了京工商朝企监听告字[2018]第10号《行政处罚听证告知书》，告知当事人我局决定作出行政处罚决定的事实、理由、依据、内容以及当事人依法享有的陈述权、申辩权和要求举行听证的权利。当事人在法定期限内未提出陈述、申辩意见。

当事人的上述行为违反了《中华人民共和国企业法人登记管理条例》第二十条的规定，构成了不按规定办理注销登记的行为。依据《中华人民共和国企业法人登记管理条例》第二十九条第一款第

(三) 项规定，决定处罚如下：

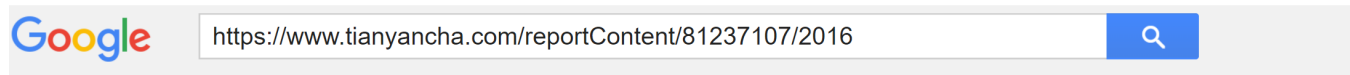
吊销当事人营业执照。

当事人如不服本处罚决定，可自接到行政处罚决定书之日起60日内向国家工商行政管理总局或北京市人民政府申请复议，也可以自收到行政处罚决定书之日起6个月内向北京市海淀区人民法院提起诉讼。

北京市工商行政管理局

二〇一八年一月二十二日

Annex 2: 2016 Annual Return Information for PEFIS Electronic Technology Co.



都在用的商业安全工具
国家中小企业发展基金旗下

查公司 查老板 查关系

请输入公司名称、人名、产品名称或其它关键词

天眼一下

2016年年报

2015年年报

2014年年报

2013年年报

培富士电子技术(北京)有限公司2016年年度报告

企业基本信息

注册号	110000410111651	企业名称	培富士电子技术(北京)有限公司
企业联系电话	64419326	邮政编码	100029
企业经营状态 ?	开业	从业人数	14人
电子邮箱	pefis@public.bta.net.cn	是否有网站或网店	否

企业通信地址	北京市朝阳区胜古中路2号院8号楼企发大厦F225	企业是否有投资信息或购买其他公司股权	无
--------	--------------------------	--------------------	---

股东及出资信息

股东	认缴出资额(万元)	认缴出资时间	认缴出资方式	实缴出资额(万元)	实缴出资时间	实缴出资方式
朝鲜鸭绿江技术开发总会社	45万元		货币	45万元		货币

企业资产状况信息

资产总额	46.74万元	所有者权益合计 ?	-33.77万元
销售总额	274.1万元	利润总额	22.83万元
营业总收入中主营业务收入	274.1万元	净利润	20.55万元
纳税总额	15.02万元	负债总额	80.51万元

Source: www.TianYanCha.com, accessed January 2018 and as it appears at time of writing.

Annex 3: Website for PEFIS Electronic Technology Co.

← → ↻ ⓘ pefis.cn/en/

Apps New Tab

PEFIS Pefis Electronic Technology (Beijing)Co.,Ltd.

Ideal Choice for Biometric Identification

Key is with You forever

Home | About us | Products | Solutions | Online order | Download | Contact

中文版 ENGLISH

Company News

Contact

Profile

Address: Qifa Mansion, Chaoyang District, Beijing
Tel: (86-10) 64419326
Zip code: 100029
E_mail: pefis@public.bta.net.cn

DOWNLOAD

Link

- GuangZhou Hysoon Electronic Co., Ltd.
- Shenzhen Union Timmy Techno-logy
- Beijing Security Equipment Co., Ltd.
- ZKS Group Inc.
- Beijing NeoNetech Co.,Ltd.

Profile

MORE<<

Pefis Electronic Technology (Beijing) Co., Ltd., established in 1982, specializes in developing fingerprint, palm-print, face identification and other biometric application products with development of the internationally progressive fingerprint identification algorithms as its main strategy.

