NEWS D.A.D.

100% COVERAGE OF EACH & EVERY RELEVANT NEWS

SOURCES

PIB » The Hindu » Live Mint » HT » TOI

RBI » ET » Indian Express » PRS Blog and more.....

14 leading sources for **CURRENT AFFAIRS** covered on **Daily basis.**

Topic-wise
Daily News

For all those who don't
want to be left out

"Every News counts and we make sure that you don't miss any relevant News."

CRACKACADEMY

Index

Source : www.thehindu.com Date : 2023-11-02

MALWARE MALICE: THE HINDU EDITORIAL ON THE APPLE CYBERATTACK ALERT

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

November 02, 2023 12:30 am | Updated 12:30 am IST

In a thriving democracy, the Opposition and the press are vital components of a structure controlled by a ruling establishment that requires accountability for it to be effective. That over a dozen Opposition leaders and journalists received email alerts from Apple that their devices were targeted by “state-sponsored attackers” suggests that this could be a repeat of what these members of the first and fourth estate went through in the Pegasus episode recently. In early 2022, an article in The New York Times detailed how Pegasus, a spyware developed by the Israel-based NSO Group, was used as a tool to advance Israeli interests, as Tel Aviv offered it to other countries which used it against Opposition leaders, journalists and dissidents. In July 2021, a reporters’ consortium, the Pegasus Project, found that at least 40 journalists, cabinet Ministers and other officials in India were possibly subject to surveillance using Pegasus software. A Supreme Court of India panel, however, found no conclusive evidence of the spyware on the 29 phones that it had examined; but the apex court also noted, tellingly, that the Union government was not cooperating with the panel. Unlike the Indian government’s lackadaisical and dismissive approach towards the NSO group and its products — which The NYT reported as allegedly bought by the Indian government from Israel as part of a $2 billion package including sophisticated weapons and intelligence gear in 2017 — other governments in the West implemented stringent steps following the disclosures on spyware use.

Apple’s iPhones are used by nearly 20% of smartphone users worldwide, and by nearly 7% of such users in India, largely for their diverse facilities and robust security provisions. Researchers had found that spyware software such as Pegasus had targeted iPhones and the operating system iOS as early as 2016, and Apple had come up with updates to fix Pegasus exploits, besides going on to sue NSO. The company clarified that the alerts sent now did not accuse a “specific state actor”; it also said that it would not be able to disclose how the targets were discovered, but reiterated that the alerts had to be taken seriously. Yet, with the specific targets being Opposition leaders and journalists, the question whether it is the ruling establishment that is subjecting them to surveillance is important. This can only be verified by an independent and empowered investigation, involving the apex court again, which should, this time around, compel the Union government to cooperate. More immediately, the government must come clean on its dealings with NSO and its use of software provided by such agencies and also emulate steps taken by other governments in proscribing such entities.

SHARE

democracy / Israel / technology (general) / mobile phones / politics / Pegasus surveillance / USA / United Kingdom / espionage and intelligence / government / France

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END

Source : www.thehindu.com Date : 2023-11-03

TO INTERVIEW, OR NOT TO INTERVIEW? THAT IS THE QUESTION

Relevant for: Security Related Matters | Topic: Role of Media and Social Networking Sites in internal security challenges

November 03, 2023 03:00 am | Updated 03:00 am IST

In 1997, four years before the 9/11 attacks in the U.S., journalists from CNN interviewed Osama bin Laden in a cave in a remote mountain in Afghanistan. When they asked the al-Qaeda chief, once an ally of the U.S.- and Pakistan-trained mujahideen in Afghanistan who fought against Soviet troops, about his future plans, bin Laden replied, “You’ll see them and hear about them in the media, God willing.” Back then, he was wanted for terror attacks in Africa and Saudi Arabia. When the 9/11 attacks took place in 2001, the journalists, Peter Bergen and Peter Arnett, were in great demand for their insights into the man who could have masterminded attacks that left thousands dead. Both men went on to write bestsellers on that encounter.

At the time, interviewing terrorists, guerrilla fighters, and revolutionaries was seen as a part of any credible journalist’s repertoire. At the beginning of the LTTE’s violent attacks in Sri Lanka in 1983, *TIME* magazine’s Anita Pratap interviewed Velupillai Prabhakaran. In 2002, more than 10 years after he masterminded the assassination of former Indian Prime Minister Rajiv Gandhi, and several other Sri Lankan leaders, Prabhakaran decided to hold a press conference in the deep forests of Kilinochchi. Three hundred journalists from around the world flew to Sri Lanka to attend it.

