
ZEROFOX
Intelligence
G20 Summit
Event Assessment

G20 Summit Event Assessment

TLP:CLEAR A-2023-09-06a

ZEROFOX Intelligence

Introduction

India's hosting of the Group of 20 (G20) summit in New Delhi was supposed to be the culmination of its years-long strategy to become a global superpower. While India's summit will still be attended by a high-profile list of world leaders led by U.S. President Joe Biden, most attendees will be Western leaders now that both Russian President Vladimir Putin and Chinese President Xi Jinping will not be attending. Putin's absence was expected, but Xi's absence is a surprise and comes two weeks after he led the BRICS summit in Johannesburg, South Africa, that saw BRICS announce six new potential members—all of whom are in China's sphere of influence. Xi's absence will exacerbate the G20's ability to reach consensus on key issues like Russia's war in Ukraine, food insecurity, the global debt crisis, and climate change. However, the key takeaway is that China is likely leading a pivot away from mainly Western-led groupings and creating its own alternative. It will also likely worsen relations with India, which views the summit as key to establishing itself as a global leader and is the prime candidate to overtake China as the world's second-largest economy after already surpassing it in population.
Xi's absence and other indignities targeting India(mainly centered on a disputed border between the two countries) send a strong signal that China is not interested in repairing relations with India or the West.

The G20 is the world's primary multilateral bloc dedicated to global economic issues. While previous summits have not been without disagreements between major powers, recent years have seen a greater degree of antagonism, with Western countries and their allies on one side and China, Russia, and their allies on the other. Last year's summit in Indonesia saw members issue a last-minute joint statement of agreement after tensions over Russia's war in Ukraine drove a wedge between major powers. Those attitudes have only hardened since then, resulting in not a single joint statement being issued this year during any of the smaller ministerial meetings leading up to the summit. If the trend continues and no joint statement is issued during the coming summit, it will be a blow to India's status as a rising power.

Extensive security restrictions will be in place in Delhi, a city of around 17 million people, beginning on September 8. Travel into and out of New Delhi, the national capital and a part of greater Delhi, will be off limits to all drivers except residents and essential services. Travel between New Delhi and the business hub of Gurugram will also be impacted due to high security along the route from Indira Gandhi International Airport, where many foreign leaders will arrive. Over 130,000 police and military personnel will deploy to maintain security.

Key Threats

- Sikh separatists and pro-democracy hacktivists could target the event.
- Road and aviation travel will be greatly restricted during the event.
- India leads the world in internet outages tied to protest activity.
- The threat of terrorism during the summit is low.
- India leads the world in mobile phone thefts.
- Chinese and Pakistani groups are the most likely sources of nation-state cyberattacks.
- Effective security is a main focus for Indian officials.
- Security will be tight around venue locations.

Key Findings

- Security will be tight around the event venue and throughout the city of New Delhi.
- Presidents Xi Jinping of China and Vladimir Putin of Russia will not attend in a sign of increasing tensions with the West.
- Key topics of discussion will include reforms to the World Trade Organization. multilateral development banks, and the possible inclusion of the African Union into the G20.
- Several domestic terror groups are active within India, though the likelihood of a successful attack on the summit is low.
- Protests against Indian Prime Minister Narendra Modi's democratic record are possible, though are unlikely to be large or particularly disruptive.
- India Stack, which links users to a series of government run apps, is vulnerable to hacking.

SCOPE NOTE ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 8:30 AM (EDT) on September 5, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

G20 Summit Event Assessment

TLP:CLEAR A-2023-09-06a

ZEROFOX Intelligence

Physical Security

There will be a heavy security presence throughout Delhi, with over 130,000 police and military expected to deploy across the city. Security will be particularly tight at the meeting venue, which alone will receive a complement of nearly 5,000 police officers.[1] Special security measures will be implemented for the airport where world leaders will arrive, city entrances, malls, markets, monuments, and places of worship. Police will also monitor social media for threats.[2]

The summit will take place at the Bharat Mandapam Center in Pragati Maidan, a 123-acre green space and event venue. The venue is located in central New Delhi not far from Connaught Place, one of the city's primary business and finance hubs, and Rashtrapati Bhavan, the official residence of the President of India. Bharat Mandapam is a roughly 17-kilometer (10.5-mile) drive from Indira Gandhi International Airport.[3] Numerous hotels are also located in the vicinity.