The fingerprint application products of Pefis won golden prizes four times at the Geneva International Invention Exhibitions in Switzerland from 1990 to 1996. The Pefis fingerprint identification technology recognized as one of the most excellent techniques throughout the world

Pefis Electronic Technology (Beijing) Co., Ltd. is the first developer of a fingerprint lock in China.

Products

MORE<<

Product: Face Identification Mac
Performance: Loaded with one o

Product: Palm-print Scanner
Performance: Ink had been used to captur

Source: www.pefis.cn/en, accessed April 2018 and as it appears at time of writing.

Annex 4: Example Listings for Fingerprint Scanners on B2B Websites

www.bossgoo.com/product-detail/fingerprint-door-lock-with-north-korea-12908896.html


Sign In | Join Free My Bossgoo For Buyers For Suppliers Select Language

BOSSGOO Global trade starts here! .com

Products Search Products Search or Post Buying Request

Popular Searches: Door hole , Stainless Steel Door , Aa korea rhinestone

Home > All Categories > Construction & Decoration > Lock



Fingerprint Door Lock with North Korea Algorithm with 10 Administrators and 100 General Users

Unit Price: [Get Latest Price](#)
Payment Type: Telegraphic Transfer (TT,T/T)

Quantity: Bag/Bags

Please write your requirement here.

Your message must be between 20 to 2000 characters

Mr. Tian [Contact Now](#)

[Add to Product Favorites](#) [Add to Basket](#)

Product Details **Company Profile**

Product Description

Model No.: ZKS-L1- FD

- Introduction:
 - New version of North Korean algorithms with dependability and accuracy, identification speed obviously improved, less than 0.7second
 - Dedicate appearance with silver color
 - Stable electronic component, superior reliable, durable and low power consumption
 - Sensor with quality image, accepts dry and wet fingers
 - Streamline front panel and four key-strokes (numbers 0, 1, 2 and 3)
 - Adjust image distortion and assure fingerprint matching consistency

China

ZKS Technology Inc
[Shanghai, Shanghai, China]

Categories: Fingerprint door locks
OEM service:yes

Contact Details
-> Company Profile

[Post Buying Request](#)

Our Products Range

All Products

Fingerprint door locks

Combination biometric access contr...

Access control systems

Fingerprint access control

Smart card readers


Time recorders

Access control keypads


Facial recognition systems

Proximity-card readers

You May Like



Source: www.bossgoo.com, accessed January 2018 and as it appears at time of writing.



CE FC FINGERPRINT

[Basic Information]

Brand ZKS

Place of Origin CN

Category
Security & Protection > Access Control Systems & Products > Fingerprint Access Control

Keyword access control , biometric , fingerprint , video door phone

[Additional Information]

Material Plastic + Metal

Trader

[ZKS Group Company Limited]

China

Add to My Interests

Send inquiry

Product Detail Information

9106100000

New version of North Korean algorithms with dependability and accuracy, identification speed obviously improved, process 3,000 fingerprints, no matter good or poor, within 0.7 second.

- Built in embedded standalone module (ZKS710) with high performance SAMSUNG 32 bit X-scale CPU, big capacity FLASH and CMOS chips, it is easy to integrate with various systems.
- Alarm clock function for giving the correct time
- Be equipped with system of calendar which is on an equal footing with PC.
- Sensor with quality image, accepts dry, wet fingers.
- Support 360-degree rotation identification, easy to use.
- Adjust image distortion, assure fingerprint matching consistency.
- Accept ODM or OEM, providing system local voice, menu language, software analysis, casing-making.

It is a good option for enterprise / factory / office / bank use.