I remember travelling to remote parts of Jammu and Kashmir in 1995, where Pakistan-backed separatist groups were being trained in camps. These local groups were responsible for killing hundreds of people, including Kashmiri Pandits, forcing the Pandit community to flee the Valley. It was imperative to contextualise their words and fact-check their claims, speak to officials from the government and the military who countered their narrative, as well as bring in the victims’ stories; no one suggested that we should not speak to the militants. On the other hand, journalists were seen as adding an extra perspective to these conflicts through such interviews. In some cases, they even played the role of intermediaries.

However, the new age of terrorism post-9/11 changed that understanding. The kidnapping and brutal murder of American journalist Daniel Pearl in 2002 by al-Qaeda, and the horrific killings of American journalists James Foley and Steven Sotloff in 2014 by the Islamic State, became lessons that journalists were no longer seen as important for getting the word for groups with a political cause. They were now an easy target, and graphic videos of their killings made for the sensational headlines that transnational terror groups wish to grab. For governments too, there was less desire to engage with such groups and globally, counter-terror strategies aimed at the

elimination of all violent groups inimical to the various states they operated in.

On some groups, there is consensus, as they are designated as terrorist by the UNSC, but given that there is no global agreement on how to define terrorism, many countries come up with their own lists with the understanding that journalists no longer engage with such groups. Governments, too, change their positions, making the question of whether to interview or not more complex: while Taliban leaders today are regularly interviewed by the Indian media, and Indian diplomats publicly engage them, they are still designated terrorists, wanted by India particularly for attacks that killed Indian personnel.

In the absence of any legal code, journalists are left to take their own editorial calls, a fact that UNESCO accepted in a 2017 document called 'Terrorism and the Media: A Handbook for Journalists'. The organisation said that while it is important to retain control of the narrative and not offer a platform to any terrorist, "ultimately, the choice mainly depends on each media's editorial policy and idea of journalistic independence and responsibility". This week, The Hindu Group's magazine *Frontline* came under attack for publishing an interview with a Hamas leader based in Doha. It is important to note that neither the UNSC nor India has as yet put Hamas on their lists of designated terrorists, although the External Affairs Ministry has said that it considers Hamas's killing of 1,405 Israelis in the October 7 attacks as "terrorist acts".

END

Source : www.thehindu.com Date : 2023-11-14

CHINA PROPOSES CYBERSECURITY CHECK FOR AUDITORS IF NATIONAL SECURITY INVOLVED

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

To enjoy additional benefits

CONNECT WITH US

November 13, 2023 06:17 pm | Updated 06:17 pm IST - BEIJING

COMMents

SHARE

READ LATER

China’s finance ministry has proposed that auditors undergo or conduct additional cybersecurity checks when their work involves national security. | Photo Credit: Reuters

China's finance ministry has proposed that auditors undergo or conduct additional cybersecurity checks when their work involves national security.

A draft of the new measures, made public on Friday, also lays out how accounting firms should manage data that relates to Chinese firms.

Over the past two years, China's cybersecurity authority has established policies that outline how all businesses should handle and implement security assessments and checks.

The new measures apply specifically to auditors that have been hired by domestic firms or are conducting cross-border work. The chief partner of an auditing firm is the person responsible for data security, the draft rules say.

(For top technology news of the day, subscribe to our tech newsletter Today’s Cache)

The draft is open for public consultation until Dec. 11.

PricewaterhouseCoopers, Deloitte, KPMG and EY - the world's big four auditing firms - did not immediately respond to requests for comment.

Concern about data security has prompted Chinese authorities to step up scrutiny of auditors in recent years.

Rules issued in May already stipulate that state-owned companies and listed enterprises should strengthen checks on accountants' ability to manage information security.

Beijing has asked some state-owned firms to stop using the four big global accounting firms as it seeks to curb the influence of Western auditors, Bloomberg News reported in February.

The United States and China last year reached a deal to settle a long-running dispute over auditing compliance of U.S.-listed Chinese firms, agreeing to conduct audit inspections in Hong

Kong as China hesitates to grant full access to U.S. regulators.

