The Daily Star

FOUNDER EDITOR
LATE S. M. ALI

DHAKA MONDAY OCTOBER 23, 2017, *KARTIK 8, 1424 BS*

Rohingya persecution

China's policy of non-interference!

NO one can take issue with the statement of the Deputy Head of the Chinese Communist Party's International Department that foreign interference in the internal affairs of a country is counterproductive. The Chinese government's support for Myanmar's efforts to maintain stability in the country is understood. But how can China overlook the consequences of more than half a million new refugees in Bangladesh? It must be stated that non-interference in others' internal affair is also our stated policy to which we steadfastly adhere. However, it would be remiss to consider whatever is obtaining today in Rakhine as entirely an internal problem of Myanmar.

Certainly, Myanmar's internal policy, manifested in the planned violence against an ethnic minority, has had the most serious impact on this country. The pressure of the exodus from Myanmar on Bangladesh has been constant, over the last decade in particular. Thus, it was only too natural for Bangladesh to expect its very good friend, which China certainly is, to display equal empathy for the sufferings Bangladesh has had to endure in this regard. Is it not expected that equal concerns would be expressed by China for the security and safety of Bangladesh? We have already expressed our concerns in this regard, and the entire world has acknowledged the adverse security potential of the Rohingya crisis for Bangladesh.

More than half a million Rohingya refugees have crossed into Bangladesh since August 25, adding to the quarter million of them already here. What, may we ask, would have been China's reaction if it were to face an influx of equal proportion? Are we to be penalised for being humane? Should we have mined our borders and prevented the Rohingyas form seeking succour here? It is a matter of regret that China, by choosing to overlook reality, has in fact endorsed the killings of innocent people.

It seems an incongruous proposition to leave the resolution of a situation entirely alone on a government which is the very cause of the problem.

Special concessions for habitual defaulters

Will encourage more loan defaults

SONALI Bank, which is struggling to reduce nearly 30 percent of its bad loans, has made the strange decision to waive interest of Tk 129 crore of Alltex Group, owned by a former lawmaker and Awami League leader, who reportedly happens to be one of its top five defaulters. The decision was made on "special consideration" according to bank officials, which makes one wonder whether banks nowadays have a "special" way of conducting business with "special people".

That such concession is being made for a regular defaulter begs the question as to what sort of an example the bank is setting. And what the problem is in trying to recover the loan now, given that the bank had no qualms in giving such huge loans in the first place—which must mean that the bank had reasons to believe that it would be repaid at the time of issuance or, that it had given the loans without necessary appraisals.

What is guaranteed, however, is that the most likely outcome of this would be to encourage more defaults in the banking sector, which is already tottering from being hit by one financial scandal after another. All of which, it is important to mention, had happened right under the nose of the Bangladesh Bank, whose performance as regulator has been less than stellar to say the least, as evident from the current disastrous condition of public banks.

Therefore, what is needed now is better regulation and the urgent recovery of loans, rather than greater concessions for habitual defaulters. And the sooner the regulators realise that, the better.

LETTERS TO THE EDITOR

letters@thedailystar.net

Relocate JnU to a new place, as promised

Jagannath University (JnU) marked its 12th anniversary on October 20. The university, as an educational institution, started its journey in 1858 when Dhaka Brahma School was founded. Not too long ago in 2005, it became a university.

In its 12 years of history, JnU has produced some of the brightest minds in the country. Currently, it has 24,000 students in 38 departments and institutions. Despite the fact that the university is allotted a very low budget, it performs better than many of its counterparts.

Unfortunately, it is the only public university in the country with no student halls. Students took to streets to realise their demands in vain. The government decided to shift the university to avail all necessary facilities. As a student, I urge the authorities to fulfil their promise as soon as possible.

Rashidul Hasan, *Jagannath University*

Alarming rise in lightning deaths

The number of deaths caused by lightning has increased in Bangladesh. Last year, 261 persons were killed by lightning, forcing the government to declare it as a major natural disaster. As of October, a total of 170 persons died due to lightning, according to media reports.

Experts put the blame on climate change. The internationally renowned journal, *Nature*, for example, in a report last year, supported the argument. It said lightning incidents had increased around the world.

I draw the attention of the concerned authorities to work and research more to develop precautionary techniques. In the urban areas, building owners must be forced to install lightning prevention systems. In the rural areas, the plantation of palm trees may help. In addition, people should be made aware of what to do during a lightning.

