The Daily Star
FOUNDER EDITOR: **LATE S. M. ALI**

Biman can't seem to stay out of trouble

It risks being stripped of the right to fly to KSA after latest debacle

WE are quite concerned to learn about the failure of Biman Bangladesh Airlines to operate flights to Saudi Arabia with one general sales manager. According to a report, the General Authority of Civil Aviation (GACA) of Saudi Arabia had set a January 1, 2022 deadline for Biman to start operating with a single agent, instead of two. Although Biman appointed a new sales agent on January 1, it could not function properly due to complications over arrear settlements with previous agents and several other issues, including transferring the *iqama* (work permit) of Biman employees. Now, if Biman authorities cannot solve these issues and comply with the GACA directive, the national flag carrier may lose its right to fly to that country.

The situation, as per the Bangladeshi ambassador to the kingdom, is "horrifying" because if Biman loses its right to operate Saudi flights, it will affect thousands of our migrant workers who take its flights to go to their destinations of work and return home. Currently, the carrier sends planes to four destinations in Saudi Arabia, for 18 times a week, earning a substantial amount of money through ticket sales. Biman losing the right to fly will thus mean a huge financial loss as well. All this because of its lack of planning and competence as well as mismanagement.

It's surprising that with all the government support and funds it gets, Biman couldn't handle such a simple issue on its own. Rather, it had to seek help from the Bangladesh embassy in Saudi Arabia and the civil aviation ministry. Even after their interventions and several deadline extensions granted by the Saudi authorities, Biman couldn't resolve the matter, and is now asking for more time.

It is really unfortunate that in its 50-year journey, Biman couldn't become a profitable organisation due to various shortcomings. While previously it operated flights to 29 international destinations, currently it flies to only 19. Reportedly, Biman's market share has reduced 20 percent in recent years. It is not hard to understand why. Its chronic mismanagement, inefficiency, improper planning, flawed marketing policy and absence of professionals have repeatedly acted as barriers to its becoming a profit-making organisation. The recent debacle was also a result of inefficiency and poor management. Biman cannot go forward without addressing these internal issues.

About the current problem with Saudi Arabia, we hope the Biman authorities, with proper assistance from the ministry and the Bangladesh embassy in the Gulf country, will resolve the issue as soon as possible and ensure that it does not linger further.

When fake currency and drugs collude

Step up vigilance to combat transnational gangs

IT'S alarming to know that syndicates both inside and outside the country are active in smuggling fake currency and drugs including phensedyl despite regular checking at the borders. Reportedly, a transnational currency forgery gang has joined hands with a group of Bangladeshi drug traffickers to bring in phensedyl from India using fake Indian rupees printed in Pakistan. Law enforcers have reportedly been able to identify and apprehend some members of the gangs that include Pakistani nationals as well. Apparently, criminals are using the sea routes to bring in fake notes from Pakistan.

These counterfeit notes ultimately find their way to their gang members in India to pay for the phensedyl bought there. According to intelligence sources, the nexus of criminals also uses the fake notes to buy drugs like marijuana and uses Bangladesh as a transit route due to its favourable geographical position. We appreciate the fact that the detective branch of Bangladesh Police worked for months to gain actionable information and initially arrested eight members of the gang, including a fake rupee notes dealer, between November 27 and February 7. According to police, fake notes worth 7.45 crore rupees have also been seized from their possession.

However, what we find quite intriguing is that once the fake notes reach the Chattogram port, these are smuggled into India through different border points in Chapainawabganj, Benapole, Sunamganj, Rangpur and Rajshahi. If one calculates the distance between Chattogram port and the bordering areas, questions arise as to how the smugglers or their couriers can carry them undetected all the way. The long route has many check posts at different points. We think the Chattogram port authority should do its own investigation to apprehend the criminals involved in smuggling of counterfeit Indian notes by cargo ships, especially those coming from Pakistan. If they increase their surveillance of the containers and of the workers handling them, it will work as a deterrent for smugglers in the future.

