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.

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

CRACKACADEMY

Index

Source : www.thehindu.com Date : 2023-10-05

UNDECLARED EMERGENCY: THE HINDU EDITORIAL ON THE ARRESTS IN THE NEWSCLICK CASE

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

October 05, 2023 12:15 am | Updated 07:25 am IST

Even for a government that has shown itself to be intolerant of critical journalism, the actions by the Bharatiya Janata Party-led regime on the news website NewsClick smack of extreme vendetta and brazen harassment. The government has, thus far, disclosed no specific allegation on what exactly merited the arrest of the site's Editor-in-Chief Prabir Purkayastha and another person under the draconian provisions of the Unlawful Activities (Prevention) Act among others. Reportedly, the website is under investigation for a "terror case with Chinese links", but no article or content has been brought to light that allegedly suggests any link to "terror" or pro-Chinese propaganda. The news organisation has also said it has not been given a copy of the First Information Report or informed about the particulars of the offences it has been charged with. And yet, the journalists, contributors and employees associated with it have been subjected to raids, with many of their mobile phones and laptops seized. These actions against the website are not new — it has been under the scrutiny of the Enforcement Directorate (ED) and the Income-Tax Department since 2021, with seizures of electronic equipment, but no charge sheet was ever filed against it. The Delhi High Court, finding a prime facie case in favour of NewsClick, granted interim protection to Mr. Purkayastha from arrest and also deterred the ED from taking coercive action against the organisation. A lower court had dismissed a complaint filed by the Income-Tax department on a similar matter.

The trigger for the set of actions now is apparently an article in *The New York Times* that questioned the motives of an investor in NewsClick and alleges his proximity to the Chinese government, but it did not point to any specific article on the site that amounted to illegal propaganda against India. Government representatives first engaged in a systematic vilification and disinformation campaign against the site based on this article. Tuesday's actions seem driven by an impulse to scapegoat a media outlet and to bring about, therefore, a chilling effect on critical journalism. No government can or should so brazenly target journalists solely based on suspicion about its funding and thereby undermine the freedom of expression, which is guaranteed under the Constitution. Mr. Purkayastha was arrested and kept in jail during the Emergency in 1975 under the draconian Maintenance of Internal Security Act, on trumped up charges, when he was a student-activist at Jawaharlal Nehru University. Today, history seems to be repeating itself, but without even the fig leaf of a declared Emergency.

SHARE

government / Bharatiya Janata Party / arrest / media / laws / China / terrorism (crime) / judiciary (system of justice) / freedom of the press / history / constitution

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 : 2023-10-07

A WARNING SHOT FOR COMMITTING THE ‘CRIME’ OF JOURNALISM

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

October 07, 2023 01:19 am | Updated 01:19 am IST

A protest in Bengaluru against the arrest of *NewsClick* founder and editor-in-chief Prabir Purkayastha and Amit Chakravarty, the firm’s human resources head, under the UAPA. | Photo Credit: Getty Images

In an interview to the BBC shortly after the Gujarat pogrom of 2002, Chief Minister Narendra Modi was asked: “When you look back, do you think there is anything you should have done differently?” His response was clear and unvarnished: “Yes, one area where I was very weak, and that was how to handle the media.” Both the question and the answer were contained in the BBC documentary that was barred from being aired in India in 2023. The raids that followed on the BBC offices in Delhi and Mumbai following the broadcast of the documentary elsewhere in the world showed that Mr. Modi had learnt his lessons well in nine years as Prime Minister.

If a global giant could be so brazenly smothered by the ‘Mother of Democracy’ strutting around in her G20 baubles, the fate that has befallen tiny *NewsClick* should not surprise too many. After securing the co-option, cooperation, and capitulation of vast chunks of big media, an image-obsessed government is turning the screws on the bit players. A piece of legislation here to shackle; an early-morning knock there to scare. As the general elections of 2024 loom, preceded by the semi-finals in five States, it is a warning shot to the few who are still committing the unpardonable crime of journalism in the “land of Buddha and Gandhi”.

