



| Brief |

Threat Actors Exacerbate Divisions Ahead of Pakistan Elections

B-2024-02-05a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Government, Social Unrest

February 5, 2024

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 10:00 AM (EST) on February 1, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief

Executive Summary

What was originally going to be a tight November 2023 general election now looks settled in February 2024. During the delay, the government of Prime Minister Shehbaz Sharif managed to nullify the electoral threat posed by former Prime Minister Imran Khan, who at the time looked to be the most likely winner. Backed by the powerful military, the government launched a crackdown on Khan and his supporters, which has left Khan isolated in jail while his party has languished politically. With both the political status quo and the military on the same side, expect a more predictable economic and foreign policy position from Pakistan. These well-laid plans could, however, unravel because of the dual threat of social unrest posed by Khan as well as the elevated risk of terrorism inside Pakistan. If either of those issues is worse than anticipated, Pakistan could become even more unstable. Cyber threat actors appear to be working diligently to exacerbate these risks.

Details

Pakistan was originally due to hold elections in November 2023,¹ but they were rescheduled—ostensibly over unspecified security concerns. In the meantime, the front-runner for prime minister (PM), former PM Imran Khan, was imprisoned and disqualified from running, while former PM Nawaz Sharif returned to the country and had his previous corruption conviction removed, paving the way for him to win the election.

¹

[hXXps://www.reuters.com/world/asia-pacific/costs-crackdown-put-damper-pakistans-election-campaigns-2024-02-01/](https://www.reuters.com/world/asia-pacific/costs-crackdown-put-damper-pakistans-election-campaigns-2024-02-01/)

- Khan was removed from office in April 2022 and replaced by Shehbaz Sharif, the brother of Nawaz Sharif. After his removal, Khan led widespread popular protests, and his Pakistan Tehreek-e-Insaf (PTI) party won many local elections.
- However, during Khan's term as PM from 2019–2022² and the subsequent period of elevated protest activity, Khan angered the powerful Pakistani military, whose backing is necessary for political success in Pakistan.

With the backing of the military, Shehbaz Sharif managed to delay the elections, successfully prosecute Khan and other PTI leaders,³ mitigate the impact of disruptive PTI protests with threats of lengthy prison terms, and coordinate the return of exiled former three-time PM Nawaz Sharif to Pakistan.⁴

- Like Khan, Nawaz Sharif had previously run afoul of the military and left Pakistan for a period of four years over a corruption conviction.⁵
- In the run-up to the election, Shehbaz Sharif pushed through a law that removed indefinite political bans for candidates convicted of corruption and replaced it with a five-year ban,⁶ permitting Nawaz Sharif to run in the election. At the same time, Khan had several convictions upheld barring him from running.
- None of this would have been possible without the close coordination of the executive, judiciary, and military branches of the Pakistani government.

Nawaz Sharif's alliance with the powerful military leadership that opposes Khan should ensure his Pakistan Muslim League–Nawaz (PML–N) party wins the most seats in the general election. Closer ties between the military and political establishment mean that some of the biggest issues for investors and multinationals in Pakistan proceed more predictably.

² [hXXps://www.cfr.org/in-brief/pakistan-edge-ahead-2024-elections](https://www.cfr.org/in-brief/pakistan-edge-ahead-2024-elections)

³

[hXXps://dunyanews.tv/en/Pakistan/767973-Wife-says-Fawad-Chaudhry-is-arrested,-drove-away-to-undisclosed-place-](https://dunyanews.tv/en/Pakistan/767973-Wife-says-Fawad-Chaudhry-is-arrested,-drove-away-to-undisclosed-place-)

⁴ [hXXps://www.economist.com/asia/2023/10/26/nawaz-sharif-returns-to-pakistan-again](https://www.economist.com/asia/2023/10/26/nawaz-sharif-returns-to-pakistan-again)

⁵

[hXXps://www.csmonitor.com/World/Asia-South-Central/2023/0621/Why-Pakistan-army-is-targeting-Imran-Khan-s-party](https://www.csmonitor.com/World/Asia-South-Central/2023/0621/Why-Pakistan-army-is-targeting-Imran-Khan-s-party)

⁶ [hXXps://www.brecorder.com/news/40249679](https://www.brecorder.com/news/40249679)

- This includes making economic reforms that permit an International Monetary Fund (IMF) bailout in Pakistan
- Previous governments have ultimately backtracked on IMF reforms when faced with domestic protest movements. While that outcome is not impossible, it is greatly reduced given the close alliance between the government and the military.