Technical Parameters:

Fingerprint capacity: 3,000
 Transaction Storage: 80,000
 Period of data: Keep data for 3 years when no current.
 Collecting rate: Port rate (9600BPS, 19200BPS, 38400BPS)
 Verification mode: 1: N
 FAR: <0.0001%
 FRR: <0.01%
 Response time: <0.7 second
 Alarm clock: embedded alarm clock
 Communication: RS232, TCP/IP, U-Disk
 The capacity of connecting net: 31 units (RS485 mode), 255 units (TCP/IP)
 Show: Time, ID number, Name
 Language: English, French, Spanish, Czech, Indonesian, Portuguese, Turkish and so on
 Working mode: Time & attendance, standalone, can working persistently

<http://www.tradekorea.com/product/detail/P243852/ZKS-T23-Fingerprint-Time-Attendance---Access-Control-System.html>

Source: www.tradekorea.com, accessed January 2018 and as it appears at time of writing.

ZKS™ ZKS GROUP CO., LIMITED

Products (20)

Safety Products

- CCTV Camera (16)
- Home Security (15)
- Surveillant Camera (7)
- Video Door Phone (14)
- Central Lock (1)
- Surveillant Equipmen (13)
- Electronic Safe (2)
- Security Gate (10)
- Fingerprint Lock (17)
- Proximity Sensor (15)
- Safe (17)
- Video Doorphone (2)
- Home Safety (13)
- Door Monitor (9)
- Parking Sensor (5)
- Video Camera (2)
- Intercom (4)
- Rescue Equipment (1)
- Door Screen (1)
- Electric Lock (2)
- Electromagnetic Lock (1)
- IC Card Lock (2)
- Dome Camera (1)

Other Companies

- ✕ Pesh Group
- ✕ Mun Mun Enterprise
- ✕ Shanghai Delex Mould Pro
- ✕ New Top Electronic Facto
- ✕ Guang
- ✕ Brand Solutions India
- ✕ Shenzhen Forzen Technolo
- ✕ Calcutta Plastic Industr
- ✕ Sengar Offset
- ✕ Dongxiao Biotechnology C
- ✕ Neil Chemical
- ✕ Shenzhen Yiergao Station
- ✕ Modest Infratructure Ltd
- ✕ Natural Nutrition Market
- ✕ Tianjinchaoxiangchemical
- ✕ Zongsglobal Service Llc
- ✕ S.N.Hardwaremart
- ✕ Emerio
- ✕ Consultanat
- ✕ Martino
- ✕ Zera Consultancy
- ✕ Mcd
- ✕ Ore
- ✕ Innospacer Engineering T

Product



ZKS-T2B Fingerprint Time Attendance & Access Control

T2B is an innovative stand-alone fingerprint recorder that can be used in both Time Attendance and Access Control applications, it adopts advanced North Korean algorithms integrates ZKS attendance management software, low price with good performance, designed specially in the purpose of popularizing the fingerprint products. It could store 3,000 fingerprint templates and 80,000 transaction records. It is a kind of selection for your attendance and security purpose. T2B-professional time attendance and access control system RS232, TCP/IP, USB, Embedded alarm clock 3000 fingerprint templates

. New version of North Korean algorithms with dependability and accuracy, identification speed obviously improved, process 3,000 fingerprints, no matter good or poor, within 0.7 second.

- . Built in embedded standalone module (ZKS710) with high performance SAMSUNG 32 bit X-scale CPU, big capacity FLASH and CMOS chips, it is easy to integrate with various systems.
- . Build in alarm clock to give correct time
- . Be equipped with system of calendar and is on an equal footing with PC.
- . Sensor with quality image, accepts dry, wet fingers.
- . Support 360-degree rotation identification, easy to use.
- . Adjust image distortion, assure fingerprint matching consistency. . Accept ODM or OEM, providing system local voice, menu language, software analysis, casing-making.
- . It is a good option for enterprise / factory / tax / bank use.