“Show me the man and I’ll show you the crime,” was the boast attributed to Joseph Stalin’s ruthless secret police chief, Lavrentiy Beria, i.e., he could fabricate a case against anyone, even the innocent. Taking a leaf from the Bolshevik’s book, a political establishment that feasts on the excesses of 1975 has mastered the art of plausible deniability. Every attack on press freedom is painted as anything but: it is about money-laundering (*NewsClick*, NDTV); it is about income-tax evasion (BBC, *Dainik Bhaskar*); it is about national security (MediaOne); it is about glorifying terrorism (Fahad Shah); it is about disrupting peace (Siddique Kappan). At least Indira Gandhi had the courage to formally declare an Emergency — and the censors sat alongside journalists in the newsroom, not the Prime Minister’s office.

Editorial | Undeclared Emergency: On the arrests and actions in *NewsClick* case

L’affaire *NewsClick* is a particularly egregious case — even M/s Thomson & Thompson wouldn’t find it funny. A mighty state going after a news operation that began in a basement. The police landing up without a copy of the FIR or a list of the offences committed. Seizing the phones and laptops of the “suspects” despite every court saying ‘don’t’. A case of economic offence turning into a conspiracy to undermine the republic. And the 76-year-old founder of the portal being arrested under a law made for terrorists. So many questions can be asked, but just one is enough: exactly whose activity is “unlawful” here, the second estate’s, or the fourth?

“If anyone has committed anything wrong, agencies are free to carry out investigations against them under set guidelines,” were the gratuitous words of the Union Information and Broadcasting Minister Anurag Thakur. But when the “suspects” are questioned about the protests against the Citizenship (Amendment) Act, the Delhi riots that followed, or the farmers’ agitation on the farm laws, it reveals a perverse mindset which is so used to unfiltered propaganda that it sees ear-to-the-ground journalism not as a public service, but as an avoidable hindrance. And it ticks all the boxes of media capture — harassment, intimidation, vendetta, vilification.

When Indira Gandhi routinely invoked the “foreign hand” to brush away her every failing, India was literate enough to guffaw at it. But in Bharat, when the state accuses a website of “Chinese links” and peddling Chinese propaganda, the WhatApp University admins cannot find the smarts to ask, what is illegal about it, even if true? If the custodians of the world’s fourth largest economy think that its journalists do not have the intellectual wherewithal to empathise with peasants and pensioners, women and workers, the poor and the marginalised, Dalits and the disenfranchised, without the Renminbi lining their pockets, it shows that Inspector Clouseau didn’t click on the news headlines.

“In furtherance of this conspiracy to disrupt the sovereignty of India and to cause disaffection against India, large amount of funds were routed from China in a camouflaged manner and paid news were intentionally peddled criticising domestic policies, development projects of India and promoting, projecting and defending policies and programmes of the Chinese government,” reads the comical FIR, with scant understanding of what “paid news” is, oblivious of the Reserve Bank of India-mandated 26% limit on foreign funding of digital platforms, and mocking the 49 crore that Chinese companies donated after COVID-19, including to the PM CARES fund, no less.

This investigation by insinuation, by weaponising every arm of the state, can be read as a sign of creeping political nervousness, but that would be too charitable a view given the stellar record vis-a-vis the media since 2014. When the White House press corps can be disdainfully kept waiting in a van while the U.S. President is bumping fists in the Prime Minister’s residence, or when a BJP-ruled government with blood on its hand can be blithely allowed to proceed against the Editors Guild of India for ferreting out the facts in Manipur, it points to a systemic contempt for the news media bordering on pathological hatred. But, for public consumption, every June the tweets should read: “We must not forget that dark period of Emergency. Censorship was so stringent that nothing could be published without approval.”

The bottomless thirst for approval and approbation — and the limitless allergy for scrutiny and criticism — that the retrofitted witch-hunt against *NewsClick* highlights, offers a useful chance for a hypnotised citizenry to pause and ponder: why is a government, which spends thousands of crores to promote itself through the media, so intent to crush the outliers, bringing disrepute in the eyes of the world? And why is a government which periodically issues (self-attested) certificates of India’s growing prowess so uninterested in improving its ranking on the World Press Freedom index, where it now stands below Taliban-run Afghanistan, at 161 out of 180 countries? (In 2014, it was at 140; in 2022, it was at 150.)