There is an elevated risk that Khan's PTI supporters will stage disruptive protests against the election results or the expected increase in unemployment and inflation that accompany economic reforms. An increase in terror attacks could also turn the local population against the government. Lastly, geopolitical adversaries could seek to promote divisions via the use of misinformation or other cyber campaigns.

Economic

Pakistan's economy remains on the verge of default ahead of the election. Global inflation has hit Pakistan particularly hard because it is a major food and energy importer. COVID-19 economic impacts have also weakened its currency, the Pakistani rupee, leaving the country unable to pay for high fuel and food bills.

- Inflation is rampant.⁷
- International business confidence is also harmed because of the complex political and security environment.

Pakistan has secured a USD 3 billion IMF loan in theory;⁸ however, the terms of the loan require Pakistan to institute economic reforms that will temporarily further weaken the rupee and exacerbate issues with inflation and unemployment while simultaneously broadening the tax base. Previous governments have rolled back IMF-imposed terms like removing subsidies for fuel and electricity and increasing taxes in the face of widespread protests.

⁷ [hXXps://tradingeconomics\[.\]com/pakistan/inflation-cpi](https://tradingeconomics[.]com/pakistan/inflation-cpi)

⁸

[hXXps://www.aljazeera\[.\]com/news/2023/11/16/pakistan-and-imf-reach-deal-for-releasing-700m-from-3bn-bailout-package](https://www.aljazeera[.]com/news/2023/11/16/pakistan-and-imf-reach-deal-for-releasing-700m-from-3bn-bailout-package)

With the cover offered by the military, there is a higher probability that Pakistan will abide by the terms of the IMF loan deal in the face of widespread protests. Cyber threat actors could spread misinformation about the terms of the loan or its economic benefits to encourage protests or undermine the government's popularity.

Protests

Destabilizing protests are common in Pakistan. Protests over economic issues like inflation and unemployment are common; there were large nationwide protests over high electricity costs in August 2023.⁹

- Recently, the largest protests have been political.
- Since his ousting in 2022, former PM Imran Khan has initiated several "large march" protests calling for new elections, which clog roadways for days to weeks.¹⁰

One tactic the Nawaz Sharif government will likely utilize in the event of pro-Imran Khan protests is internet blackouts to curb the spread of information related to the protests.

- Starting on May 9, 2023, there was a four-day nationwide internet blackout amid widespread protests against the arrest of Imran Khan.¹¹
- On January 20, 2024, an internet outage affected access to Facebook, YouTube, X, and Instagram¹² during a virtual election rally conducted by former PM Imran Khan's Pakistan Tehreek-e-Insaf (PTI) party.
- A similar nationwide internet outage disrupted PTI's virtual fundraiser on January 7, 2024.¹³
- While these outages have been officially attributed to technical glitches, there is speculation that these were part of the ruling establishment's tactics to throttle the reach of the PTI among prospective voters.