COMMents

SHARE

technology (general) / internet / World / cyber crime

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END

Source : www.thehindu.com Date : 2023-11-14

A COUNTRY NEED NOT BE INVADED TO BE PUNISHED

Relevant for: Security Related Matters | Topic: Role of External State & Non-state actors in creating challenges to internal security incl. Terrorism & illegal Migration

November 14, 2023 01:00 am | Updated 01:00 am IST

In this file photo taken on November 27, 2008, Indian firefighters attempt to put out a fire as smoke billows from the Taj Mahal Palace hotel, which was the site of attack by terrorists, in Mumbai. | Photo Credit: AFP

There are animated discussions on social media on the Israel- Hamas conflict, with a large number of people sympathising with Israel, which suffered an unprecedented attack by Hamas on October 7. This is perhaps because India went through the trauma of the Mumbai attacks in 2008 (known as 26/11), among others. Opinion, however, became more strident when *The New York Times* columnist, Thomas Friedman, published an article last month praising former Prime Minister Manmohan Singh's "remarkable act of restraint" in not attacking Pakistan immediately after the Mumbai attacks. Some social media warriors were outraged, condemning India's past inaction as an act of cowardice. This is perhaps because India prides itself on its air strikes on Balakot in Pakistan in 2019 to avenge the Pulwama terror attack.

But counter-terrorism is a delicate act; it is to be carried out with due thought and realism, not raging machismo, as India showed. First, terrorists strike in the hope of eliciting a response that will highlight their cause. Hamas attacked Israel when the Saudis and Israelis were on a path to peace, which would have led to the Palestinian cause taking a back seat. With Israel's violent response, the Palestinian issue has taken centre stage now. Let's assume that after 26/11, India had bombed major cities and cantonments in Pakistan. That would have led to a nuclear stand-off, with the international focus shifting to how to 'solve' the India-Pakistan issue, which centres around Kashmir, rather than terrorism itself.

Here is what happened by doing nothing. The gravity of the 26/11 attacks was equated to that of the 9/11 attacks in the U.S. Soon after the attacks, U.S. President George W. Bush sent a strong statement of support to India, world leaders condemned the attacks, and India was praised for being a "responsible nuclear power". The path-breaking India-U.S. Civil Nuclear agreement was operationalised just a month before the attacks in Mumbai. In addition, there was another issue. The global financial crisis had just hit, with the collapse of the Lehman Brothers. In India too, the stock market crashed by 41% between June and December. A war would have been disastrous.

Second, it is vital to frame an issue in terms of the prevailing international circumstances and how that can best be used to achieve one's own objectives. Delhi decided to ally itself with the 'war on terror', which was being fought across continents. The result of a war would have been

not just finger-wagging from the international community, but also the loss of international money. Investors hate instability.

Pakistan's fortunes began to tumble soon after 26/11, furthered by an internal mess of its own making. The country, under General Pervez Musharraf, milked 9/11 for all it was worth: the U.S. military's aid rose exponentially during this period in order to enable Pakistan to fight Taliban and al Qaeda militants. Joe Biden, who was Senator, repeatedly called for reducing this aid in 2008. Real GDP growth crashed after 2008-09 and later recovered briefly, but it never recovered to previous growth rates. Foreign Direct Investment, which had risen in the 9/11 period, dropped by 42% by 2010, as Pakistan became identified with the 'war on terror'. The focus on Pakistan increased further when the United Nations designated the Lashkar-e-Tayyiba (LeT) as a terrorist organisation in 2010. In 2009, the U.S. Senate passed the revised version of the Kerry-Lugar Bill, which tripled U.S. non-military assistance to Pakistan from $400 million to $1.5 billion annually for the next five years, with clauses that Pakistan considered offensive. For instance, the bill said that Pakistan must show that it is "ceasing support" for terrorists and that it must prevent groups such as LeT from carrying out attacks on "neighbouring countries." Pakistan was furious. This narrative began to build as notable scholars such as Stephen Cohen began to call it "America's most dangerous ally". India was de-linked from Pakistan as it drew closer to the U.S., while Pakistan's future was evaluated entirely by its terrorist antics.

It can be argued that the collapse of present-day Pakistan is in part due to India's decision not to attack and instead craft an international response. Alongside, India created a path for a $3 trillion economy, while Pakistan's economic fortunes continue to tumble. None of this might have happened if India had gone to war.