The answer to those questions explains why a sledgehammer was taken to swat a fly. When a BJP minister in Uttar Pradesh tweeted that journalism began during the time of ‘Mahabharata’, a film-maker replied tartly: “And ended in 2014”.

Krishna Prasad is former Editor-in-Chief, Outlook, and former member, Press Council of India

COMMents

SHARE

media

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 : 2023-10-09

HOW THE DIGITAL INDIA ACT WILL SHAPE THE FUTURE OF THE COUNTRY’S CYBER LANDSCAPE

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

To enjoy additional benefits

CONNECT WITH US

October 09, 2023 08:30 am | Updated 08:30 am IST

COMMents

SHARE

READ LATER

For representative purposes. | Photo Credit: Getty Images

Nations worldwide are grappling with the need to update their legal frameworks to adapt to the evolving digital landscape. India, with its ambitious ‘Digital India’ initiative, is no exception. The recent announcement of the Digital India Act 2023 (DIA) represents a significant step towards establishing a future-ready legal framework for the country’s burgeoning digital ecosystem. This move by the Ministry of Electronics and Information Technology (MEITY) signals a proactive approach to regulating and shaping the digital future of the nation.

The DIA, poised to replace the two-decade-old Information Technology Act of 2000 (IT Act), is designed to address the challenges and opportunities presented by the dramatic growth of the internet and emerging technologies. It is imperative to understand the key aspects of this legislation and why it is essential in the contemporary context.

The primary motivation behind the DIA is to bring India’s regulatory landscape in sync with the digital revolution of the 21st century. The IT Act of 2000, crafted during a time when the internet was in its infancy, has struggled to keep pace with the rapid changes in technology and user behaviour. Since its inception, India’s internet user base has exploded from a mere 5.5 million to a staggering 850 million. The nature of internet usage has also evolved, with the emergence of various intermediaries and the proliferation of new forms of user harm, such as cyberstalking, trolling, and doxing. The DIA recognises these changes and aims to provide a comprehensive legal framework to address them.

The DIA encompasses several pivotal clauses that mirror the dynamic evolution of the digital environment, addressing its multifaceted challenges and opportunities. These provisions underscore the legislation’s responsiveness to the ever-changing digital landscape.

The proposed DIA encompasses a spectrum of significant provisions aimed at addressing the ever-evolving digital landscape. Firstly, it places a strong emphasis on online safety and trust, with a commitment to safeguarding citizen’s rights in the digital realm while remaining adaptable to shifting market dynamics and international legal principles.

Secondly, recognising the growing importance of new-age technologies such as artificial intelligence and blockchain, the DIA provides guidelines for their responsible utilisation. Through this, it aims to not only encourage the adoption of these technologies but also to ensure that their deployment is in line with ethical and legal principles. This means that the DIA does not just leave it to the market to dictate the course of these technologies but actively engages in shaping their development and use within a regulatory framework. And by doing so, the DIA strikes a balance between fostering innovation and safeguarding against potential harms. It promotes ethical AI practices, data privacy in blockchain applications, and mechanisms for accountability in the use of these technologies.

This forward-looking stance is not only beneficial for citizens and businesses but also positions India as a responsible player in the global technology landscape, ready to harness the full potential of new-age technologies while mitigating associated risks.

Thirdly, it upholds the concept of an open internet, striking a balance between accessibility and necessary regulations to maintain order and protect users. Additionally, the DIA mandates stringent Know Your Customer (KYC) requirements for wearable devices, accompanied by criminal law sanctions.

Lastly, it contemplates a review of the “safe harbour” principle, which presently shields online platforms from liability related to user-generated content, indicating a potential shift in online accountability standards. These provisions underscore the proposed DIA’s commitment in addressing the complexities of the digital age.

While the introduction of the DIA is a commendable step towards addressing the challenges of the digital age, there are certain aspects that warrant a critical evaluation.