⁹

[hXXps://www.aa\[.\]com\[.\]tr/en/asia-pacific/nationwide-protests-against-inflated-power-bills-continue-in-pakistan/2977655](https://www.aa.com.tr/en/asia-pacific/nationwide-protests-against-inflated-power-bills-continue-in-pakistan/2977655)

¹⁰ [hXXps://tribune\[.\]com\[.\]pk/story/2393244/political-turmoil-the-eventful-year-of-long-marches](https://tribune.com.pk/story/2393244/political-turmoil-the-eventful-year-of-long-marches)

¹¹ [hXXps://restofworld\[.\]org/2023/pakistan-internet-outage-tech-workers/](https://restofworld.org/2023/pakistan-internet-outage-tech-workers/)

¹²

[hXXps://www.bloomberg\[.\]com/news/articles/2024-01-20/pakistan-s-internet-disrupted-during-rally-by-imran-khan-s-party](https://www.bloomberg.com/news/articles/2024-01-20/pakistan-s-internet-disrupted-during-rally-by-imran-khan-s-party)

¹³ [hXXps://asia.nikkei\[.\]com/Politics/Pakistan-social-media-outages-squeeze-Imran-Khan-party-s-last-bastion](https://asia.nikkei.com/Politics/Pakistan-social-media-outages-squeeze-Imran-Khan-party-s-last-bastion)

Pakistan has managed to nullify the impact of protests by Khan supporters since August 2023, when Khan and a number of high-profile officials were arrested.¹⁴ Khan has less ability to communicate and orchestrate protests from behind bars, and threats of lengthy prison terms are major disincentives to protest.¹⁵ Because of the security crackdown on PTI protests, Khan supporters could choose to show their support on the internet rather than via physical protests.

- In a December 2022 online rally with over 1.4 million views, jailed leader Imran Khan used an AI-generated image and voice clone. While this instance involved the use of AI for “legitimate” purposes, other AI-generated content may be more malicious in nature.¹⁶
- Such media content (either authentic or AI-generated “deepfakes”) have a roughly even chance of being propagated right before the elections.

In September 2022, just after Khan’s removal as prime minister, recordings of conversations involving key personnel in the prime minister’s office were leaked over social media.¹⁷ Khan used the leaks to allege there was collusion to remove him from office and demonstrate the overall incompetence of the new government.

- Embarrassing photos and videos of political leaders have been leaked in the past, with the likely aim of weakening their candidacy and depressing voter enthusiasm.

Cyber threat actors may view tensions between PTI supporters and the military/political establishment as a key source of tension they can exploit.

- In October 2023, Facebook’s official page was apparently hacked by a threat actor calling for Khan’s release.¹⁸

¹⁴ [hXXps://www.nytimes\[.\]com/2023/06/14/world/asia/pakistan-imran-khan-defection.html](https://www.nytimes.com/2023/06/14/world/asia/pakistan-imran-khan-defection.html)

¹⁵ [hXXps://www.bbc\[.\]com/news/world-asia-66436731](https://www.bbc.com/news/world-asia-66436731)

¹⁶ [hXXps://www.dawn\[.\]com/news/1803005](https://www.dawn.com/news/1803005)

¹⁷

[hXXps://www.livemint\[.\]com/news/world/pakistan-pm-caught-in-another-audio-leak-controversy-here-s-what-h-e-said-11665791451269.html](https://www.livemint.com/news/world/pakistan-pm-caught-in-another-audio-leak-controversy-here-s-what-h-e-said-11665791451269.html)

¹⁸ [hXXps://www.hackread\[.\]com/facebook-s-official-page-hacked-release-imran-khan/](https://www.hackread.com/facebook-s-official-page-hacked-release-imran-khan/)

