NORTH KOREA STEPS UP ON SEVERAL FRONTS

An increasingly intrusive North Korean intelligence effort is gathering information even on its partners, Russia and China.

North Korea finances its weapons programme by coercively controlling and extracting profits from its overseas labour diaspora.

Businesses must be vigilant against North Korean front companies to avoid sanctions breaches. Thorough background checks on potential partners are essential whenever their identity or origin is in doubt.

In recent years, North Korea, which has provided Russia with weapons, ammunition and soldiers, has increased its activity in other areas. North Korean diplomats have begun to actively gather intelligence not only in Europe but also in Russia and China.

The regime in Pyongyang seeks access to any information that could help advance its domestic defence industry, manufacturing capabilities, technology and other sectors. Intelligence is gathered both by diplomats and their subordinates. Some embassies have even created posts for "science and technology attachés", whose tasks include collecting large volumes of scientific articles and purchasing various products through procurement networks.

The North Korean regime is interested in a wide variety of information, technology and equipment, including:

- production technologies and materials for anti-fouling paint intended for warships and submarines;
- construction plans for nuclear power plants;
- rare-earth metals technology from Russia;
- devices used in satellites;
- seeds for cultivating new agricultural varieties;
- information on a ball-bearing plant in Russia;
- information needed to build new factories in North Korea, including fertiliser and cement plants and facilities for producing high-pressure components;
- information for establishing a fertiliser plant;
- biotechnology;
- artificial intelligence and data technologies;
- technologies for generating electricity from wave and tidal energy;
- graphene (used in the defence industry and other sectors);
- nano- and composite materials and nanotechnology;
- electronics;
- electric tractors from China;
- technologies for processing rock and for mining.

North Korea's latest intercontinental ballistic missile, the Hwasong-20, unveiled at a military parade marking the 80th anniversary of the Workers' Party. Its reported range is 15,000 km.

Source: CGTN

In China, North Korean intelligence is most active in the northern cities of Beijing, Dalian and Shenyang. In Russia, its activity is concentrated in Moscow and in Blagoveshchensk, a city in the Far East on the border with China. North Korean authorities are also seeking to send students to Russian universities to study nuclear and other high-technology fields.

A LABOUR DIASPORA THAT FILLS THE REGIME'S COFFERS

Pyongyang has an unusual source of income: North Korea sends its workers abroad, primarily to Russia and China, to generate revenue for the regime and its weapons programmes. According to United Nations estimates, the number of these workers exceeds 100,000.

The North Korean regime accumulates nearly half a billion euros from its labour diaspora.

The bulk of the wages paid to these workers flows into the state treasury, leaving the workers with only a tiny portion of their earnings. For example, highly paid IT professionals are required to surrender nearly 90% of their earnings to the North Korean government. Given that an IT specialist can earn hundreds of thousands of euros a year and that there are several thousand of them working globally, the regime generates hundreds of millions of euros annually from this workforce. Overall, it accumulates nearly half a billion euros from the entire labour diaspora.

North Koreans sent abroad work mainly in construction and industry, and their living and working conditions are often inhumane. They are frequently tasked with obtaining specific goods in their host countries and sending them back to North Korea – for example, food, clothing, medicines, cigarettes, furniture, other consumer goods, and even building materials.

North Koreans working abroad often look for ways to earn additional income and improve their living conditions. A common method is selling traditional Korean medicine products manufactured in North Korea. The regime also sends doctors overseas, and they, too, may use deceptive practices to extract more money from their patients, diagnosing illnesses the patients do not have, and then selling them unnecessary medicines.

NORTH KOREAN COMPANIES OPERATING UNDER COVER

North Koreans have become increasingly active in the IT sector – such as in developing cryptocurrencies and blockchain technologies – and they offer services to clients around the world while attempting to conceal their true origins. To do this, they often use falsified IDs and front companies registered in other countries, including China and Russia. For example, Yanbian Silverstar Network Technology Co., Ltd., based in China, and Volasys Silver Star, based in Russia, are in fact run by North Koreans closely linked to the Munitions Industry Department, which is responsible for developing North Korea's ballistic missiles. There is a real risk that Estonian companies might unknowingly become clients of these seemingly legitimate firms.

The true purpose of North Korean IT companies is again to generate revenue for the Pyongyang regime and its weapons programme. It is crucial to remember that any activity that helps finance North Korea's armaments programme is subject to international sanctions and is therefore punishable. Penalties range from fines to lengthy prison sentences.

Any activity that helps finance North Korea's armaments programme is subject to international sanctions and is therefore punishable.

North Korean IT specialists also attempt to seek employment directly with European and American companies. In one documented case, a Western firm unwittingly hired a North Korean national who used a false identity and work history. The individual exploited the access granted as part of their position to infiltrate the company's IT systems and download confidential business information. When the company later attempted to terminate the employment, the individual threatened to make the information public unless they were paid a specified amount.

In this context, it is critical for Estonian companies to verify the true identity and background of job applicants from third countries. Additionally, firms must remain vigilant when operating in the cryptocurrency and blockchain sectors to ensure that their business partners are not front companies for North Korea.