Beginning one day prior to the summit, the municipality of New Delhi, located within the larger city of Delhi, will be off limits to all vehicles except residents and essential services. Vehicles not destined for New Delhi will be diverted to the eastern and western peripheral expressways that ring the city. Residents will be required to show proof of residency to gain entry. A specialized ambulance service has also been set up to provide medical care during the summit. Around 10,000 police officers will be deployed to ensure the smooth flow of traffic.[4]

India's ranks among the leading countries for iPhone and wider smartphone theft; the capital Delhi and Mumbai are among the leading cities. In 2021, Mumbai saw 134 smartphone thefts a day, which are then sold on the blackmarket.[5]

India likely sees the summit as an opportunity to prove its security capabilities as a rising power. City officials, the police, and the military will be under pressure to maintain a high degree of professionalism and effectiveness.

› Assessment:

- A large number of police officers and military personnel have been deployed throughout Delhi and New Delhi to provide security and ensure the smooth flow of traffic.
- The summit will take place at Bharat Mandapam in central New Delhi, near prominent business districts and hotels.
- Travel into New Delhi will be heavily restricted beginning one day prior to the summit. Most vehicles will be diverted to the ring highways surrounding New Delhi. A small number of vehicles belonging to essential services and residents will be allowed to enter.

› Recommendations:

- Carry identification around event sites and avoid unnecessary travel.

Broader Geopolitical Context

This year's G20 summit occurs at a time of rising geopolitical tensions. Last year's summit took place against the backdrop of Russia's invasion of Ukraine, which divided many member states but did not stop them from issuing a joint communique (an expression of common agreement among members)at the summit's conclusion. Those divisions have worsened as the invasion continues and other powers mount challenges to the Western-led world order. During the first two G20 ministerial meetings earlier this year, members failed to coalesce around joint communiques amid mounting disagreements.[6] If no joint communique is issued during the upcoming summit, it will be the first time in the G20's history.

These disagreements reflect a possible shift in the G20's focus. The grouping has historically been a forum to discuss global economic issues, but recent tensions between Western-leaning nations and those more aligned with Russia and China have made it difficult for G20 members to see eye-to-eye on a variety of topics. Notably, the G20 includes all G7 members—often seen as leaders of the West—as well as all members of the BRICS grouping, which has begun aligning itself as an alternative to the Western worldview. Disagreements between these two blocs over geopolitical matters could jeopardize their ability to cooperate on economic issues. The 2023 annual meetings of BRICS and G7 were among the most consequential in years. At the G7 summit in Japan, leaders focused on isolating China and Russia economically; the BRICS meeting focused on adding new members.

These disagreements will likely be heightened by India's desire to focus the summit on economic development in the Global South, where major powers from both groupings have sought support in recent years. Members will likely seek to reach agreements that will make it easier for their bloc to partner with countries there.

Tensions between India and China will also likely influence the proceedings. Both countries regard each other with suspicion over a long-running border dispute that has led to hand-to-hand clashes between border guards. Chinese President Xi Jinping has confirmed he will not travel to New Delhi for the summit, which is seen as a snub as he recently traveled to South Africa for the BRICS summit.[7]

› Assessment:

- The summit will feature disagreements between major powers but could still result in substantive agreements that will benefit developing countries.

› Recommendations:

- Configure ZeroFox geopolitical team monitoring and alerting for geographic areas of interest.

FOOTNOTES

[1] hXXps://www.cnbctv18[.]com/india/G20-summit-massive-security-arrangements-underway-in-delhi-ahead-of-mega-event-17667791.htm
[2] hXXps://www.newindianexpress[.]com/cities/delhi/2023/aug/25/national-capital-to-turn-into-fortress-ahead-of-G20-summit-2608442.html
[3] hXXps://www.bqprime[.]com/business/G20-summit-new-delhi-dates-venue-theme-members-and-all-you-need-to-know-bqc
[4] hXXps://indianexpress[.]com/article/cities/delhi/delhi-police-traffic-restrictions-diversions-G20-8909645/
[5] [6] hXXps://www.mid-day[.]com/sunday-mid-day/article/as-the-kauwwa-flies-23296783
[6] hXXps://thewire[.]in/diplomacy/with-geopolitics-taking-centre-stage-is-the-G20-fundamentally-changing
[7] hXXps://www.cnn[.]com/2023/09/04/china/china-sends-premier-li-qiang-g20-intl-hnk/index.html#:~:text=China%20on%20Monday%20indicated%20that,this%20weekend%20in%20his%20place.