One key concern is the potential impact on innovation and the ease of doing business. Stricter regulations, particularly in emerging technologies, could inadvertently stifle entrepreneurial initiatives and deter foreign investments. Additionally, the review of the “safe harbour” principle, which shields online platforms from liability for user-generated content, could lead to a more cautious approach among these platforms, possibly impinging on freedom of expression. Furthermore, the DIA’s success hinges on effective enforcement, which will require substantial resources, expertise, and infrastructure. Balancing the interests of various stakeholders, including tech giants, while ensuring the protection of citizen rights, poses a significant challenge. Therefore, while the DIA is a progressive move, its implementation and potential repercussions warrant vigilant monitoring and adaptability to avoid unintended consequences.

The DIA is a crucial step towards ensuring a secure, accountable, and innovative digital future for India. It represents a forward-looking approach to regulation in an age of constant change and has the potential to shape the country’s digital landscape for generations to come. As consultations continue, it will be interesting to see how this proposed legislation evolves and plays out in the dynamic digital arena.

Sanhita works in the Applied Law and Technology Vertical of Vidhi Centre for Legal Policy

COMMents

SHARE

Text and Context / technology (general) / India

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal.

END

Source : www.thehindu.com Date : 2023-10-09

NEWSCLICK NON-CASE: THE HINDU EDITORIAL ON THE STRANGE CASE OF A TERRORISM FIR WITHOUT A TERRORIST ACT

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

October 09, 2023 12:20 am | Updated 09:41 am IST

The FIR registered by the Delhi Police against Prabir Purkayastha, the founder of *NewsClick*, and others is a vague amalgam of sweeping accusations that do not actually disclose any offence, leave alone one of terrorism. Without citing any published content, the FIR alleges offences range from a conspiracy to undermine the country’s security to disrupting the 2019 parliamentary polls, from causing disaffection against the government to disrupting essential services. It invokes provisions of the Unlawful Activities (Prevention) Act (UAPA) and penal provisions relating to conspiracy and promoting enmity between different groups. Quite notably, it does not mention any overt act that may be described as unlawful activity or a terrorist act. There is a general description that foreign funds were infused illegally into India by forces inimical to the country with the objective of causing disaffection against the government, disrupting the sovereignty and territorial integrity of India, and threatening its unity and security. It refers to a ‘conspiracy’ based on purported email exchanges to show Arunachal Pradesh and Kashmir as “not part of India”, and also moves to protract the farmers’ agitation of 2020-21 and thereby disrupt supply of services and other essential supplies.

Overall, it is quite clear that the police are combining the remittances by American businessman Neville Roy Singham in *NewsClick*with its journalistic content to build a case that “Chinese” funds are being used for propaganda, fomenting unlawful activities, and undermining the country’s security. The UAPA is also conducive to such misuse as its widely defined terms can as easily help criminalise people for ‘thought crimes’ as for their acts. The resort to UAPA is also a tactical aid to prolong the incarceration of dissenters and the disfavoured, and send out a chilling message to the wider media fraternity. There is also the likely electoral spin-off in its potential for the ruling BJP to milk the ‘Chinese conspiracy’ theory in the run-up to the Lok Sabha polls. A related question is whether the alleged creation of shell companies by two telecom companies does not merit more than a casual mention in an unrelated FIR and warrant a separate probe into these conduits for funding terror. In mentioning that a lawyer was among those who helped create a legal network for these companies’ defence, the police seem to be considering criminalising legal services. The case flags a disturbing trend: the present regime’s propensity to misuse anti-terror laws and invoke national security sentiment to undermine individual and media rights.

SHARE

terrorism (crime) / laws / media

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 : 2023-10-12

CERT-IN ISSUES ALERT FOR NOESCAPE RANSOMWARE

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

To enjoy additional benefits

CONNECT WITH US

October 11, 2023 02:15 pm | Updated 02:15 pm IST

COMMents

SHARE

READ LATER

The Avaddon encryptor utilized AES for file encryption, with NoEscape switching to the Salsa20 algorithm. | Photo Credit: Reuters

Indian Computer Emergency Response Team (CERT-In) issued an alert for NoEscape ransomware which is believed to be a rebrand of Avaddon, a ransomware gang that shut down and releases its decryption keys in 2021. The Avaddon ransomware gang used phishing campaigns to target corporate victims.