Shafkat Rahman, *By email*

Looking beyond the obvious

The security factor in the Rohingya crisis

STRATEGICALLY SPEAKING

BRIG GEN SHAHEDUL ANAM KHAN NDC,PSC (RETD)

IT is undeniable that the Rohingya problem imposes a huge security burden on Bangladesh. The international community is unable to realise the fact that we are sheltering a population of the size of three electoral constituencies, and that in real-estate terms means two or three upazilas. The sheer magnitude of it is incomprehensible. But not only that, more than half of the refugees are children suffering from severe malnutrition.

In fact, security was the reason why Bangladesh was extremely cautious about allowing refuge to the Rohingyas when they faced persecution, although not of the same scale, in 2012. And many of them were forced back, as was attempted unsuccessfully this time too. It would not be misplaced to take issue with those who tend to think that the Rohingya problem is a border issue that has graduated to a humanitarian issue eventually and might become a security issue in the long run. The magnitude of the problem and its true character must be grasped. It was never a border issue and was always a security and humanitarian issue.

And we had commented in this very column in 2012 to the effect that one had perhaps not heard in the past our foreign minister being more forceful on any other bilateral issue, involving our security and national interest, than when vehemently refusing to allow the Rohingyas refuge in Bangladesh. But the question is, what kind of security are we talking about?

The Rohingya issue was never a border problem; it was most certainly a humanitarian issue with severe security ramifications. But did we really think seriously about security in dealing with Myanmar on this problem in the last decade in particular? While it was the primary concern of ours to see that the Rohingya refugees were repatriated in toto to their own country, we did not project the matter strongly enough internationally to persuade the military in Myanmar to accord the Rohingyas the right that was theirs – *jus soli* – the right of the soil. It is not a fact that these people had moved into a new country. They were citizens of a country, the territory of which had been appropriated by Myanmar. It was not the people of Arakan that had moved in large numbers from one 'country' to another; it was its border that had moved over three centuries towards the east. So how can they not be citizens of a country the Rohingyas and their forefathers were born in?

Rohingya refugees who crossed the border from Myanmar a day before, wait to receive permission from the Bangladeshi army to continue their way to the refugee camps, in Palang Khali, October 17, 2017. PHOTO: **REUTERS/JORGE SILVA**

And while we were satisfied that some of the refugees had gone back, we should have alerted the world to the impending catastrophe and what that might mean for Bangladesh. But the more sceptical amongst us might question the efficacy of such an effort given that the UN has itself bottled two contemporary reports on the Rohingyas. Its attitude is fairly representative of the attitude of the international community on this matter in the past. One of the reasons for according red-carpet treatment to Myanmar leadership, while the Rohingyas were being persecuted, was that the West did not want to step on the toes of its favourite girl. The ostensible reason was that she was the window of opportunity for the democratisation of Myanmar. The real reason was more parochially strategic and economic. So, for Bangladesh, it might have been a difficult venture to make the world see through the ultimate objective the Myanmar military had set itself—of denuding Rakhine of the Rohingyas, but nonetheless worth a try. Nothing palpable was done.

Again, in this very column, we had also written that we would go wrong if we acted on the premise that the Rohingya was Myanmar's problem alone, and it is exactly because we are its neighbour that our stake is so much higher. What happens in Myanmar impacts our security and we should be more concerned to see that the situation is not exacerbated. And that is exactly what we did not do. The consequences are there for the world to see and for Bangladesh to suffer.

Regrettably, the role of the international organisations and the global community should have been more forceful. One had hoped that these organisations would be more vocal and brought to bear more pressure on the Myanmar government to address the root cause of the problem.

But we would go wrong again if we bought the story which Myanmar military is selling to the world. That the Rohingyas are a bunch of terrorists, and it is the terrorists that they are after. The hoax of ARSA attack on the military camps has been exposed by a UN report that suggests that the preparation of military operation in Rakhine predates the so-called ARSA attacks on August 25.

Yes, the Rohingya issue can and will become a security threat. Some countries still wrongly consider the matter to be an internal affair of Myanmar and would like to leave it to resolve the problem. The logic, given the ground reality, is mindboggling. Is it wise to expect the final denouement of a problem to be peaceful, just and equitable when the main stakeholder – the Myanmar government – is the cause of the problem?

