



# **| Brief |**

## **Fake Geopolitical Consultancy Jobs: China's Espionage Tactic**

B-2025-07-21a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Remote Working, Espionage Campaign, Fake  
Jobs

**July 21, 2025**

## 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 00:00 AM/PM (EDT) on July 21, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

# **Brief** | Fake Geopolitical Consultancy Jobs: China's Espionage Tactic

## Key Findings

- State-sponsored actors are exploiting online job platforms such as LinkedIn and Indeed to recruit candidates with security clearances and other insiders for intelligence-gathering under the guise of remote consultancy work.
- ZeroFox observed a likely espionage campaign in India using online job platforms to recruit individuals with privileged access to the Indian government's diplomatic activities. The entity used social engineering and phishing tactics to recruit citizens as unwitting informants for the operation.
- Cybersecurity researchers suggest that the IP addresses and domain used in the India campaign likely belong to an advanced persistent threat (APT).
- Similar espionage campaigns have been reported in the United States and Europe. Multiple intelligence agencies, including that of the United States and the United Kingdom, have linked such campaigns to Chinese intelligence operations.

## **| Introduction**

ZeroFox has identified a recent case of a likely state-sponsored intelligence operation exploiting widely adopted digital recruitment protocols in furtherance of intelligence-gathering agendas in India. Similar intelligence campaigns have been previously investigated and publicly reported in the United States and Europe through official mediums.<sup>1</sup> These cases have been attributed to Chinese intelligence operations by the investigating authorities of the targeted countries. The actors' common tactics, techniques, and procedures (TTPs) include leveraging fake remote geopolitical consultancy jobs as a cover for espionage operations, exploiting the anonymity of online recruitment to evade detection and avoid being physically present in the target country. The remote nature of the jobs makes it difficult to verify employer legitimacy, unlike in-person roles that would require physical infrastructure and presence.

## **India Incident: Espionage Jobs Under the Guise of Geopolitical Consultancy Roles**

In India, ZeroFox observed an operation resembling previously reported Chinese intelligence tactics in which an entity claiming to be the legitimate Australian tech firm Geopolitical Intelligence Group (GIG) posted a job advertisement for an "Analyst-Consultant Geopolitical" on the online job platform Indeed. The post was made via the employer account of a likely unrelated California-based tech firm. The use of an unrelated employer account likely suggests that a compromised account was utilized to hide the real identity of the actors and post the advertisement.


- ZeroFox researchers have observed over 220 records of compromised credentials (including email addresses and passwords) relating to employees of GIG used to facilitate the job advertisement.
- The records originate from various data breach packages and botnet compromised credentials available on the deep and dark web (DDW). One such package included details of GIG's Chief Executive Officer and President.

---


<sup>1</sup>


[hXXps://www.fdd\[.\]org/analysis/2025/05/16/fdd-uncovers-likely-chinese-intelligence-operation-targeting-recently-laid-off-u-s-government-employees/](https://www.fdd.org/analysis/2025/05/16/fdd-uncovers-likely-chinese-intelligence-operation-targeting-recently-laid-off-u-s-government-employees/)

The job post did not provide any website URL; the email address provided (info@geopoliticalrisks[.]com) is similar to that of GIG's legitimate email ID: info@geopoliticalrisks[.]global. This spoofing was almost certainly intended to gain the trust of potential recruits before initiating espionage-linked tasks, a ploy that is also used in phishing attacks.

 **This job has expired on Indeed**  
Reasons could include: the employer is not accepting applications, is not actively hiring, or is reviewing applications

### Analyst Consultant Geopolitical

NathCorp  • 3.0 ★  
Remote  
₹4,54,249.48 - ₹14,45,745.14 a year



**Location**  
📍 Remote

**Full job description**

Drive the Global Agenda as an Analyst Consultant

Join the Geopolitical Intelligence Group (GIG)

Are you ready to shape decisions that define the global narrative? The Geopolitical Intelligence Group (GIG) seeks experienced Analyst Consultants to clarify the complex interplay of geopolitics and national security. Use your expertise to guide clients through critical challenges in a rapidly evolving world.