Technical Parameters:

User capacity: 3000 (Can expand to 5000, 10000)
 Transaction Storage: 80000 (Can expand to 200,000)
 Period of data: Keep data for 3 years when no current
 Collecting rate: Port rate (9600BPS, 19200BPS, 38400BPS)
 Verification mode: 1: N, 1:1
 FAR: <0.0001%
 FRR: <0.01%
 Response time: <0.7 second
 Communication: TCP/IP, USB
 Alarm clock: embedded alarm clock
 Door access control: Connect EM lock and EM bell.
 The capacity of connecting net: 31 units (RS485 mode), 255 units (TCP/IP)
 Distance: 1200m (RS485)
 Show: Name, time, ID number
 Language and voice: English, French, Spanish, Czech, Indonesian, Portuguese and Turkish etc.
 Working mode: Time & attendance, standalone, can work persistently
 Time & Attendance mode: Fingerprint and password
 Save function: Turn off device automatically for saving
 External function (access control): Connect to external E-lock, E-bell and annunciator
 Size: 188*50*146mm
 Power supply: DC9V, 1A (AC 100V to 240 V, 50 to 60 Hz)
 Warranty of period: 24 months
 Temperature and humidity: 0 - 45, 20%-80%
 Optional: Proximity or Mifare card reader, USB and Backup battery
 Applications: Factory/office/bank/hotel etc.

Modal No. : ZKS-T2B



SXL-33 FINGERPRINT TIME ATTENDANCE MACHINE

R4,250-00

Download the software for the SXL-33 Fingerprint and Time Attendance Machine [HERE](#) »



Add to cart

Category: [Biometrics Time Attendance and Access Control Devices](#) Tags: [biometric machine](#), [clocking machine](#), [fingerprint machine](#), [time attendance terminal](#)

Built in battery back up

Description

DESCRIPTION

1. Download the software for the SXL-33 Fingerprint and Time Attendance Machine [HERE](#) »
2. Click [here](#) to download the SXL Series Software Manual »
3. Click [here](#) to read about Biometric Technology »

Features:

- Stand-alone terminal with **built in battery back up**
- SXL-33 is professional time attendance & access control system designed for factory, school, bank, office from medium to large size businesses.
- SXL-33 can also be used out in the field, building sites etc
- High operation speed and registration capacity. Using the USB cable protocol, 5-10 times faster than traditional serial ports.
- SXL-33 adopts new version of North Korean algorithms with dependability and accuracy.
- Adopts the ATMEL industrial chip, 200M dominant frequency.

Source: <http://machinetech.co.za/shop/sxl-33-fingerprint-time-attendance/>, accessed February 2018 and as it appears at time of writing.

ET90A Fingerprint Time Attendance & Access Control

Features

Specification

Drawing

Download

ProductSeries

• Info

- * Time Recorder ET90V is professional Fingerprint Time Attendance and Access Control System with ARM 9.
- * ET90V supports Net connection(31 units (RS485 mode), 255 units (TCP/IP) User can view the device via remote visit.
- * ET90V support multi languages.
- * In addition, it has embedded alarm clock.

• Feature

- * **New version of North Korean algorithms with dependability and accuracy, identification speed obviously improved.**
- * Fingerprint Capacity: 3000; Record Capacity:60000;
- * Built in embedded standalone module with high performance ATMEL, big capacity FLASH and CMOS chips, it is easy to integrate with various systems.
- * Embedded with Alarm function.
- * Be equipped with system of calendar and is on an equal footing with PC.
- * Sensor with quality image, accepts dry, wet fingers.
- * Support 360-degree rotation identification, easy to use.
- * Adjust image distortion, assure fingerprint matching consistency.
- * Accept ODM or OEM, providing system local voice, menu language, software analysis, casing-making.
- * It is a good option for enterprise / factory / tax / bank use.

Source: www.epordo.com, accessed January 2018 and as it appears at time of writing.

Annex 5: Comparison of Fingerprint Scanners



Fingerprint scanner sold by a Southeast Asian company, where the algorithms integrated into the product allegedly won gold prizes at the International Exhibition of Inventions in Geneva in the 1990s.