However, this does not reduce the vital importance of the air strikes on Balakot. Those were carried out when India's defence capability had vastly improved, its economy was strong, and it enjoyed a solid relationship with the U.S. The strikes were carefully calibrated to send a signal to Pakistan that its terrorism was not cost-free. Importantly, it freed Indians from a defensive mindset. Strong leadership matters. But strength can come from a deliberated move rather than the kind of chest-beating that Israeli Prime Minister Benjamin Netanyahu has adopted.

Finally, whether then or now, there is no question of having 'boots on the ground' given that India and Pakistan are nuclear powers. Pakistan can be punished, but without being invaded. Those calling for India to be as "decisive" as Israel miss the point. Mr. Netanyahu has just given Hamas the priceless gift of publicity; now, support for the Palestinian cause has swelled everywhere. The trick is to outwit a country, even as the threat of a slashing sword is seen to be ever-present.

Tara Kartha, formerly with the National Security Council Secretariat, is a Distinguished Fellow at the Institute of Peace and Conflict Studies. She posts on X as @kartha_tara

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END

Source : www.thehindu.com Date : 2023-11-15

LIMITING SEARCH AND SEIZURE: THE HINDU EDITORIAL ON DIGITAL DEVICES AND MEDIA PROFESSIONALS

Relevant for: Security Related Matters | Topic: Role of Media and Social Networking Sites in internal security challenges

To enjoy additional benefits

CONNECT WITH US

November 15, 2023 12:10 am | Updated 12:10 am IST

COMMents

SHARE

READ LATER

The Supreme Court's direction to the Union government to frame guidelines to protect the interests of media professionals with regard to the seizure of their digital devices is a timely first step. Recent actions against journalists, whose laptops and smartphones were seized and searched, have sent a chilling message not just to the wider media fraternity but also to whistle-blowers and others who speak to journalists on the condition their identity will not be revealed. If a journalist's communication devices can be seized and their data examined on the flimsy grounds of allegations, it compromises sources and impedes news professionals' ability to do their job. In this way, it impinges on the freedom of the press and also strikes at the right to livelihood of journalists, as digital devices have become the critical tools of the profession.

The guidelines must ensure that law enforcement agencies are not permitted to seize or search devices without a prior judicial warrant, clearly laying out the information that the agency expects to find, rather than authorising an unlimited fishing expedition. Journalists must not be forced to incriminate themselves or their sources by being compelled to provide passcodes or biometric data. The guidelines must include protocols to safeguard the devices and the data, to ensure that it is not leaked or tampered with, or passed on to third parties, and that data irrelevant to an investigation is deleted in a timely manner. Technological interventions allow for the cloning of a device, thus allowing journalists to continue their work and not depriving them of their own data for an unspecified period. Similarly, it is important to create a record of the device at the time of seizure to ensure that incriminating material is not planted on it during the investigation process. The Court, in its directive to the Additional Solicitor-General, indicated the need for a "balancing of interests". Thus, the guidelines must be drafted in a transparent manner and involve public consultations. The Court referred to the fact that "privacy itself has been held to be a fundamental right", indicating that this is an issue involving all citizens whose professional and personal lives are increasingly contained in a vulnerable hand-held device. Beyond these guidelines for media professionals, there is a need to update the laws allowing search and seizure by law enforcement agencies to take these new digital realities into account.

COMMents

SHARE

judiciary (system of justice) / government / media / technology (general) / communication infrastructure / law enforcement

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END

Source : www.thehindu.com Date : 2023-11-20

INDIAN CYBERSPACE SEEING INCIDENTS AT HIGHER RATE THAN GLOBAL AVERAGE: NATIONAL CYBERSECURITY COORDINATOR

Relevant for: Science & Technology | Topic: Science and Technology- developments and their applications and effects in everyday life

November 19, 2023 04:27 pm | Updated 04:27 pm IST - Bengaluru

The Indian cyberspace has seen cyber incidents at an average of 2,127 times during the past six months, which is much more than the global average of 1,108. Representational file image. | Photo Credit: Reuters

The Indian cyberspace has seen nearly double the number of cyber incidents as compared to the global average, National Cybersecurity Coordinator M.U. Nair said on November 19..

Addressing a session on ‘Aligning Technologies to Future Conflicts’ at the Synergia Conclave 2023, Mr. Nair said ransomware attack payments of nearly $1.54 billion have been made on an average over the past 10 months, which has doubled since 2022.