**Your Role: Uncovering Strategic Insights**

As an Analyst Consultant with GIG, you'll be at the forefront of intelligence analysis, delivering actionable insights to address the most pressing geopolitical questions.

**What Sets You Apart**

We're looking for individuals with:

- **Security Clearance:** An active TS/SCI clearance is mandatory.
- **Educational Foundation:** A bachelor's degree in national security, international relations, political science, or a closely related discipline.
- **Hands-On Expertise:** Proficiency with intelligence production tools, databases, and methodologies.
- **Critical Thinking Skills:** Exceptional research abilities to synthesize diverse intelligence sources and predict strategic trends.
- **Communication Mastery:** Outstanding writing and presentation skills to produce engaging, client-ready reports, articles, and visual content.
- **Preferred:** Background in government, military, or high-stakes intelligence operations.

- **Career Growth:** Work alongside industry leaders in a dynamic, mission-driven setting.
- **Innovation-Driven Environment:** Collaborate in a team culture that values critical thinking, innovation, and analytical precision.

**Take the Next Step**

Be part of a team that drives actionable intelligence and shapes global strategy. To get started, send your CV and a statement of interest to info@geopoliticalrisks.com.

**Shape the future. Drive insights. Join GIG.**

**Job Type:** Full-time

**Pay:** ₹454,249.48 - ₹1,445,745.14 per year

**Experience:**

- total work: 1 year (Preferred)

**Work Location:** Remote

## Screenshots of the Job Advertisement by "Geopolitical Intelligence Group"

Source: [hXXps://in.indeed\[.\]com/viewjob?jk=3df1a8906f326d58&from=shareddesktop\\_copy](https://in.indeed[.]com/viewjob?jk=3df1a8906f326d58&from=shareddesktop_copy)

The email address info@geopoliticalrisks[.]com also appeared in a LinkedIn job advertisement for a "Risk Analyst" role in the United States for the same alleged firm, GIG.<sup>2</sup> However, this advertisement was posted through the account of an entity called "Confidential Careers," which claims to be a recruitment agency located in Haryana, India.

<sup>2</sup> [hXXps://www.linkedin\[.\]com/jobs/view/risk-analyst-at-confidential-4164760152/](https://www.linkedin[.]com/jobs/view/risk-analyst-at-confidential-4164760152/)

# Brief | Fake Geopolitical Consultancy Jobs: China's Espionage Tactic

B-2025-07-21a

TLP: CLEAR



- According to WHOIS, the domain geopoliticalrisks[.]com was registered on July 30, 2024, with NameSilo, LLC, and has an IP address of 91.195.240[.]123.
- It is currently a parked domain that is not being actively used for hosting content or services. However, the actors in this operation are using an email associated with the parked domain, very likely suggesting domain spoofing.
- In comparison, the legitimate Australian firm GIG uses the domain geopoliticalrisks[.]global, which was registered in 2016 and is associated with Cloudflare servers.

|  |   |
|--|---|
| <b>geopoliticalrisks.com</b><br>WHOIS Information<br>IP Address: 91.195.240.123<br><a href="#">Whois</a> <a href="#">RDAP</a> <a href="#">DNS Records</a> <a href="#">Uptime</a> <a href="#">Diagnostics</a> <a href="#">Hide Data</a> <a href="#">Refresh Data</a><br><br><b>Registrar Information</b><br>Registrar: NameSilo, LLC<br>Referral URL: <a href="http://www.namesilo.com">http://www.namesilo.com</a><br>WHOIS Server: whois.namesilo.com<br><br><b>Important Dates</b><br>Created: 7/30/2024<br>Expires: 7/30/2025<br>Updated: 3/26/2025 | <b>geopoliticalrisks.com</b><br>Uptime & Server Information<br><a href="#">Whois</a> <a href="#">RDAP</a> <a href="#">DNS Records</a> <a href="#">Uptime</a> <a href="#">Diagnostics</a> <a href="#">Hide Data</a><br><br><b>Current Status</b><br>Status: Active<br>Server Type: Parking/1.0<br>Page Title: geopoliticalrisks.com - geopoliticalrisks Resources and Information.<br>Meta Description: geopoliticalrisks.com is your first and best source for all of the information you're looking for. From general topics to more of what you would expect to find here, geopoliticalrisks.com has it all. We hope you find what you are searching for!<br>Meta Keywords: Not available<br>Most Recent Data: 0 hours, 0 minutes ago |
|--|---|