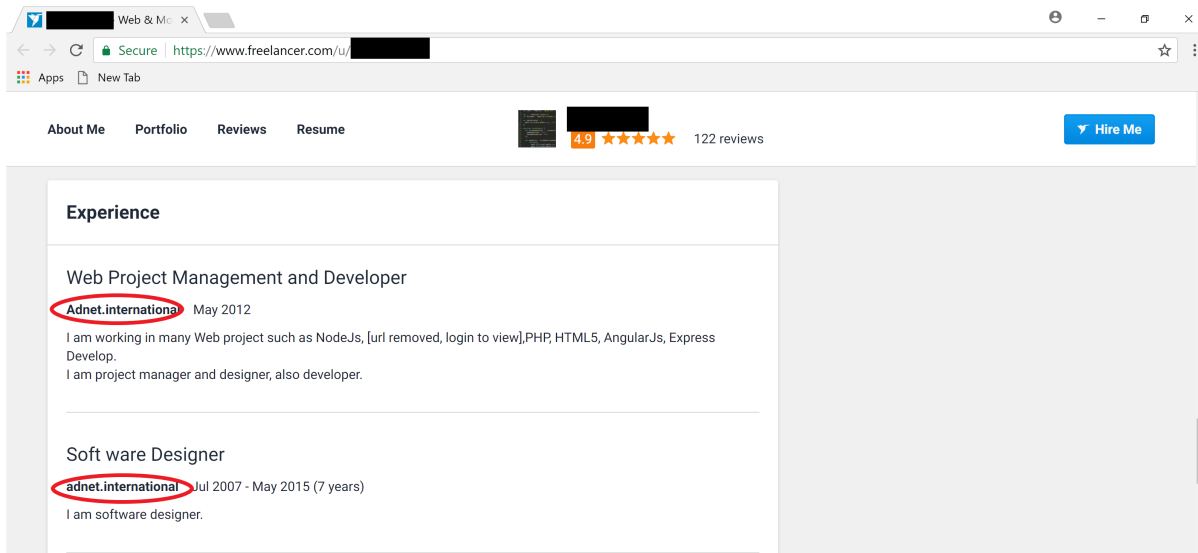
Source: Company's website, as accessed by the authors in February 2018, and as displayed at the time of writing.



Fingerprint scanner sold by a company linked to from the PEFIS homepage. The corresponding advertisement boasts "world class algorithms". It is unclear whether the similarity in the display screens exists because of shared underlying technology, or for other reasons.

Source: Company's website, as accessed by the authors in February 2018, and as displayed at the time of writing.

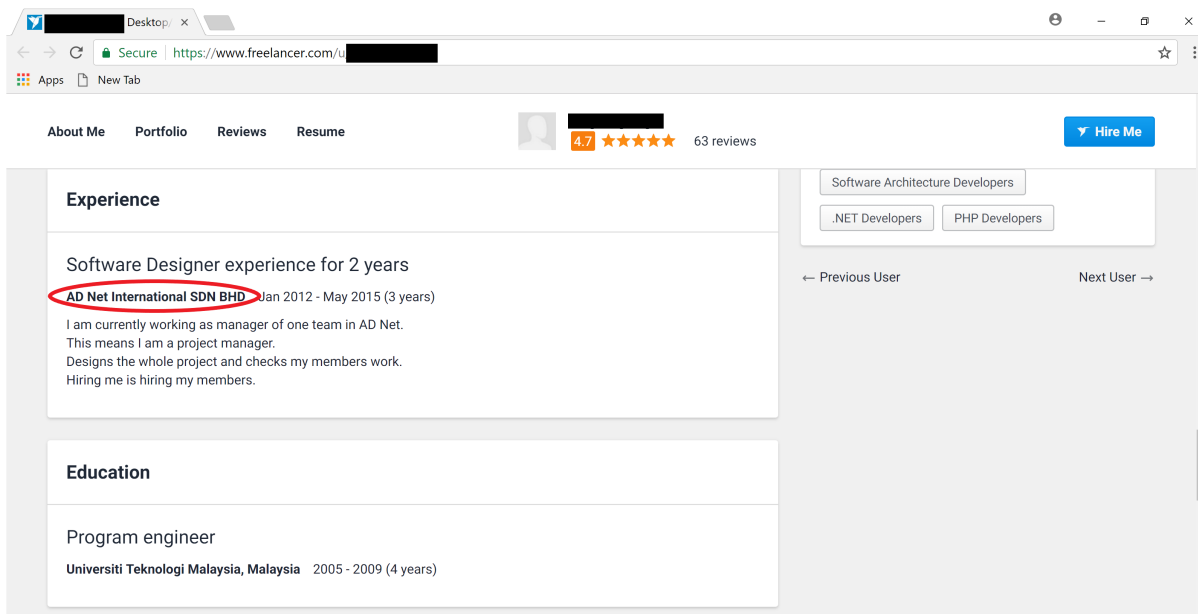
Annex 6: Freelancer Profiles Possibly Connected to Adnet International



