AL govt's secret surveillance state

FROM PAGE 1

The equipment listed and their total value calculated for this story are based on a limited dataset and imports recorded under specific Harmonised System (HS) codes. Similar products may have been imported under different HS codes, which are not reflected in this report.

While surveillance systems are essential to prevent crimes, track criminals, gather intelligence and neutralise threats to national security, experts warn that without transparency and due legal process, such a powerful surveillance system can be abused to suppress political opponents and snoop on ordinary citizens in violation of their constitutional right to privacy.

MASS SURVEILLANCE SYSTEM

While the Rab and police had been focussing on building specific target-based surveillance, the NTMC opted to build a mass surveillance infrastructure by installing an ILIS.

By 2022, it purchased the components necessary to monitor and intercept the everyday communications of citizens, store that data centrally, and ensure access by various law enforcement agencies, documents show.

Of the Tk 1,382 crore spent on surveillance equipment by the NTMC, police and Rab between 2016 and 2024, the NTMC's expenditure alone accounted for more than 65 percent (Tk 904.39 crore).

A copy of a contract agreement shows that US-based Yaana Technologies and its UK subsidiary Yaana Limited helped the NTMC set up the ILIS infrastructure for Tk 546.7 crore.

The ILIS platform, having 10 components, aims to "collect, collate, analyse and disseminate all information to law enforcing agencies that provide pinpoint targets who are actively and passively threatening national security," reads the contract.

The first two components are the mobile and data interception systems capable of intercepting "any individual's all types of electronic communication" as well as data and internet communication "originating, terminating and passing through Bangladesh".

The third component is a mass data acquisition system capable of collecting all internet communication from the national gateway and national internet exchange levels.

The fourth component allows law enforcement agencies to monitor, intercept, and analyse any person's communications across all connected networks and operators, all from a single control point.

The fifth component, called a "unified target profiling system," can collate all intercepted data, analyse communication patterns and give a "full 360 degree picture of any individual over time, place and communication platform".

The sixth and seventh components are a call detail record analysis system and a geolocation system, respectively.

The eighth and ninth components are a digital command centre inside the NTMC premises and an overall operation and management system.

The 10th component includes an "active intrusion system", which can "stealthily capture from any target device, is not limited by encryption or any encoding mechanism, does not depend on user interaction to perform operation and presents all application, file and communication content," contract documents read.

This essentially meant capturing the whole device, according to experts.

The government can inject malware into users' devices using very benign apps that they may have been downloaded to access services, and gain access so much so that the authorities can essentially see the entire device, said Sabhanaz Rashid Diya, executive director of Tech Global Institute, a technology nonprofit, which has long been studying the surveillance landscape of Bangladesh.

"There is one malware that can track keyboard strokes, so it can see what you are typing. Another software can create a backdoor in iOS systems, read messages and download contacts," she added.

The last component of the ILIS also involved a satellite phone interception system.

The Daily Star has no information on the extent to which citizens were targeted by this system during Sheikh Hasina's rule. It is also unclear how the system is being used at the moment.

In a rewritten response to The Daily Star, the NTMC admitted having installed the ILIS systems and said that some of its components are still in operation for intelligence gathering and investigation purposes.

"As part of the reform process, NTMC, under the Ministry of Home Affairs, is working on formulating an Act/Ordinance related to Lawful Telecommunication Interception with special attention to Privacy of the Citizens and maintaining International Standard," it said.

HOW THE SURVEILLANCE WORKS

The Daily Star shared the list of components purchased by the NTMC with our in-house network specialists. Using information about the components, they reconstructed the ILIS network (see the operational and network structure online) as outlined by its contract.

The surveillance with ILIS begins by intercepting data packets from the internet infrastructure, including undersea fibre optic cables, satellite systems, ISP routes, and telecom networks.

To do this, it uses three Copper Tap Modules (10/100/1000), which split incoming and outgoing data streams and sends them to monitoring ports. Fibre Taps mirrors high-speed fibre optic traffic and redirects it for analysis.

These feeds are then processed by DeepProbe units, which prepare the data for inspection.

The second step is the decryption of the encrypted traffic. SSL(secure sockets layer) is a way to keep data safe when it travels between a browser and a website by locking it with encryption.

The ILIS uses a SSL Decryption Platform, which intercepts secure connections, decrypts the traffic for inspection, then re-encrypts it before forwarding the data.