Unfortunately, smuggling of various commodities including contraband items across the long and porous borders between Bangladesh and India has been taking place on a regular basis. We feel that these sensitive places need to be better manned and monitored by the law enforcing agencies of both countries to deter transnational criminal gangs.

ILLUSTRATION: ANWAR SOHEL

Is the state's surveillance apparatus out of control?

Shayan S Khan *is the executive editor of the Dhaka Courier.*

SHAYAN S KHAN

IN 2014, UK-based surveillance watchdog Privacy International published a procurement tender document issued by the Rapid Action Battalion (Rab) showing they were looking to buy mobile phone surveillance equipment known as "IMSI Catchers."

IMSI Catchers, or "stingrays" are powerful spying tools that let you listen to mobile telecommunications. They are portable devices used to covertly intercept mobile communications by infiltrating GSM networks and capturing the International Mobile Subscriber Identity (IMSI) of the target.

When activated, they send a signal that tricks mobile phones in a defined area into thinking they are communicating with a legitimate mobile phone network—that is why they are also known as "fake cell towers." In this way, IMSI Catchers allow users to indiscriminately gather data from thousands of mobile phones in a specific area and at public events such as political demonstrations, for which their highly portable "backpack" versions are very popular.

A subsequent investigation by Privacy International, together with Swiss magazine *WOZ*, uncovered that representatives from Rab were being hosted in Zurich by a manufacturer of IMSI Catchers, Neosoft, in August 2014. The Swiss authorities confirmed to Privacy International that they had reason to believe that the Rab representatives were in Zurich to receive technical training from Neosoft on how to use the surveillance technology.

Because such training would require an export licence, and none was sought by NeoSoft, the Swiss export authorities referred the company to federal prosecutors for a potential violation of export control laws, and the deal fell through.

At the time, the then additional director general of Rab, Colonel Ziaul Ahsan, told the media in Bangladesh that the import of some equipment from Switzerland had been stopped "just before the shipment of the materials" by the Swiss authorities due to campaigning by a human rights organisation.

But that didn't stop Rab from continuing to look for IMSI Catchers. In a June 2019 update, Privacy International reported three more tenders from the paramilitary unit—in November 2015, December 2016, and January 2017—for the purchase of such equipment.

It doesn't end there. Since procurement tenders are public documents, you can do a simple Google search for "Rab tender IMSI" and see the results for yourself. For the purposes of this article, three of them are mentioned from just the first page of the results: one each from the website of the Central Procurement Technical Unit (February 2019, for Backpack IMSI Catcher), the *Daily Sun* newspaper (December 2020, for Backpack IMSI Catcher), and the Rab website itself (February 2019, for Backpack IMSI Catcher).

Rab is far from the only one from Bangladesh on the market looking for these products. Tender documents show that in July 2018, the Bangladesh Police sought to buy an "IMSI Monitor/Mobile Tracker" and a "Back Pack IMSI Monitor/Location Finder." There is also one from October 2017 in the name of the police, for "IMSI Monitor/Mobile Tracker" and "Location Finder Equipment."

Additionally, Privacy International has reported on the basis of publicly available documentation that:

I) Four police officers received approval to travel to Canada in June 2019 for a "Factory Acceptance Test (FAT) relating to shipment of 04 pcs Back Pack IMSI Monitor/Location Finder."

II) In June 2019, six police officers received approval to travel to Canada for training on "Back Pack IMSI Monitor/Location Finder Tuning Antenna."

III) Six police officers were slated to receive training on using an "IMSI Monitor/Mobile Tracker" in Germany in September 2019.

From what is available in the public domain, we also know of at least one case, in which the tender process was followed all the way through to purchase and import of the said equipment.

In March 2021, the *Toronto Star* reported that Canadian tech company Octasic had sold IMSI Catchers to Rab in 2019. Octasic CEO Sebastien Leblanc confirmed to the *Star* that the Canadian government had approved the export of IMSI Catchers to Bangladesh, and that the technology itself was exported.

What all this indicates is that the capability to intercept, eavesdrop and store away—for use later, for better or for worse—our phone conversations extends significantly beyond the National Telecommunications Monitoring Centre (NTMC), the nationally-mandated body for such activity, which does its own procurement.