The screenshot shows a browser window with the URL [https://www.freelancer.com/u/\[redacted\]](https://www.freelancer.com/u/[redacted]). The profile header includes navigation links for 'About Me', 'Portfolio', 'Reviews', and 'Resume', a profile picture, a 4.9 star rating with 122 reviews, and a 'Hire Me' button. The 'Experience' section contains two entries:

- Web Project Management and Developer**
Adnet.international May 2012
I am working in many Web project such as NodeJS, [url removed, login to view],PHP, HTML5, AngularJS, Express Develop.
I am project manager and designer, also developer.
- Soft ware Designer**
adnet.international Jul 2007 - May 2015 (7 years)
I am software designer.

Source: www.freelancer.com, accessed February 2018 and as it appears at time of writing.



The screenshot shows a browser window with the URL [https://www.freelancer.com/u/\[redacted\]](https://www.freelancer.com/u/[redacted]). The profile header includes navigation links for 'About Me', 'Portfolio', 'Reviews', and 'Resume', a profile picture, a 4.7 star rating with 63 reviews, and a 'Hire Me' button. The 'Experience' section contains one entry:

- Software Designer experience for 2 years**
AD Net International SDN BHD Jan 2012 - May 2015 (3 years)
I am currently working as manager of one team in AD Net.
This means I am a project manager.
Designs the whole project and checks my members work.
Hiring me is hiring my members.

The 'Education' section contains one entry:

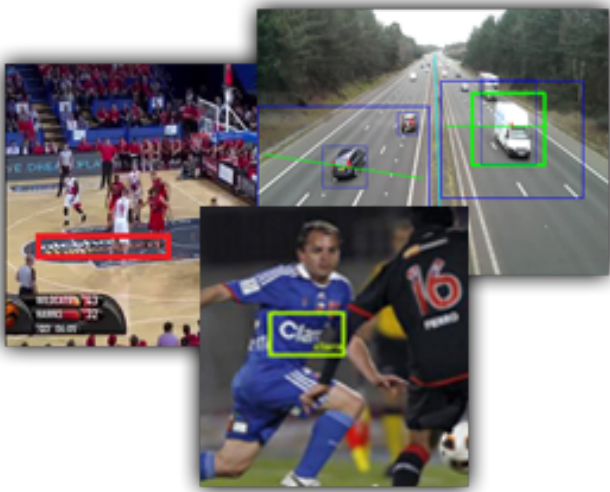
- Program engineer**
Universiti Teknologi Malaysia, Malaysia 2005 - 2009 (4 years)

On the right side of the profile, there are skill tags: 'Software Architecture Developers', '.NET Developers', and 'PHP Developers'. Navigation links for 'Previous User' and 'Next User' are also visible.