Data show the NTMC purchased 15 DeepProbe monitor ports from Yaana, which identifies application usage (e.g., WhatsApp, Signal), timestamps, data volumes, IP addresses, communication types, and user behaviour patterns.

A GSM/Signalling Network Monitoring The Platform is also deployed to extract metadata from voice calls, SMS, and mobile internet traffic. This allows the NTMC to build user profiles based on activity patterns, even without accessing message content.

Its Social Media Monitoring System, purchased from Ecomtrade Holdings Pte Ltd for Tk 45.11 crore, is capable of tracking activity across platforms.

Kamal Shakil, the manager of foreign trade at Ecomtrade, told The Daily Star that this platform was procured from a Netherlands-based supplier and that they were only the reseller.

To store the large volume of data, the NTMC acquired two DRS Hadoop Data Node Hardware units. GPS-disciplined NTP servers ensured all intercepted data was timestamped accurately and consistently across systems.

All these were permitted by as many as 22 laws, including the Bangladesh Telecommunications Regulation Act, 2001, said Diya, the executive director of TGI.

"Bangladesh's surveillance regime is rooted in colonial-era laws that permit spyware use, communication interception, and broad law enforcement access without adequate safeguards," she said.

She called it a "security-first framework" and said that it "spans not just telecom and cyber laws, but also narcotics, anti-terrorism, trade regulations, and import controls -- creating a system ripe for abuse."

TARGET-BASED SURVEILLANCE

Import data obtained by this newspaper begins with the purchase of a radio frequency jammer by the Rab in 2016, from Samel 90, a Bulgarian electronics and defence manufacturer.

A radio frequency jammer is not a surveillance device per se – it is a device that deliberately disrupts wireless communication by transmitting interfering signals on the same frequencies used by phones, GPS, or Wi-Fi, effectively blocking them.

However, it can silently thwart gatherings. On multiple occasions during the 15-year rule of the Awami League, BNP leaders, activists, and journalists reported that they were unable to place or receive calls from the rally venues.

In 2017, the Rab bought a similar network jammer, but this one could be mounted on a vehicle.

The same year, police purchased an IMSI catcher from Cyprus-based Tiersec.

An IMSI catcher, or International Mobile Subscriber Identity catcher, is a surveillance tool designed to monitor, locate, and occasionally intercept mobile phone activity. It operates by mimicking a real cell tower, causing nearby phones to connect to it rather than to an authentic cellular network. The IMSI is a unique number assigned to each mobile SIM card and is used to pinpoint a target within a larger crowd.

Import data show that the police bought more IMSI catchers – one of them bike-mounted – in 2019 and 2022 from Canadian firm Octasic. In total, the police spent Tk 43 crore on IMSI catchers, signifying police's dependence on such snooping devices.

In 2019, they also purchased a mobile tracker server from a German supplier, cleared through Bangladeshi-owned, Singapore-based Panmark Impex.

Two years later, the police acquired a Man-in-the-Middle (MitM) System Detector and Locator -- a specialised tool designed to intercept and monitor communications in real time.

The system works by mimicking trusted networks or devices to gain access to sensitive information, including phone calls, messages, emails, and online activity. It can sometimes also break through encrypted connections to expose protected data. Additionally, it can track the physical location of those being monitored.

In 2022, both police and the Rab stocked up on their interception infrastructure.

That year, police purchased a Satcom Analyser produced by Swiss surveillance company ATECS AG via a Singaporean firm. A Satcom analyser is a tool that can be used to monitor, intercept, and analyse satellite-based communications, including satellite phones and terminals.

The Rab, on the other hand, armed itself with a backpack IMSI catcher and two units of unspecified mobile communication analysers from Octasic. These analysers can generally track which devices are connecting to which networks, their unique identification numbers, phone numbers, locations, and collect information on call logs and text messages.

In 2023, police purchased a portable surveillance and signal intelligence (SIGINT) device from Cyprus-based company Delhaze Ltd. This device can detect, intercept and geolocate wireless communications like mobile phones, radios and satellite links.

The next year, they purchased an even powerful network-jammer -- a drone that could sweep across an area blocking communications.

CIRCUMVENTING EXPORT BANS

At least 20 companies exported surveillance equipment to Bangladesh from 23 countries.

Twelve of those countries -- UK, US, Bulgaria, Czech Republic, Germany, Cyprus, France, Italy, Denmark, Netherlands, Poland, Belgium -- prohibit export of surveillance equipment to repressive regimes.

The US Department of Commerce's Bureau of Industry and Security's Entity List blocks American suppliers from providing technology to actors committing human rights abuses.