NoEscape and Avaddon's ransomware encryptors are almost identical, with only one notable change in their encryption algorithm, CERT-In said in a post.

The Avaddon encryptor utilized AES for file encryption, with NoEscape switching to the Salsa20 algorithm.

The NoEscape ransomware is similarly targeting enterprises in double extortion attacks. As part of the attacks, the threat actors steal data and encrypt files on Windows, Linux, and VMware ESXi servers.

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

Cybercriminals then threaten to release stolen data if a ransom is not paid, with reported demands ranging between hundreds of thousands of dollars to over $10 million.

Upen infection the NoEscape ransomware runs a number of commands to delete Windows Shadow Volume, Local Windows backup catalogs, and to turn off Windows automatic repair.

The encryptor then begins terminating processes associated with security software, backup applications, web and database servers.

The ransomware also changes the Windows wallpaper to an image telling victims they can find instructions in the ransomware notes named “How to recover files.txt”. The note contains a “personal ID” required to log in to the threat actor's Tor payment site and access the victim's unique negotiation page. Threat actors demand ransom amount to be paid in bitcoins

This page includes the ransom amount in bitcoins, a test decryption feature, and a chat panel to negotiate with the threat actors.

The NoEscape ransomware can also spread laterally to other devices after breaching a corporate network and deploy the ransomware throughout the network.

CERT-In has advised users to maintain offline backups of data, encrypt backups, implement multi-factor–authentication for all services among other measures to avoid falling victim to the ransomware.

COMMents

SHARE

technology (general) / internet / World / India

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.pib.gov.in Date : 2023-10-24

BHARAT NATIONAL CYBER SECURITY EXERCISE 2023 CONCLUDES: ELEVATING INDIA’S CYBERSECURITY PREPAREDNESS TO NEW HEIGHTS

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

[New Delhi, October 23rd, 2023] – The prestigious SCOPE Convention Centre in New Delhi bore witness to the Bharat National Cyber Security Exercise (NCX) 2023, an event of monumental significance spanning from October 9th to 20th October 2023. This momentous occasion is a remarkable milestone in India's unwavering quest for cybersecurity excellence.

This flagship event served as a unifying platform for over 300 participants, representing a diverse spectrum of government agencies, public organizations, and the private sector, all resolutely committed to the safeguarding of critical information infrastructure.

Organized by the National Security Council Secretariat (NSCS), Government of India(GoI), in strategic partnership with Rashtriya Raksha University(RRU), Bharat NCX 2023, the closing session had Air Chief Marshal VR Chaudhari, PVSM, AVSM, VM,ADC, Chief of the Air Staff, deliver the motivational address to the participants. He stressed upon the importance of cyber security in today’s world and mentioned that future battle will be fought primarily in the cyber domain. He also stressed on the importance of operational technology in the domain of cyberspace.

Dr Samir V Kamat, Secretary DDR&D and Chairman Defence Research and Development Organisation, while speaking at the Closing Session made a special mention of such events which would enhance the Nation’s cyber security posture.

Further enhancing the event's significance, Lt Gen M U Nair, National Cyber Security Coordinator, provided a strategic overview of India's cyber domain. His insights illuminated the evolving landscape of cyber threats, emphasizing the pivotal role of collective vigilance in safeguarding the nation's digital assets.

Colonel Nidhish Bhatnagar, the Director of RRU, expressed his admiration for the steadfast dedication of the GoI to cybersecurity during the event. He underscored the vital importance of such efforts in safeguarding India's digital security, particularly in a time marked by widespread digitization and an increased exposure to threats.

Bharat NCX 2023 represents a defining moment in India's unwavering commitment to cybersecurity excellence, underscoring the paramount importance of collaboration and knowledge-sharing among stakeholders from government, public, and private sectors.

Bharat NCX 2023, organised intense training for the participants over six days and a red on blue Live Fire cyber exercise over five days, wherein participants challenged their cyber skills against a determined adversary. The exercise also had a Strategic Track for leadership level discussions on cyber threat landscape, incident response, crisis management to handle real world cyber challenges.