The image is a screenshot of a web browser displaying a profile on the Freelancer.com website. The browser's address bar shows a secure connection to <https://www.freelancer.com/>. The profile header includes navigation links for 'About Me', 'Portfolio', 'Reviews', and 'Resume', a profile picture placeholder, a 4.7 star rating with 63 reviews, and a blue 'Hire Me' button. The 'Qualifications' section lists 'IT Professor (2013)' from 'AD Net International' with the text 'I have IT professor certificate from AD Net International.' The 'Publications' section is titled 'Many Software Products' and lists 'No' publications. Underneath, the text reads 'I have published too many software products on my hand. Such as ev360ultimate, car recognition system, general desktop applications and mobile applications and etc.' The name 'AD Net International' is circled in red in the original image.

Source: www.freelancer.com, accessed January 2018 and as it appears at time of writing. Note that the authors cannot confirm that “Adnet International Sdn Bhd” and “AD Net International Sdn Bhd” (the latter as displayed on the above freelancer profile) refer to the same entity. No entity by the name of “AD Net International Sdn Bhd” is registered in Malaysia.

Annex 7: Profile information for “Richard Minh”



Source: Snippet of the www.future-techgroup.com website page for “object recognition”, accessed July 2017.

Computer Vision - Face F x

Secure <https://www.guru.com/service/computer-vision-face-recognition-anpr/vietnam/hanoi/hanoi/3587704>

Richard Minh ♥
Hanoi, Hanoi, Vietnam

Get a Quote

- Overview
- Portfolio
- Feedback
- Skills

← Computer Vision - Face Recognition, ANPR

I'm a Computer Vision experts team manager whose team has built some excellent SDKs performing image processing. Specifically, Face Recognition SDK is even better than several commercial SDKs such as VeriLook or Luxand which is very useful in building surveillance system. ANPR is based on good top SDKs so its accuracy is reliably high. Logo Detection is also one of the core products which my team can deliver. In addition, we can do a lot of things related to computer vision.

\$50 / Hour
\$2,000 minimum budget

Skills & Expertise


android development asp.net c# c++ computer vision delphi dotnet image processing
ios development opencv processing vb.net

Related Work Collections

- Face Recognition
- Vehicle Counting System
- Logo Detection

Source: www.guru.com profile for “Richard Minh”, accessed July 2017.

Annex 8: Future Techgroup Page for Vehicle Recognition Software

support@future-techgroup.comHome About Products

Vehicle License Number Recognition

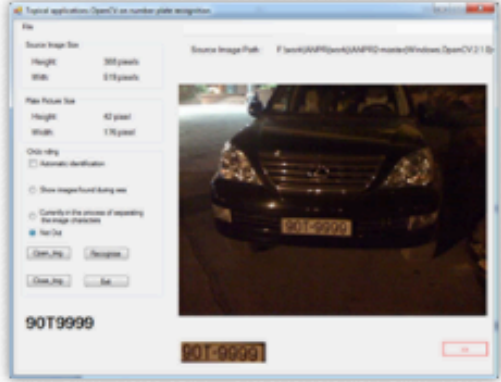
Download »

This program can be used in various kinds of system such as vehicle volume monitoring system, vehicle-theft protection system, road charges auto-management system, criminal pursuing system and so on.

Recognition Principle

It is divided largely into detection of the license number plate and recognition of number. The stage of detection of license plate is the stage of detection of the license plate from camera's image. There are several methods and typical examples are the method using information of shape of plate, neuron network method, AdaBoost method and so on.

The method using information of shape of plate which is the first used is the method which gets edge image and selects rectangular shape which can become license plate from the image. This has advantage of simplicity and disadvantage of low recognition ratio, so it is no used independently but combined with other methods. The methods of neuron network and AdaBoost learn previously many license plates and find target. They are used widely nowadays because they have high recognition ratio. The recognition of the license plate is performed by recognition of number from license plate given. This can be seen as one kind of OCR and it can get high recognition ratio because recognition target is limited to license numbers and various restricted kinds can be added.