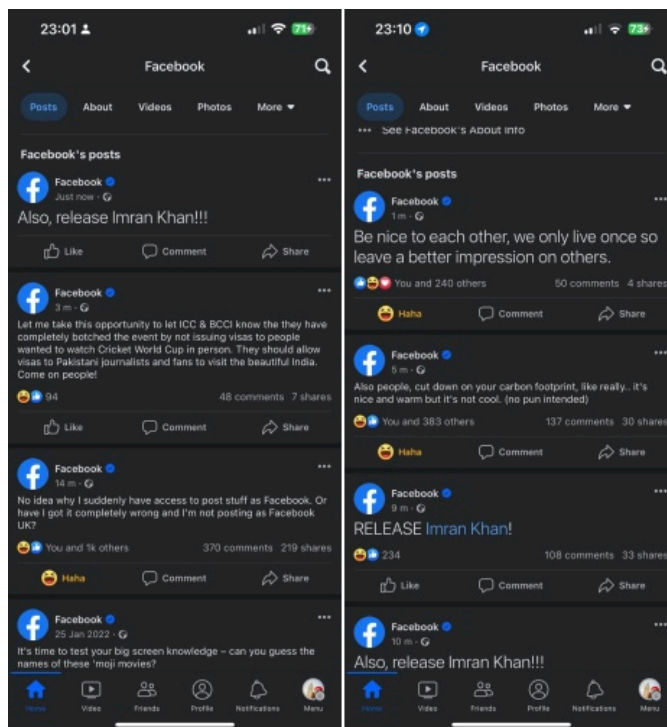


Image of a Facebook hack calling for Imran Khan's release in October 2023

Source: [hXXps://www.hackread\[.\]com/facebook-official-page-hacked-release-imran-khan/](https://www.hackread[.]com/facebook-official-page-hacked-release-imran-khan/)

Terrorism

In January 2024, Pakistan and Iran staged dual air strikes inside each other's territories. After Pakistan retaliated for the initial strikes, both sides agreed to resolve the crisis,¹⁹ and further attacks between Pakistan and Iran are unlikely in the short term.

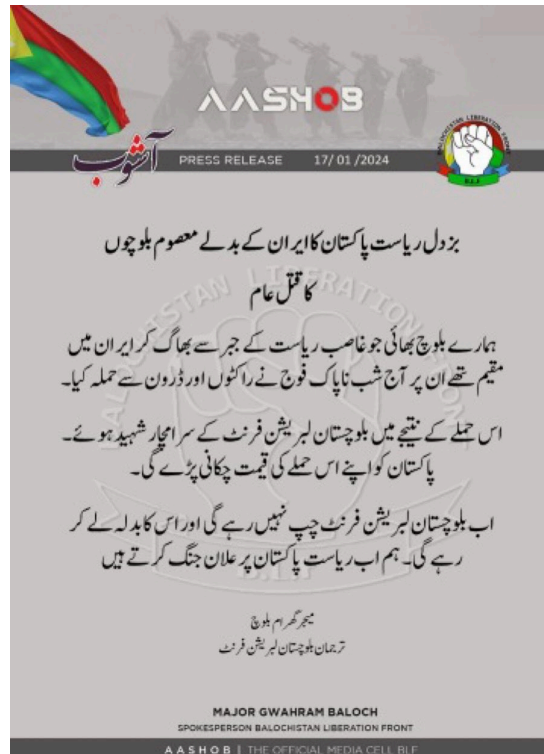
There is a risk that Iran's January 2024 missile strikes and Pakistan's retaliatory strikes will lead to cyberattacks by Iran-aligned actors (both hacktivists and advanced persistent threats, or APTs) targeting the elections.

In targeting the Balochistan Liberation Army (BLA) inside Iran, Pakistan chose to target a separatist group that, even before the dual airstrikes, had been elevating its activity against the Pakistani state.

¹⁹

[hXXps://www.aljazeera\[.\]com/news/2024/1/22/iran-and-pakistan-rebuilding-diplomatic-ties-following-tit-for-tat-s-trikes](https://www.aljazeera[.]com/news/2024/1/22/iran-and-pakistan-rebuilding-diplomatic-ties-following-tit-for-tat-s-trikes)

- The BLA calls for an independent Balochistan region of western Pakistan and has vowed to increase its targeting of Pakistan after the airstrikes; there have been several notable attacks since.²⁰ BLA strikes are likely to continue in the lead-up to the election and could continue afterwards.
- BLA attacks have notably become more radical in recent years. The group began utilizing suicide bombers in 2018, and there have been two recorded instances of female suicide bombers targeting Pakistani military positions since 2022.²¹



BLA statement threatening retaliatory attacks after the Pakistan Air Force targeting of its positions in southeast Iran on January 17, 2024