In addition to the core exercise, Bharat NCX 2023 hosted the prestigious Bharat NCX CISOs Conclave, with a gathering of over 200 Chief Information Security Officers (CISOs) from government, public organizations, and the private sector. This exclusive gathering of industry leaders provided a unique platform for in-depth discussions and deliberations on the evolving cyber threat landscape.

Bharat NCX 2023 also showcased an exclusive exhibition spotlighting the innovation and resilience of Indian Cyber Security start-ups and Micro, Small, and Medium-sized Enterprises (MSMEs). The exhibition presented cutting-edge solutions and technologies developed by these dynamic entities, underscoring their pivotal role in fortifying India's cybersecurity ecosystem.

Bharat NCX 2023 while making endeavours to fortify our cyber defences also highlighted the need for a National Cyber Security Strategy resulting in governance structures supported by legal frameworks, efficient processes for threat intel sharing and enhancing Public Private Partnership.

In an era characterized by burgeoning digitalization, Bharat NCX 2023 serves as a compelling reminder of the paramount importance of collective vigilance and preparedness in safeguarding our nation's invaluable digital assets.

"Nation First, Always First"
BHARAT
NATIONAL CYBER SECURITY
EXERCISE 2023

NATIONAL SECURITY
COUNCIL SECRETARIAT
Rashtriya Raksha University
BHARAT
NATIONAL CYBER SECURITY EXERCISE
BHARAT
BHARAT
NATIONAL CYBER SECURITY EXERCISE
2023
"Nation First, Always First"

***

DS

[New Delhi, October 23rd, 2023] – The prestigious SCOPE Convention Centre in New Delhi bore witness to the Bharat National Cyber Security Exercise (NCX) 2023, an event of monumental significance spanning from October 9th to 20th October 2023. This momentous occasion is a remarkable milestone in India's unwavering quest for cybersecurity excellence.

This flagship event served as a unifying platform for over 300 participants, representing a diverse spectrum of government agencies, public organizations, and the private sector, all resolutely committed to the safeguarding of critical information infrastructure.

Organized by the National Security Council Secretariat (NSCS), Government of India(GoI), in strategic partnership with Rashtriya Raksha University(RRU), Bharat NCX 2023, the closing session had Air Chief Marshal VR Chaudhari, PVSM, AVSM, VM,ADC, Chief of the Air Staff, deliver the motivational address to the participants. He stressed upon the importance of cyber security in today's world and mentioned that future battle will be fought primarily in the cyber domain. He also stressed on the importance of operational technology in the domain of cyberspace.

Dr Samir V Kamat, Secretary DDR&D and Chairman Defence Research and Development Organisation, while speaking at the Closing Session made a special mention of such events which would enhance the Nation's cyber security posture.

Further enhancing the event's significance, Lt Gen M U Nair, National Cyber Security Coordinator, provided a strategic overview of India's cyber domain. His insights illuminated the evolving landscape of cyber threats, emphasizing the pivotal role of collective vigilance in safeguarding the nation's digital assets.

Colonel Nidhish Bhatnagar, the Director of RRU, expressed his admiration for the steadfast dedication of the GoI to cybersecurity during the event. He underscored the vital importance of such efforts in safeguarding India's digital security, particularly in a time marked by widespread digitization and an increased exposure to threats.

Bharat NCX 2023 represents a defining moment in India's unwavering commitment to cybersecurity excellence, underscoring the paramount importance of collaboration and knowledge-sharing among stakeholders from government, public, and private sectors.

Bharat NCX 2023, organised intense training for the participants over six days and a red on blue Live Fire cyber exercise over five days, wherein participants challenged their cyber skills against a determined adversary. The exercise also had a Strategic Track for leadership level discussions on cyber threat landscape, incident response, crisis management to handle real world cyber challenges.

In addition to the core exercise, Bharat NCX 2023 hosted the prestigious Bharat NCX CISOs Conclave, with a gathering of over 200 Chief Information Security Officers (CISOs) from government, public organizations, and the private sector. This exclusive gathering of industry leaders provided a unique platform for in-depth discussions and deliberations on the evolving cyber threat landscape.