Boycott and Protest Activity

Prime Minister Narendra Modi's perceived democratic backsliding will likely be a source of protest. Domestic pro-democracy groups will likely seek to use the visibility of the G20 summit to bring attention to Prime Minister Modi's governance, which has been marked by accusations of Hindu favoritism, media intimidation, and unfair prosecution of political opponents. Protests could be staged by opposition parties such as the Indian National Congress and its INDIA coalition or by grassroots activists. On August 19, over 70 civil society groups attempted to stage a pro-democracy forum in New Delhi called We20: People's Summit, but the proceedings were broken up by the Delhi police.[8] Continued intimidation of political dissenters will likely fuel further criticism of Modi's government and could drive further protest activity.

In the run-up to the main event, the host country holds smaller G20-related events throughout the year. In one such event in May 2023, there were protests as India chose to hold the G20 tourism ministers event in Srinagar, which is the capital of Kashmir and claimed by both India and Pakistan. In addition to the event-related protests, there was also a rise in militant attacks by Kashmiri separatist groups.[9]

Protesters could also target other world leaders in attendance. The Delhi police have received intelligence that Tibetan activists could chain themselves to immobile objects to protest Chinese President Xi Jinping, though it is unclear if these plans will be called off now that President Jinping has declared he does not plan to attend. Similar protests against Bangladeshi Prime Minister Sheikh Hasina are possible. Delhi police have been issued chain and bolt cutters to remove such protesters.[10]

The last G20 summit in Bali, Indonesia, came months after the start of Russia's war in Ukraine, and there were calls to kick Russia out of the group. With the war still ongoing potential protests are possible, but tight security and India's largely neutral stance on the war make it unlikely.

› Assessment:

- Large-scale physical protests are unlikely at this event.
- Protesters could target Prime Minister Modi's perceived democratic backsliding or other world leaders in attendance.

› Recommendations:

- Avoid the vicinity of event locations and any possible protests, as security is likely to be tightly controlled with security forces sensitive to possible threats.

Key Topics of Discussion

India has set the theme of the summit as "One Earth. One Family. One Future." and hopes to push for financial reforms that would favor countries in the Global South. Among the expected topics of discussion will be reforms to the World Trade Organization (WTO) and multilateral development banks (MDBs). India has attempted to steer discussion away from the war in Ukraine, but that topic is certain to arise and will very likely cause division among attendees.[11][12]

In keeping with the focus on the Global South, Prime Minister Modi has called for admitting the African Union (AU) into the G20. This suggestion has met with approval from most members, including Germany and the United States, but has also received objections from some Southeast Asian members. The AU consists of 55 countries, only one of which, South Africa, currently has membership within the bloc. It is not clear if the AU has reached a consensus on joining the G20.[13]

Chinese President Xi Jinping and Russian President Vladimir Putin both plan to skip the summit but will send foreign ministers in their place. This does not mean that Western countries and their allies will have disproportionate power during the summit; disagreements are all but certain to arise and could result in attendees being unable to issue a joint communique.

Terrorism

India has a history of terrorist activity stretching back to its independence in 1947. Most terror attacks take place in the Jammu and Kashmir union territory in the north, where a decades-long insurgency seeks to expel government forces, and attacks in mainland India are often perpetrated by Islamist groups based in Pakistan like Lashkar-e-Toiba of Jaish-e-Muhammad. Central states including Chhattisgarh have also seen terror attacks in recent years, mainly by Marxist rebels targeting police forces. [14] To prepare for the possibility of attacks, Delhi police will deploy about 100 quick response teams across the city trained in terror response.

Most terror groups in India have been degraded by years of government counterinsurgency efforts and are unlikely able to mount large-scale operations. However, the 2008 Mumbai attacks showed that groups can still inflict large amounts of damage using simple and relatively cheap methods. Despite the diminished terror threat, India did have a scare in August 2023, when police arrested two suspected Islamic State (IS) militants in the city of Pune. They were reportedly planning to attack the Chabad House in Mumbai, which was also attacked in 2008.[14]

High security levels around New Delhi during the summit combined with terror groups' general degradation will reduce the likelihood of an attack. Nevertheless, the G20 summit is a lucrative target for terror groups, and an attack cannot be ruled out.

› Assessment:

- The risk of a terror attack on the G20 is low.
- Locations in New Delhi outside of the immediate vicinity of G20 events are the most likely sites for an attack.