Until 2013, the NTMC was based at the headquarters of the Directorate General of Forces Intelligence (DGFI), the military intelligence agency. It is now under the home ministry. DGFI, however, continues to be involved in its operation, and it is headed up by a brigadier general.

It has long been alleged, of course, that advanced surveillance equipment procured to fight militancy, as Bangladesh became embroiled in the global War on Terror, was also being used on the civilian population. The established pattern was of an inopportune leak through government-friendly media outlets, putting opposition figures or critics of the government in an awkward or embarrassing position, and drawing some criticism of the intelligence services for allowing it. But lately, it's been more of a mixed bag.

Take the recent leaked conversation between the prime minister's adviser—on private sector affairs and business—and the law minister, talking about High Court judges and a pet project of Sajeeb Wazed Joy—possibly the most high-profile leak the country has witnessed since the famous conversation between Prime Minister Sheikh Hasina and Leader of the Opposition Khaleda Zia in 2013.

Or the one of the disgraced former state minister for information and broadcasting, Murad Hassan, in December. Both of these cases would seem to have been aimed at embarrassing the government, and they have driven feverish speculation as to who might have been behind them, along with their intentions.

The law minister has since come out and defended the content of the conversation he engaged in. The home minister, however, was forced to address how it may have occurred. It would be investigated, he said, while reiterating that the NTMC is the only agency authorised to carry out lawful interceptions.

Clearly, however, the capability to engage in such activity is not restricted to the NTMC, or the DGFI. The diffuse ownership of the requisite technology—IMSI Catchers—among different agencies means the entire apparatus of state surveillance is a lot more decentralised than what it once was, or what the home minister would have us believe.

That means less scope for exercising control over not only what gets recorded, but also what gets leaked.

The more pernicious threat

The Canadian government has received its fair share of criticism from privacy advocates for having allowed Octasic to export IMSI Catchers to Rab. In an article in *The Globe and Mail* last year, Edin Omanovic of Privacy International and Siena Anstis of Citizen Lab, which tracks the spread of surveillance software from its base at the University of Toronto, wrote, "That Ottawa may have sanctioned the export of this technology while the Digital Security Act (DSA) continues to be exploited is therefore of serious concern."

They also came down hard on Justin Trudeau's administration for failing to be open about it. While the Canadian government provides an annual report on the export of Canadian military goods, it excludes "dual-use or other sensitive items," including surveillance technologies.

While the ownership of such technologies (by the DGFI alone, it was long-assumed) has often come to the fore in the event of leaks, the really pernicious threat to democracy from equipment like IMSI Catchers is that by enabling authorities to spy on mobile phones in a blanket and non-targeted manner—covertly and independently of any operator—they endanger journalists, protesters and others wherever security agencies are deployed to crack down on government critics. It does nothing to stop what is already out there.

An overlooked aspect of the US government's announcement of sanctions against a range of actors, including Rab and seven of its current and former officials, in December last year was the Export Controls and Human Rights Initiative (ECHRI), which was part of the same announcement. The ECHRI is meant to help curb authoritarian governments' "misuse of technology and promote a positive vision for technologies anchored by democratic values."

It will seek to do this by working to develop a written code of conduct to guide the "application of human rights criteria to export licensing policy and practice." It was joined in this initiative by Australia, Denmark, Norway, the Netherlands, France, the UK, and following extensive lobbying by Citizen Lab—in which the Octasic deal with Bangladesh figured heavily—Canada. The next time Rab floats an international tender for surveillance equipment, you can be sure they won't be getting takers from any of these countries. That was the good news. The bad news is that it does nothing to stop what is already out there.

While the ownership of such technologies (by the DGFI alone, it was long-assumed) has often come to the fore in the event of leaks, the really pernicious threat to democracy from equipment like IMSI Catchers is that by enabling authorities to spy on mobile phones in a blanket and non-targeted manner—covertly and independently of any operator—they endanger journalists, protesters and others wherever security agencies are deployed to crack down on government critics.