The European Union's export regulations also do not allow for surveillance sales to countries if there is proof that they could be used to commit human rights abuses.

Many of these countries used clearing houses in Singapore, Cyprus and the United Arab Emirates to circumvent the export restrictions.

Kamal Shakil, the manager at Ecomtrade which supplied some surveillance equipment to the NTMC, said, "The NTMC contacted the Netherlands-based supplier directly. The supplier did not want to export directly to Bangladesh and wanted to come through a reseller. We did not even know what the product being sent to Bangladesh was. We faced no restrictions in the Netherlands. Singapore provides transshipment facilities for many imports coming into Bangladesh."

At least three of the companies Bangladesh sourced from -- Passitora, Teledyne and Tiersec -- have Israeli links.

According to its company registration documents, Passitora Ltd, headquartered in Cyprus, is a rebranded version of WiSpear and is linked to Israeli intelligence networks through its founder, Tal Jonathan Dilian, a former Israeli army officer currently under US sanctions for rights abuse. One of its directors at the time of NTMC's purchase was Mivtah Shamir Technologies, a Tel Aviv-based firm.

The NTMC purchased a portable surveillance system from Passitora, costing Tk 52.1 crore.

The company Tiersec is located in Cyprus, but its director is Israeli surveillance entrepreneur Yaron Baratz, and is effectively an Israeli company operating out of Cyprus.

Baratz is the founder of an Israeli surveillance company called Septier.

Teledyne FLIR Detection, Inc, a US manufacturer of thermal and surveillance technologies, maintains a research and development centre in Israel. Its subsidiaries and DVTEL Israel Ltd are incorporated in Israel.

While Yaana Technologies scored the most expensive bid, Singapore-based, Bangladeshi-owned logistics firm Panmark Impex came in second place, having exported surveillance equipment worth Tk 366 crore. They sent 20 shipments, of which 75 percent went to the police and the rest went to the Rab.

The company's Managing Director Khorshed Alam Chowdhury said they are not legally liable for any abuse of the devices they supplied.

"Our supplied equipment are tactical "IMSI" device having no surveillance capabilities; primarily used for finding convicted criminals. To tell you the truth, we are unaware of any instances where our supplied equipment has been used in any act of human rights violations," said Chowdhury.

"Even then, if any misuse of supplied equipment occurred towards violation of human rights, it is the end users who have to take the total responsibility for such an occurrence," he said.

Singapore-based Ecomtrade Holdings Pte Ltd is in the top 10 suppliers, providing Tk 45.1 crore of equipment. The company is led by Bangladeshi-origin businessman Nurul Amin.

Sixteen other companies supplied goods in 146 shipments worth Tk 418 crore.

One of those suppliers, called Spider Digital Innovation FZE, despite being UAE-based, is Bangladeshi-led. The company belongs to Kazi Monirul Kabir, who was formerly the communications lead at two major telecom operators in Bangladesh. He is also the former country manager for Google in Bangladesh.

They provided the NTMC with at least 30 shipments, including the SSL decryption platform, a covert surveillance tool that silently eavesdrops on mobile calls and data called Tactical Passive Cellular Interceptor, and components for an internet traffic inspection system called the Gigamon GigaVUE-HC3 visibility platform.

Kabir categorically stated that they never supplied systems that could be used for human rights abuses. Regarding the Gigamon platform, he said, "You have correctly noted that it gives network traffic visibility, but the project is based on metadata collection, focussing solely on gathering metadata for visibility purposes. There is no option to collect user content.