FOOTNOTES

[8] hXXps://frontline.thehindu[.]com/news/news-analysisG20-summit-dissent-suppression-modi-government/article67218552.ece
[9] hXXps://www.reuters[.]com/world/india/india-boosts-security-G20-meeting-kashmir-after-attacks-2023-05-17/[]
[10] hXXps://timesofindia.indiatimes[.]com/city/delhi/summit-clash-delhi-cops-to-get-chain-bolt-cutters-to-break-G20-protests/articleshow/103224815.cms?from=mdr
[11] hXXps://www.reuters[.]com/markets/G20-agrees-work-wto-reforms-ahead-key-meet-early-next-year-2023-08-25/
[12] hXXps://www.indiatoday[.]in/business/story/how-indias-G20-summit-agenda-plans-to-reform-multilateral-development-banks-2430816-2023-09-04
[13] hXXps://timesofindia.indiatimes[.]com/india/india-pitches-for-african-union-in-G20-as-sherpas-meet-start/articleshow/103332900.cms?from=mdr
[14] hXXps://www.thehindu[.]com/news/national/other-states/jawans-killed-in-dantewada-maoist-attack/article66780794.ece
[15] hXXps://www.indiatoday[.]in/india/story/mumbai-police-on-alert-after-chabad-house-images-found-from-terror-suspects-2413546-2023-07-29

Cybersecurity Threats

In the run-up to the G20, Prime Minister Modi wanted to put India's digital public infrastructure (DPI) on the agenda as a showcase of how India has developed applications that can simply interact with public and private institutions to handle issues like a health care crisis or international payments.[15] However, a potential hack of one of those apps, the CoWin vaccination database, saw it removed from the agenda. The incident highlighted India's cybersecurity flaws when it comes to its DPI, which is known as "India Stack" and connects Indians with a series of apps via biometric data affiliated with a unique user ID.[16] The hack showed that one could obtain information about where a user got their vaccine, their ID number, and personal information like their date of birth simply by querying their phone number.[17]

The sheer amount of data being shared on India Stack makes it a valuable target for hackers—as well as nation-state actors seeking to undermine the utility of India's DPI. It also leaves users vulnerable if they are located in an area undergoing an internet shutdown, as they will not be able to access the apps.

Travel and Service Restrictions

Travel and available services within New Delhi will be heavily impacted by the high level of security surrounding the event. Essential services such as grocery stores and pharmacies will remain open throughout the duration of the security presence. Major roadways around the event venue and other relevant locations will be off limits, including Mathura Road beyond Ashram Chowk, Bhairon Marg, and Purana Qila Road. Heavy vehicles will also be excluded from the city except those carrying essential goods. Metro stations will remain operational throughout the event, and residents are encouraged to utilize the metro to reduce street congestion.[18] Road travel between Gurugram and New Delhi will likely be heavily congested in the lead-up to and after the summit due to the arrival and departure of foreign leaders and their entourages from Indira Gandhi International Airport.

Service restrictions will include a total shutdown of all delivery services within New Delhi, including food deliveries, beginning on September 8. Delivery of essential items such as medicine will still be allowed. Postal services and medical services will remain operational.[19] Auto rickshaws and taxis will be allowed to operate within New Delhi in a limited capacity to serve residents and visitors who are able to prove they are staying within the capital.

Visitors who choose to travel by car should be aware that lax traffic enforcement and aggressive driving make Indian roads some of the most dangerous in the world. High security around the summit will likely reduce the number of drivers on the road, but safety risks will continue to exist due to poor road design and maintenance, lack of pedestrian sidewalks, and corrupt law enforcement.[20]

Internet Outages

Over the last five years, India has led the world in internet outages.[21] Most of these have been located in the disputed territory of Jammu and Kashmir and include outright internet outages and deliberate throttling of internet speeds so that they function as de facto internet outages. India uses internet outages during periods of protest to reduce communication and the spread of protest activity. The capital, Delhi, last saw widespread internet outages during the 2020 and 2021 farm bill protests. The northeastern state of Manipur has been under an internet blackout since May 2023 to create an information vacuum and deprive the rest of the country and globe of access to information on the destruction in the state.[22]

The outages make it difficult to operate digital platforms in locations experiencing protests or widespread violence. Access to a VPN should help visitors avoid an internet shutdown during the summit. Mobile internet will be the most likely to be throttled first, as it is where the bulk of the population accesses the internet. [23]

Social Engineering

Social engineering poses one of the greatest threats to organizations and participants of the G20. There is likely to be a spike in event-related lures both in the lead-up to and during the event, as threat actors will aim to capitalize on heightened global interest to harvest credentials, deploy follow-on payloads, and conduct financial fraud. India has weak record of protecting government-held data coupled with high-profile attendees from the world's 20 largest economies could further inspire cyber criminals.