QA

1. Can this software be used both of image and video from camera?
It can be used for both of them. It can support full real time processing for video from camera.
2. Can this software recognize license numbers of all countries in the world?
You know, it is different the form of license numbers in every country. This software uses form of license numbers of specified country increasing recognition ratio. For example it is very difficult to identify English word 'l' or number '1'. But if we use form of license number, we can identify easily because the English words and numbers are restricted by their position. So in order to recognize license numbers of every country it is necessary to correct program according to form of license numbers of their country. Now this software can be used practically in United States and Europe, especially in Turkey.

Source: www.future-techgroup.com, accessed July 2018.

OCCASIONAL PAPERS AVAILABLE FROM CNS

online at https://nonproliferation.org/category/topics/cns_papers

#36 • North Korea's Information Technology Networks

#35 • Countering North Korean Procurement Networks Through Financial Measures: The Role of Southeast Asia

#34 • Open-Source Monitoring of Uranium Mining and Milling for Nuclear Nonproliferation Applications

#33 • WMD Proliferation Risks at the Nexus of 3D Printing and DIY Communities

#32 • Taiwan's Export Control System: Overview and Recommendations

#31 • Revisiting Compliance in the Biological Weapons Convention

#30 • Crowdsourcing Systems and Potential Applications in Nonproliferation

#29 • The Verification Clearinghouse: Debunking Websites and the Potential for Public Nonproliferation Monitoring

#28 • Geo4nonpro.org: A Geospatial Crowd-Sourcing Platform for WMD Verification

#27 • Searching for Illicit Dual Use Items in Online Marketplaces: A Semi-Automated Approach

#26 • 2016 Symposium Findings on Export Control of Emerging Biotechnologies

#25 • Outlawing State-Sponsored Nuclear Procurement Programs & Recovery of Misappropriated Nuclear Goods

#24 • Strengthening the ROK-US Nuclear Partnership

#23 • Replacing High-Risk Radiological Materials

#22 • A Blueprint to a Middle East WMD Free Zone

#21 • Biotechnology E-commerce: A Disruptive Challenge to Biological Arms Control

#20 • Countering Nuclear Commodity Smuggling: A System of Systems

#19 • Alternatives to High-Risk Radiological Sources

#18 • Stories of the Soviet Anti-Plague System

#17 • Ugly Truths: Saddam Hussein and Other Insiders on Iraq's Covert Bioweapons

#16 • Rethinking Spent Fuel Management in South Korea

#15 • Engaging China and Russia on Nuclear Disarmament

#14 • Nuclear Challenges and Policy Options for the Next US Administration

#13 • Trafficking Networks for Chemical Weapons Precursors: Lessons from the 1980s Iran-Iraq War

#12 • New Challenges in Missile Proliferation, Missile Defense, and Space Security

#11 • Commercial Radioactive Sources: Surveying the Security Risks

#10 • Future Security in Space: Commercial, Military, and Arms Control Trade-Offs

#09 • The 1971 Smallpox Epidemic in Aralsk, Kazakhstan, and the Soviet Biological Warfare Program

#08 • After 9/11: Preventing Mass-Destruction Terrorism and Weapons Proliferation

#07 • Missile Proliferation and Defences: Problems and Prospects

#06 • WMD Threats 2001: Critical Choices for the Bush Administration

#05 • International Perspectives on Ballistic Missile Proliferation & Defenses

#04 • Proliferation Challenges and Nonproliferation Opportunities for New Administrations

#03 • Nonproliferation Regimes at Risk

#02 • A History of Ballistic Missile Development in the DPRK

#01 • Former Soviet Biological Weapons Facilities in Kazakhstan: Past, Present, and Future



nonproliferation.org



Middlebury Institute of
International Studies at Monterey
James Martin Center for Nonproliferation Studies