“These payments are just the tip of an iceberg since several of these incidents go unreported,” he said.

Also read | Cyberattacks are rising, but there is an ideal patch

Mr. Nair said the Indian cyberspace has seen cyber incidents at an average of 2,127 times during the past six months, which is much more than the global average of 1,108.

Mr. Nair said it's time for countries to rally together to contain and limit disruptive practices on cyberspace.

“There are a large number of initiatives in this direction under the UN and regional forums where nations are looking for solutions to cyberspace which is not confined to national boundaries,” he said.

Mr. Nair said several international initiatives are addressing the evolving challenges of cybersecurity. One notable effort is the UN Group of Governmental Experts (UN GGE) on advancing responsible state behaviour in cyberspace, appointed by the United Nations General Assembly, he said.

In 2021, the UN GGE adopted a report that contributes significantly to the development of

international cybersecurity, he said.

“Key recommendations from the UN GGE include the development of international norms and principles, promotion of international cooperation, and strengthening of national cybersecurity capabilities.”

“Additionally, an ad hoc committee is collaborating on a comprehensive international convention to counter the use of ICTs for criminal purposes,” he added.

COMMents

SHARE

cyber crime

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END

Source : www.thehindu.com Date : 2023-11-28

THE MANY GRAVE RISKS CONFRONTING THE WORLD TODAY

Relevant for: Security Related Matters | Topic: Linkages of organized crime with terrorism

November 28, 2023 01:30 am | Updated 08:17 am IST

Palestinians pray near the bodies of members of the Hijazi family, killed in Israeli strikes, in Rafah in the southern Gaza Strip. The two-state solution for resolving the Palestinian conflict has been confined to the detritus of history and the region is all set for another half a century of conflict. | Photo Credit: AFP

If, as is sometimes mentioned, war reflects geo-political incompetence, then the first quarter of the 21st century reflects incompetence of the highest order, with several nations contributing to this state of affairs. Europe, Asia, and Africa seem to be in a state of permanent dissonance today, while North and South America are plagued by problems of varying magnitude. All this has set the stage for multi-polar disorder.

Liberal democracy confronts a multitude of dangers. On September 11, 2001, with al-Qaeda attacking the Twin Towers in New York, terrorism gained a new dimension. A few years later, we saw the rise of the Islamic State, which even talked of establishing a state of its own. Meanwhile, there were, and still exist, many lesser-known terrorist outfits such as the Pakistan-backed Lashkar-e-Taiba, which was responsible for carrying out attacks in Mumbai on November 26, 2008, and the Boko Haram in Africa, which continues to indulge in terror attacks in different regions of the globe.

The attack on the State of Israel by Hamas, a Palestinian terror outfit, however, represents a new high in the evolution of terrorism. That a little-acknowledged Palestinian terror outfit could take on Israel, which boasts of one of the most powerful armies in the world, is having a seismic impact across the world. Hence, there appears to be no end in sight to the challenges posed by fanaticised groups intending to achieve their ends and reinforce their beliefs.

The attack on Ukraine by Russia on February 24, 2022, though, falls into a different category, viz., of conventional conflicts, but is nevertheless highly disconcerting. The prolongation of the conflict, which was not expected to last for more than a few weeks, to well over 18 months, represents an even more disturbing trend. Even as the war continues to fester, neither Russia nor Ukraine (including NATO) is willing to consider a pause. A plethora of new technologies and strategies have proved insufficient to sort out matters on the battlefield. With each month, the risk of a wider conflagration is going up, and the conflict shows few signs of reaching a resolution.

A new battleground has opened up very recently in West Asia, following the terror attack by Hamas on Israel, which is turning into an all-out conflict. Much of the West is backing Israel, while the Arab world is left with little choice but to back Hamas. What is disconcerting is that several weeks into the conflict, the threat of an all-out war (in a region that has seldom had long periods of peace) looms large. The two-state solution for resolving the Palestinian conflict has, in turn, been confined to the detritus of history and the region is all set for another half a century of conflict. The Abraham Accords and other peace accords have fallen like ninepins.

There is worse to come. A massive United States Naval deployment, from the Mediterranean to the Gulf of Oman, in the wake of the Hamas-Israel conflict, has the potential of bringing Iran-backed Shia militant organisations (such as the Hezbollah) directly, and Iran at a later date, into the conflict. This would substantially alter the nature of the conflict and could lead to unpredictable consequences.