Social engineering campaigns during the G20 could vary in complexity from low-level, rudimentary email and SMS-based scams targeting mass audiences to sophisticated spear phishing attacks directed at specific organizations and individuals associated with the event, such as diplomats, journalists, and high-profile attendees. Most lures are very likely to use trademarks related to the G20 or Delhi, including event sponsors such as hotels, that are designed to appear legitimate; there will likely also be attempts to impersonate businesses operating in support of the event, such as hospitality, retail, and travel companies.

› Assessment:

- Expect that, in the lead-up and throughout the G20, threat actors will leverage the event as a lure due to its high international visibility.
- Trademarks for the G20 are likely to be utilized in scams and illegal activity as a means of adding legitimacy to campaigns.

› Recommendations:

- Utilize caution when accessing sites associated with the G20 and always review for legitimacy prior to clicking on any email links.
- For event sponsors, ensure that legitimate messaging is frequent and clear to get ahead of campaigns leveraging those brands.
- Enable two-factor authentication for all organizational accounts to help mitigate phishing and credential stuffing attacks.

FOOTNOTES

[16] hXXps://twitter[.]com/pmoindia/status/1667059358407200768
[17] hXXps://restofworld[.]org/2023/india-upi-digital-payments-diplomacy/
[18] hXXps://www.businesstoday[.]in/technology/news/story/cowin-data-leak-hacker-explains-how-he-managed-to-get-aadhaar-pan-address-other-details-of-users-385320-2023-06-13
[19] hXXps://www.wionews[.]com/india-news/G20-summit-in-delhi-heres-whats-open-and-whats-closed-in-national-capital-632493
[20] hXXps://www.dnaindia[.]com/india/report-G20-summit-restrictions-to-come-into-force-in-new-delhi-district-what-s-allowed-what-s-not-3058979
[21] hXXps://www.bloomberg[.]com/news/features/2023-05-24/four-problems-and-solutions-for-india-s-dangerous-roads
[22] hXXps://www.hrw[.]org/news/2023/06/13/india-internet-shutdowns-hurt-vulnerable-communities
[23] https://www.bloomberg.com/news/articles/2023-06-14/india-s-frequent-internet-shutdowns-hurt-its-most-vulnerable

Hacktivism

Politically-motivated hacktivists could attempt to disrupt the G20. Hacktivists often target high-profile events, particularly those that garner a global audience, as these present the opportunity for threat actors to gain notoriety while providing maximum exposure. Hacktivism is most likely to occur through disruptive attacks such as distributed denial of service (DDoS) and website defacements; these have become prevalent during global events and are typically launched in an attempt to interrupt services that are essential to the occasion, including broadcasting and event-related websites. The broadcast of the opening and closing ceremonies of the G20 or key speeches, particularly from U.S. President Joe Biden or Indian Prime Minister Narendra Modi could be targeted.

Pakistani hackers have recently stepped up cyberattacks against Indian infrastructure and may escalate them further during the summit. In 2023 alone, Pakistani hacktivist groups used malware, phishing, and DDoS attacks to target Indian educational institutions, medical facilities, government entities, and military systems.[24][25] While most of these groups are not directly affiliated with the Pakistani government, many receive training and support from Pakistan and likely have access to substantial resources. Successful cyberattacks during the summit would be an embarrassment to India, which is hoping to use its hosting duties to boost its reputation as a rising power.

An additional hacktivist threat could come from India's long-running Sikh secessionist movement, which aims to establish an independent Sikh nation in the Punjab region. While calls for an independent Sikh homeland, known as Khalistan, have persisted for decades, the issue saw a small resurgence in 2023, with Sikh expatriates staging protests in Canada, the United States, and elsewhere. Pro-Khalistan hacktivist outfits are unlikely to have the resources of Pakistani groups, but reports indicate they have already begun spreading disinformation about the summit.[26]

Finally, domestic hacktivist campaigns could focus on Prime Minister Modi's alleged moves to weaken the democratic process in India, including through intimidation of media outlets and encouragement of Hindu nationalism. India is the most-targeted country in the world by hacktivists, with many attackers citing alleged Islamophobia in India's government as the reason.[27] Hacktivist actors will likely seek to use the high profile of the G20 summit to spread their message against Modi's government. Pro-democracy campaigns could use disinformation to discredit Modi or disrupt government websites.