Source: [hXXps://twitter\[.\]com/Asr23267077/status/1747823971716796532](https://twitter.com/Asr23267077/status/1747823971716796532)

Aside from Baloch groups, Pakistan has experienced years of jihadist terrorism led by the Islamic State Khorasan group (IS-K), which operates in both Pakistan and Afghanistan,

²⁰

[hXXps://www.rfi\[.\]fr/en/international-news/20240131-balochistan-battle-death-toll-rises-to-15-says-pakistan-military](https://www.rfi.fr/en/international-news/20240131-balochistan-battle-death-toll-rises-to-15-says-pakistan-military)

²¹

[hXXps://newlinesmag\[.\]com/argument/women-suicide-bombers-and-the-changing-trajectories-of-pakistans-baloch-insurgency/](https://newlinesmag.com/argument/women-suicide-bombers-and-the-changing-trajectories-of-pakistans-baloch-insurgency/)

and the Pakistani Taliban (Tehreek-e-Taliban Pakistan, or TTP), which is also known to carry out large-scale attacks against Pakistani institutions and civilians.²² After an initial lull in TTP activity after the Taliban took control of Afghanistan, attacks inside Pakistan surged by almost 75 percent. Attacks in Balochistan surged 80 percent during this time.²³

The last major TTP attack occurred on December 23, 2023, when a TTP suicide bomber drove a vehicle-borne improvised explosive device (IED) into a military compound near the Afghan border before a group of gunmen launched a coordinated assault, killing dozens of officers.²⁴ Earlier in the year, a suspected TTP IED targeted a mosque in Peshawar, killing 100.²⁵

While insurgent groups such as TTP and BLA pose physical security threats to the elections, their cyber threat is very unlikely to be sophisticated enough to disrupt the elections. Any action these groups take will likely be limited to physical threats, such as voter intimidation at voting stations.

Any increase in acts of terrorism or high-profile attacks with mass casualties could erode support for the government, especially if the government is also experiencing widespread economic and political protests.

Cyber

The greatest cyber threats to the Pakistan elections are from mis/disinformation campaigns (including abusing synthetic media), data breaches, distributed denial of service (DDoS), and website defacements.

- The World Economic Forum's Global Risks Report 2024 listed misinformation and disinformation as major short-term risks, particularly in South Asia, with the potential to "radically disrupt" elections. The report stated that the "volume, reach and efficacy of falsified information" is challenging for both governments and social media platforms to attribute and tackle effectively.²⁶

²² [hXXps://tribune\[.\]com\[.\]pk/story/2438996/civilian-casualties-in-terror-attacks-doubled-in-september](https://tribune.com.pk/story/2438996/civilian-casualties-in-terror-attacks-doubled-in-september)

²³ [hXXps://www.dawn\[.\]com/news/1757192](https://www.dawn.com/news/1757192)

²⁴ [hXXps://www.bbc\[.\]com/news/world-asia-67690614](https://www.bbc.com/news/world-asia-67690614)

²⁵ [hXXps://www.bbc\[.\]co\[.\]uk/news/world-asia-64467247](https://www.bbc.co.uk/news/world-asia-64467247)

²⁶ [hXXps://www3.weforum\[.\]org/docs/WEF_The_Global_Risks_Report_2024.pdf](https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf)

ZeroFox assesses that Pakistan's geopolitical rivals (such as India, Iran, and Afghanistan) and other interested parties (such as China) are likely to support or endorse cyber campaigns to influence voters towards one party or embarrass the Pakistani administration via service disruptions.