Brig Gen Shahedul Anam Khan ndc, psc (Retd) is Associate Editor, *The Daily Star*.

PROJECT SYNDICATE

Cybersecurity starts at the top

LUCY P. MARCUS

EVERY time a major corporate cybersecurity breach occurs, the response looks pretty much the same: cry "havoc!" and call in the cyber first responders to close the breach. But by the time an executive or two stands before a few government committees, proffering some explanation and pledging to beef up security protocols, people—including the hackers—have largely moved on. And with each breach, the cycle accelerates: people either dismiss the threat—it probably won't happen to *them*—or accept it as an unavoidable pitfall of modern life.

The truth is that the threat posed by cybersecurity breaches is both acute and avoidable. The key to mitigating it is to understand that cybersecurity isn't simply a technology issue; it is also an urgent strategic issue that should be at the top of the agenda for every board and management team. After all, from Yahoo! to Equifax, data breaches have often been rooted in internal forces of human error, carelessness, or even maliciousness.

Already, the scale and speed of attacks is massive. It has now emerged that the 2013 Yahoo! data breach affected all three billion accounts. In May, the WannaCry ransomworm attack affected dozens of the UK's National Health Service trusts, and spread globally at lightning speed.

The recently revealed Equifax data breach—which occurred during two months when the company had a patch to a known security vulnerability, but hadn't applied it—gave the hackers access to 145.5 million consumers' personal and sensitive data. According to testimony provided by now-former Equifax CEO Richard F Smith to the US Congress, the breach reflected the negligence of one individual in the IT department.

The risks are only growing. The United Kingdom's National Cybersecurity Centre, founded last year, has already responded to nearly 600 significant incidents. The department's director recently predicted that our first "category one cyber-incident" would occur in the next few years.

One problem is that many organisations simply don't have cyber-security on their radar. They believe they are too small to be a target, or that such breaches are limited to the tech and finance sectors. But, just recently, the US fast-food chain Sonic—not exactly a tech giant—revealed that a malware attack on some of its drive-in outlets may have allowed hackers to secure customers' credit card information.

The fact is that many types of companies use, if not depend on, technology. And they collect many types of data, about everything from customers and employees to distribution systems and transactions. Consumers often don't comprehend the extent of companies' data collection, failing to understand even the basics of the "cookies" being used when they surf the web. According to a March 2017 report by the Pew Research Center, many Americans, for example, "are unclear about some key cybersecurity topics, terms, and concepts."

Of course, consumers must be informed and vigilant about their own data. But even those who are, find that if they want to engage fully in modern life, they have little choice but to hand over personal data to organisations in both the private and public sectors, from utility and finance companies to hospitals and tax authorities.

With automation, this trend will only accelerate, with people counting on technology to do everything from ordering groceries to turning on the lights and even locking the doors. The power this gives to the likes of Google and Amazon, not to mention an ever-growing array of startups, is obvious. What is not obvious is that consumers can rely on companies' knowledge and duty of care to protect the information they collect.

No company can afford a *laissez faire* attitude about cybersecurity. Yet even tech companies took some time to recognise the extent of their technical responsibilities, including the need for a C-level executive to manage their technology needs. Not long ago, such companies often maintained a "helpdesk" mindset: just make sure people could use the product and have someone to call if something went wrong.

But, with data breaches proliferating, often with business-critical consequences, there is no excuse for such inertia. Such breaches can cripple companies both operationally and financially, owing to the direct theft of funds or intellectual property and the cost of plugging the security hole or paying punitive fines. They can also diminish a company's reputation and credibility among investors, business partners, and communities, even in cases when the breach is minor and doesn't compromise sensitive information.

While board members do not all have to be technology experts, they do need to keep up with the state of their company's technology, including how well-secured it is. A board's risk committee can conduct in-depth reviews. But regular status updates to the full board, like those for other crucial issues affecting the business, are also needed.

In today's world, no organisation—public or private, commercial or non-profit—has an excuse not to be supremely vigilant and pro-active about securing their data and systems. It is not enough to meet legal requirements, which don't keep up with technological change. Instead, those requirements should be viewed as a starting point for a much more robust, closely monitored, and effectively adapted system that truly protects the data on which our societies and economies increasingly depend.

Data breaches are not a fact of modern life. They are an artifact of modern indifference.

Lucy P Marcus is CEO of Marcus Venture Consulting.