Notwithstanding the West Asia imbroglio, it is the uneasy situation in the Indo-Pacific region that contains even greater potential for a wide-ranging conflict — one that could well involve the U.S. and China directly. This region is already a byword for strategic competition and contestation. As it is, the U.S. and China have little space for cooperation here, as elsewhere, but both now seem intent on enlarging the scope of their conflict. The U.S. appears to think that with China's growth having slowed, accompanied by its inability to get advanced technology from the West, it now has the upper hand.

China, for its part, is vigorously pursuing its two contradictory goals viz., to checkmate the 'U.S.-dominated world order' and in turn ensure the success of a China-dominated order. Issues such as Taiwan are, hence, not receiving the attention they deserve.

As of now, the West is merely intent on replicating the tactics it employed in Ukraine to stymie Russia's advance, in the Indo-Pacific, ignoring the fundamental difference that exists between the situation in Europe and in the Indo-Pacific at present. The East, for instance, has no military arrangement like the NATO and has at best some loose untested security arrangements (such as AUKUS and the Quad) to confront China. Equally important is that few countries in Asia are ready for a military confrontation with China.

Additionally, in the category of grave risks that confront the world today are many that belong to the technology domain — more specifically Artificial Intelligence (AI) and cyber. Even as the digital threat scene has verily exploded, digital uncertainty is making a mockery of the established order. As growing numbers of people, cognitively and psychologically, become dependent on digital networks, many critical aspects of their thinking and functioning would be conditioned by AI. The emergence of generative AI will be the real game changer, and experts predict that the situation could become even more critical in the near future. The real risk is that it could alter the very fabric of nation states, with truth itself becoming a casualty — the deepfake syndrome.

The use of AI, especially for military and security purposes, is cause for utmost concern. It has to be managed with great care, for the dangers are immense. AI is capable of being vitiated, and subject to different types of 'adversarial attacks' viz. 'poisoning' (which typically aims to degrade a module's ability to make relevant predictions), 'backdooring' (which involves a malicious trigger input that causes the AI module into misclassifying inputs), 'evasion', etc. The need for extreme caution, hence, cannot be overemphasised.

The cyber domain and the cyber threat again pose serious security risks. The world is already aware of threats such as Ransomware and Phishing, as also the Zero-day syndrome, but there is much more to come. Digital trackers logged more than 5.5 trillion cyber-attacks worldwide in

2021 (over 14.5 billion attacks per day). Since then, the scale of attacks has been increasing in geometrical progression. The twin threats from AI and cyber are thus poised to emerge as the biggest dangers we face and will be the critical elements in future wars.

Meantime, quantum computing is another dimension that is likely to transform the world. Quantum's unique ability to crunch stacks of data is already reshaping certain designated sectors. Quantum AI simulation denotes a mind-boggling degree of effectiveness and efficiency but there are equally intrinsic risks attached to it.

Another domain of global risk is health, for as humanity advances, health has become a critical factor of everyday existence. The COVID-19 pandemic has been characterised as among the world's worst epidemics. The health forecast is that more such epidemics are slated to occur.

In the final reckoning, many experts are of the view that climate change and climate change health issues will be among the biggest global risks as the 21st century advances.

COMMents

SHARE

war / unrest, conflicts and war

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END

Source : www.thehindu.com Date : 2023-11-29

THE CHALLENGE OF MARITIME SECURITY IN THE GLOBAL SOUTH

Relevant for: Security Related Matters | Topic: Security challenges and their management in Border Areas

November 29, 2023 01:13 am | Updated 01:13 am IST

Volunteers collect trash during a beach clean-up campaign along the coast of the Arabian Sea in Mumbai. | Photo Credit: AFP

Charles Darwin is reputed to have argued that the key to human survival is not humankind's innate superiority but its natural adaptability. He felt that it was not the strongest or most intelligent species that survived, but the one with the capacity to adapt and adjust to the changing environment. Darwin's notion of resilient adaptability has withstood the test of time. It is a truism that all human progress requires a flexible approach to dealing with emerging challenges. None more so than in the maritime domain.