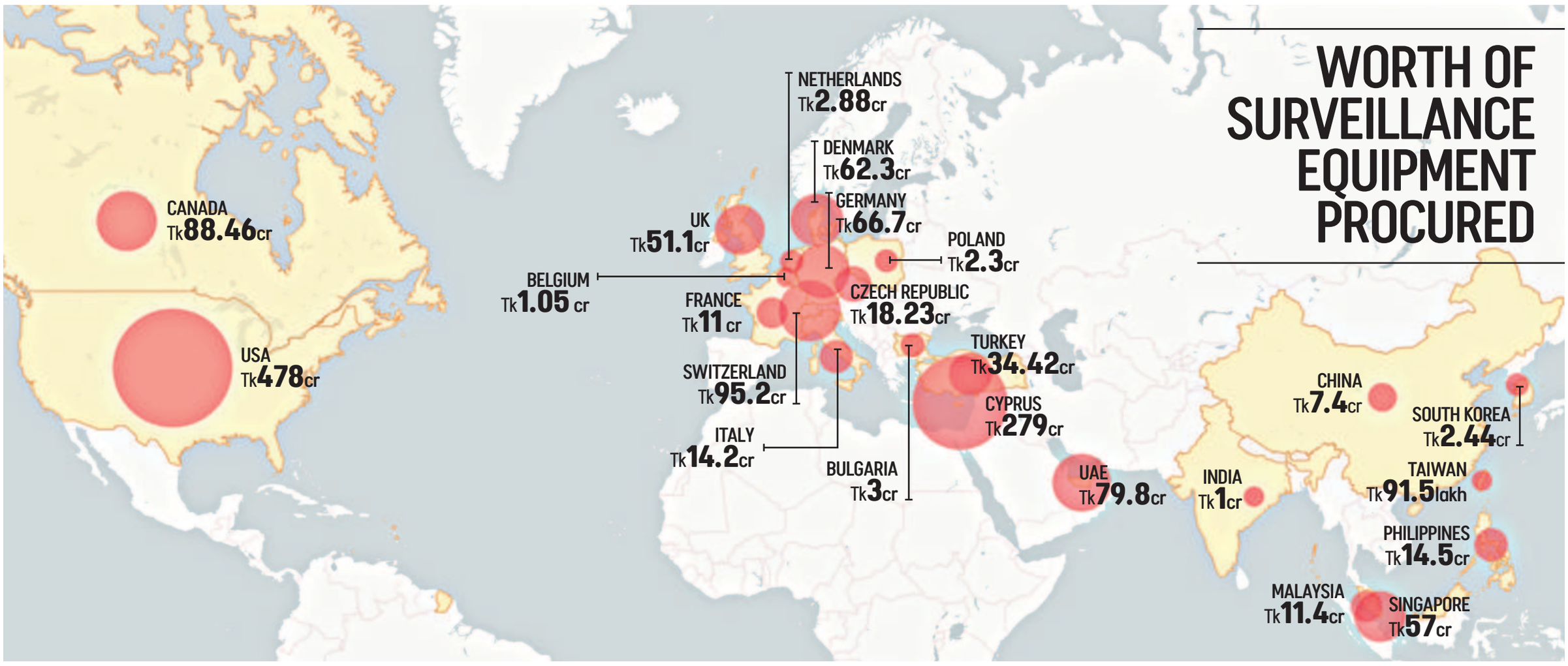
"We explicitly state that we did not supply components for, nor were we involved in the construction of a broader network traffic visibility infrastructure that collects user content."

Kabir added that there were no export restrictions.

The Daily Star also emailed Yaana, Teledyne, Octasic, Vehere and Roya International, the company which had supplied goods from the Swiss surveillance company ATECS AG, but did not receive any response. We also sent written questions to the Rab and police, but they did not respond either.

Data and visualisation: Muhammad Imran

Graphics: Anwar Sohel



NTMC'S REPLY TO OUR QUESTIONS

TDS: What steps have been taken to take out the ILIS from operation?

NTMC: Lawful Telecommunication Interception Systems are technical platforms essential for law enforcement agencies, investigation agencies and intelligence agencies to collect necessary information to investigate cases and identify the accused. Countries around the world have such practice. NTMC established and maintains a few basic LI platforms to support mentioned agencies.

TDS: The NTMC had installed Deep Packet Inspection (DPI) devices for monitoring and filtering subscriber internet usage. Are these still operational in Data Centres 3 and 4?

NTMC: DPI devices are not in operation now. Their functionality is being tested. However, a few online betting sites prohibited by the government have been blocked as test purposes. The future usage of this system will depend on proper guidelines/ policy.

TDS: In 2022, the NTMC purchased a system from Intersec (France) that allowed the NTMC to get instant, precise and historical location of individuals. Is the system installed by Intersec still active?

NTMC: Yes, the system is active now. Law enforcement agencies, investigation agencies and intelligence agencies utilise the service to locate the accused and victims. More importantly, 999 and Fire Services use this system to instantly locate the victims.

TDS: Does the NTMC still pull customer data (Registration information, CDR, SMS content, NID, roaming status, recharge details, package details etc). using an API plugin provided by telecom operators? If yes, then do you obtain a warrant from a magistrate beforehand?

NTMC: As said before, law enforcement, investigation and intelligence agencies utilise the platform to investigate cases and identify the accused. Mentioned agencies complete necessary processes at their end before collecting information.