Bharat NCX 2023 also showcased an exclusive exhibition spotlighting the innovation and resilience of Indian Cyber Security start-ups and Micro, Small, and Medium-sized Enterprises (MSMEs). The exhibition presented cutting-edge solutions and technologies developed by these dynamic entities, underscoring their pivotal role in fortifying India's cybersecurity ecosystem.

Bharat NCX 2023 while making endeavours to fortify our cyber defences also highlighted the need for a National Cyber Security Strategy resulting in governance structures supported by legal frameworks, efficient processes for threat intel sharing and enhancing Public Private Partnership.

In an era characterized by burgeoning digitalization, Bharat NCX 2023 serves as a compelling reminder of the paramount importance of collective vigilance and preparedness in safeguarding our nation's invaluable digital assets.

SCOPE
"Nation First, Always First"
MEDIA

"Nation First, Always First"
NCX
BHARAT
NATIONAL CYBER SECURITY
EXERCISE 2023

राष्ट्रीय सुरक्षा परिषद सचिवालय
NATIONAL SECURITY
COUNCIL SECRETARIAT
Rashtriya Raksha University
NCX
BHARAT
NATIONAL CYBERSECURITY EXERCISE
BHARAT
NATIONAL CYBER SECURITY EXERCISE
2023
"Nation First, Always First"

राष्ट्रीय सुरक्षा परिषद सचिवालय
NATIONAL SECURITY
COUNCIL SECRETARIAT
Rashtriya Raksha University
(An Institution of National Importance)
Ministry of Home Affairs, Government of India
National Security is Supreme
NCX
BHARAT
NATIONAL CYBERSECURITY EXERCISE
2023
BHARAT
NATIONAL CYBER SECURITY EXERCISE
2023
"Nation First, Always First"

***

DS

END

Source : www.thehindu.com Date : 2023-10-25

CYBERCRIMINALS USE ISRAEL-HAMAS CONFLICT TO SPREAD CRYPTO FUNDRAISING SCAMS ON X, TELEGRAM AND INSTAGRAM: REPORT

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

To enjoy additional benefits

CONNECT WITH US

October 24, 2023 03:50 pm | Updated 03:50 pm IST

COMMents

SHARE

READ LATER

Palestinians look at the destruction of a house in the aftermath of a strike amid the conflict with Israel in Khan Younis. | Photo Credit: Reuters

Scammers are using the Israel-Hamas conflict and the death of civilians in Palestine and Gaza to list dubious cryptocurrency wallet addresses and lure unsuspecting victims into sending them funds.

Researchers have spotted over 500 “fundraising” emails sent from entities claiming to be charities. Several posts on X, formerly Twitter, Telegram and Instagram were found to list dubious cryptocurrency wallets, a report from the Bleeping Computer said.

Similar crypto donation scams were also reported during the Ruso-Ukrainian war and earthquakes in Turkey. Posts on social networking platforms share emotive messages along with gory pictures of wounded soldiers, women and children to lure unsuspecting users into donating to their scam wallets.

An example of such an account was a “Gaza Relief Aid “account on X, which uses the aidgaza.xyz domain and maintains a presence on Telegram and Instagram. The domain presented by the account is not endorsed by any established charitable organisation contrary to its claim of being “An Islamic Relief Initiative,” the report said.

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

Operators behind the account have listed their Ethereum, Bitcoin, and USDT addresses on its website and social media accounts.

Similar scams are claiming to be support Israel are also making rounds. “Donate for Israel” was one such account on X that raised doubts around its authenticity.

Researchers at Kaspersky, a cybersecurity firm, also reported more than 500 scam emails, along with fraudulent websites designed to capitalise on people’s willingness to aid those impacted.

Websites reported by Kaspersky were found to support easy money transfer options and accept a wide range of crypto including Bitcoin, Ethereum, Tether, and Litecoin.

To avoid donating to a scam, users are advised to carefully scrutinize pages before donating as fake websites lack essential information and specifics of the charity’s workers and documentation. Users should donate using only official and through recognized charities to avoid falling victim to scams.

COMMents

SHARE

technology (general) / cyber crime / internet / World

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