Nation-State Activity

ZeroFox Intelligence assesses with low confidence that nation-state or state-sponsored actors will leverage the event to target the G20 and sponsoring organizations. In recent years, major events have been subjected to sophisticated attacks by state-backed threat actors conducting cyber espionage, as well as attempts to discredit and embarrass host nations. Physical attacks by nation-states are highly unlikely given the cost and consequences such attacks would incur.

State-sponsored cyberattacks during the G20 summit are most likely to involve sophisticated techniques that will allow threat actors to maintain persistent, undetected, and long-term access in compromised environments.

Ongoing tensions between India and China over the countries' disputed border could lead to cyberattacks by China-sponsored hacker groups. Chinese hackers have conducted cyber espionage against India in the past, including in April 2022 when they hacked into seven power grid hubs in an attempt to steal information.[28] Over a period of five days in June 2020, Chinese hackers launched an estimated 40,000 cyberattacks on India's information technology and banking sectors.[29] Reports indicate that Chinese President Xi Jinping will skip the G20 summit in a snub to India, indicating tensions remain high despite attempts to de-escalate. China may also feel threatened by India's recent moves to boost its manufacturing sector, which will likely come at China's expense.

Additional activities could come from the Pakistani government. Reports indicate that Pakistan's intelligence agency, the ISI, is already conducting a campaign to spread disinformation about the summit.[30] Pakistan has previously condemned India's decision to host smaller G20 meetings in Kashmir, which both countries claim in full despite control of it being roughly split between them. Pakistan may see the summit as an opportunity to embarrass India.

› Assessment:

- Physical attacks by nation-states are highly unlikely. India's adversaries likely see cyberattacks as a way to disrupt proceedings without incurring significant consequences.
- Cyberattacks by Chinese hackers are possible due to an ongoing border dispute with India that has worsened in recent years.
- Disruptions by Pakistani government-affiliated groups are also likely owing to the two countries' often violent rivalry that dates back to their mutual independence in 1947.

FOOTNOTES

[24] hXXps://government.economictimes[.]indiatimes.com/news/secure-india/pak-based-hackers-target-indian-army-education-sector-in-new-cyber-attack/101235241
[25] hXXps://indianexpress[.]com/article/business/companies/meta-detects-hacking-group-pakistan-targeted-indian-military-personnel-8589992/
[26] hXXps://www.the420[.]in/indian-agencies-gear-up-against-cyber-threats-to-G20-summit/
[27] hXXps://www.livemint[.]com/technology/tech-news/india-most-targeted-country-by-religiously-motivated-hacktivists-11691468198244.html
[28] hXXps://www.hindustantimes[.]com/india-news/chinese-hackers-targeted-7-indian-power-hubs-govt-says-ops-failed-101649356540330.html
[29] hXXps://www.indiatoday[.]in/india/story/chinese-hackers-attempted-40-000-cyber-attacks-on-india-1692088-2020-06-24
[30] hXXps://www.hindustantimes[.]com/cities/delhi-news/G20-summit-agencies-on-alert-against-cyber-attack-by-hackers-in-delhi-101693416730343.html

APPENDIX A:

ZeroFox Intelligence Probability Scale

All ZeroFox Intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of the occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

APPENDIX B:

Traffic Light Protocol for Information Dissemination

TLP:RED

HOW IT IS USED

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW IT IS SHARED

Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

TLP:AMBER

HOW IT IS USED

Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW IT IS SHARED

Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that TLP:AMBER+STRICT restricts sharing to the organization only.

TLP:GREEN

HOW IT IS USED

Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW IT IS SHARED

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

TLP:CLEAR

HOW IT IS USED

Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW IT IS SHARED

Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

About ZeroFox

ZeroFox (Nasdaq: ZFOX), an enterprise software-as-a-service leader in external cybersecurity, has redefined security outside the corporate perimeter on the internet, where businesses operate and threat actors thrive. The ZeroFox platform combines advanced AI analytics, digital risk and privacy protection, full-spectrum threat intelligence, and a robust portfolio of breach, incident, and takedown response capabilities to expose and disrupt phishing and fraud campaigns, botnet exposures, credential theft, impersonations, data breaches, and physical threats that target your brands, domains, people, and assets. Join thousands of customers—including some of the largest public-sector organizations, as well as finance, media, technology, and retail companies—to stay ahead of adversaries and address the entire lifecycle of external cyber risks.

READY TO SEE FOR YOURSELF?

› Request a Demo:
Sign up on zerofox.com/request-a-demo

› Learn More:
Visit zerofox.com
Contact us at sales@zerofox.com / 855.736.1400