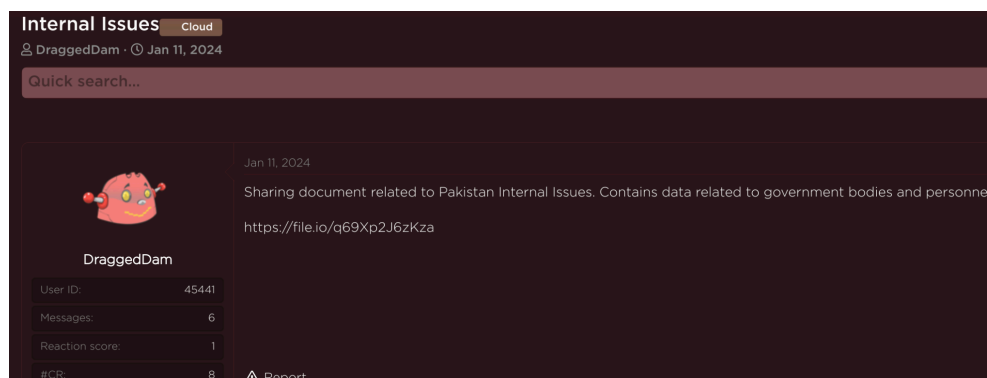
Groups directly or indirectly linked to political parties are likely to promote exaggerated and incendiary news items or social media posts via WhatsApp and other popular messaging platforms.

- The goal is to inflame existing or dormant communal fault lines to generate mass outrage and increase the turnout of voters sympathetic to their cause while demotivating potential voters from the opposite camp.

Hacktivists from India and other neighboring countries are likely to conduct low-sophistication but high-visibility attacks, such as DDoS and website defacements, to embarrass and inconvenience the Pakistani establishment.

There is evidence that geopolitically-motivated cyber threat actors have been targeting government and election-related infrastructure. It is unclear if this is by supporters of Imran Khan, opponents of the likely incoming PMLN-Nawaz party, or merely anti-Pakistan threat actors hoping to sow general unrest.

- In January 2024, ZeroFox observed a threat actor selling documents supposedly related to governmental bodies and personnel in Pakistan. The threat actor claimed that the data was linked to "internal issues" in the country.



Threat Actor Selling Pakistani Government Documents

Source: ZeroFox Intelligence

This activity follows a series of campaigns and breaches in late 2023 aimed at disrupting election campaigns, demonstrating the interest within the cybercriminal underground to infiltrate Pakistani government websites and steal data—likely for political purposes.

- In November 2023, a threat actor shared for free over 18,000 records allegedly stolen from a Pakistani police database.
- ZeroFox also observed a threat actor selling data supposedly stolen from the Pakistani Parliament in September 2023. ZeroFox can neither confirm nor deny the legitimacy of the breach or the content of the leaked package.
- In August 2023, security researchers identified a campaign using a zero-day vulnerability in the Zimbra Collaboration email server to target an undisclosed government organization in Pakistan.²⁷
- Around the same time, the Pakistan Election Commission faced an attempted ransomware attack, with employees receiving a phishing email titled “implementation of social media policy” carrying a malicious file.



Pakistani police documents shared for free by threat actor

Source: ZeroFox Intelligence

²⁷

[hXXps://blog\[.\]google/threat-analysis-group/zimbra-0-day-used-to-target-international-government-organizations/](https://blog.google/threat-analysis-group/zimbra-0-day-used-to-target-international-government-organizations/)

Such leaks are likely indicative of a more widespread issue of insecure data handling and privacy policies, including the possibility that personnel with access to governmental data would be willing to sell it for financial gain. Interested parties are likely to use information retrieved from these leaks for tactical disclosure or blackmail. Such data breaches often reveal confidential data as well as personally identifiable information (PII) that can be used by ideological and politically-motivated threat actors in various forms of attacks, including spear phishing and business email compromise.

Conclusion

Even with the outcome of Pakistan's election assured, there are still multiple risks for instability. Cyber threat actors are highly likely to use mis/disinformation tactic tactics to expose societal fissures around the economy and political divisions. Meanwhile, data brokers and other members of the digital underground have already demonstrated a desire to target Pakistani governmental bodies and election personnel with data breaches in the run-up to the election.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE 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.	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 MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	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.
	Green	Clear
WHEN SHOULD IT BE 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.	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 MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: 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 occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with 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%