In recent years, hard security challenges in the maritime domain have acquired a new, menacing dimension. Whether with Ukraine's growing use of asymmetrical tactics against Russia in the Black Sea or China's deployment of maritime militias in the South China Sea, there is an unmistakable element of improvisation. The radical new tactics at sea involve the use of grey-zone warfare, land attack missiles, and combat drones.

It is instructive, however, that the bulk of the demand for maritime security in recent years has come from states facing unconventional security threats, such as illegal fishing, natural disasters, marine pollution, human and drug trafficking, and the impact of climate change. These are difficult to fight using only military means. States must instead be prepared to commit capital, resources, and specialist personnel over prolonged periods to meet security needs. Throughout its G20 presidency, India has sought to emphasise the concerns of the Global South in discussions to find solutions to the most pressing issues in the maritime domain. Yet, there is no functioning template to fight non-traditional threats at sea. Sustainable development goals in the littorals remain unrealised, as voices from littoral states in Asia, Africa, and the Southern Pacific are ignored by the developed countries.

Also read | India to share maritime info on vessels of interest with stakeholders

There is a widespread perception in the Global South that the zero-sum competition among powerful nations in the Indo-Pacific has been to the detriment of the developing world. The contemporary security agenda is an interconnected set of objectives involving national, environmental, economic, and human security goals. The cross-jurisdictional linkages between these diverse areas make them challenging to manage. This phenomenon is particularly

pronounced in the Global South, which finds itself especially challenged in meeting the objectives of marine governance. What is more, rising sea levels, marine pollution, climate change, and natural disasters have had a disproportionate impact on less developed states, placing them in a position of vulnerability.

Worryingly, littoral states in Asia and Africa have unequal law-enforcement capabilities and lack the security coordination required to jointly combat maritime threats. Many have varying security priorities and are not always willing to leverage partner capabilities to combat threats such as piracy, armed robbery, and maritime terrorism. Some even resist maritime cooperation with partner nations in a bid to reduce reliance on foreign agencies. They are willing to share information with such states, but only enough to advance common minimum security goals.

Maritime security is more than a matter of hard military action and law enforcement. Sea power is increasingly about generating prosperity and meeting the aspirations of the people. India's Maritime Vision 2030 sets out a creative model. This 10-year blueprint for the maritime sector envisages the development of ports, shipping, and inland waterways as a way of generating growth and livelihoods. Dhaka's inaugural official document on the Indo-Pacific details guiding principles and objectives that demonstrate a developmental approach to maritime security, focused on the provisioning of goods and services, and the protection of marine resources. The talk in Africa, too, is about a thriving Blue Economy and a secure maritime domain.

This does not detract from the enormity of the task in the southern seas — in particular, the fight against illegal fishing in Asia and Africa. The sharp uptick in illegal unreported and unregulated fishing has been aided by faulty policies that encourage destructive fishing methods such as bottom trawling and seine fishing. Environmentalists highlight three specific anomalies: lenient regulations that allow for the misuse of resources; lax implementation of the law by security agencies; and the harmful impact of subsidies that states offer to incentivise smaller fishermen to shift to motorised trawling.

Among the proposals that set out ways to deal with maritime challenges is India's Indo-Pacific Oceans Initiative. It rests on seven pillars including maritime ecology, marine resources, capacity building, disaster risk reduction, and maritime connectivity. It acknowledges that countries need collective solutions to their common problems, especially since they remain economically interdependent. It is to India's credit that the initiative has the support of major Indo-Pacific states, many from the West.

Even so, implementing a collaborative strategy is challenging since it requires maritime agencies to improve interoperability, share intelligence, and agree on a regional rules-based order. States must adapt to an integrated form of maritime security operations and overhaul regulatory frameworks to align domestic regulation with international law — an unappealing proposition for many that continue to prioritise sovereignty and strategic independence over collective action.

Also read | India-Middle East-Europe Economic Corridor a 'win-win situation' for all States involved, not without its geopolitical challenges: FM

Unsurprisingly, consensus eludes the Global South. Notwithstanding their espoused positions on the need for a cooperative security architecture, many littoral states are reluctant to pursue concrete solutions to the challenges at sea. It highlights a paradox of non-traditional maritime security: the collective issues that developing nations face and the creative solutions they seek are at odds with their sense of political and strategic autonomy.

Abhijit Singh is head of the maritime policy initiative at the Observer Research Foundation

COMMents

SHARE

national security

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END