## WHOIS data on the domain geopoliticalrisks[.]com

Source: `hXXps://who[.]is/whois/geopoliticalrisks[.]com`

| <b>geopoliticalrisks.global</b><br>RDAP Information<br>IP Address: 110.232.143.47<br><a href="#">Whois</a> <a href="#">RDAP</a> <a href="#">DNS Records</a> <a href="#">Uptime</a> <a href="#">Diagnostics</a> <a href="#">Hide Data</a> <a href="#">Refresh Data</a><br><br><b>Registrar Information</b><br>Name: Dreamscape Networks International Pte Ltd<br>Public ID: 1291<br>Handle: 1291<br>Public ID Type: IANA Registrar ID<br><br><b>Registrar Contacts</b><br>Abuse Contact:<br>Email: abuse[at]dreamscapenetworks[dot]com<br>Phone: tel:+61.894220890<br><br><b>Basic Information</b><br>Handle: df7856319f9144f49962a8d06e0b5b54-DONUTS | Status: active<br>Resource URL: <a href="https://rdap.identitydigital.services/rdap/domain/geopoliticalrisks.global">https://rdap.identitydigital.services/rdap/domain/geopoliticalrisks.global</a><br><br><b>Important Dates</b><br>Expiration: 10/22/2025<br>Last changed: 12/13/2023<br>Registration: 10/22/2016<br>Last update of RDAP database: 12/14/2023<br><br><b>Nameservers</b><br><table><thead><tr><th>Hostname</th><th>IP Address</th></tr></thead><tbody><tr><td><a href="#">adrian.ns.cloudflare.com</a></td><td>172.64.32.57</td></tr><tr><td><a href="#">cleo.ns.cloudflare.com</a></td><td>172.64.33.89</td></tr></tbody></table> | Hostname | IP Address | <a href="#">adrian.ns.cloudflare.com</a> | 172.64.32.57 | <a href="#">cleo.ns.cloudflare.com</a> | 172.64.33.89 |
|--|---|----------|------------|--|--------------|--|--------------|
| Hostname   | IP Address  |          |            |  |              |  |              |
| <a href="#">adrian.ns.cloudflare.com</a>   | 172.64.32.57  |          |            |  |              |  |              |
| <a href="#">cleo.ns.cloudflare.com</a>   | 172.64.33.89  |          |            |  |              |  |              |

## WHOIS data on the domain geopoliticalrisks[.]global

Source: `hXXps://who[.]is/whois/geopoliticalrisks[.]global`

- Additionally, automated IP checking platform ThreatSTOP's indicators of compromise (IoC) data has flagged geopoliticalrisks[.]com as part of a high-confidence phishing feed and listed the IP address under "ThreatSTOP APT IPs," very likely indicating links to an espionage-grade threat infrastructure.
- APTs are frequently associated with nation-state actors.

Severity Level: 4 of 5

Confidence Level: 5 of 5

Risk Level: 4 of 5

Targets: TS Originated - Phishing - Domains

FQDNS generated by bfore.ai - standard feed , high confidence - Domains


Active Targets


Historical Targets

Related Records

Whois

DNS Lookup

PDNS 

ASN Records 

This section shows IP addresses (A records) resolved for the requested domain.

It does not perform a complete lookup of all DNS records associated with the domain.

| IOC                   | Relationship | Address        | Last Time Present | Present in Targets       |
|-----------------------|--------------|----------------|-------------------|--------------------------|
| geopoliticalrisks.com | A            | 91.195.240.123 | 10 months ago     | ThreatSTOP APT IPs - IPs |

## ThreatSTOP Data on geopoliticalrisks[.]com

Source: [hXXps://www.threatstop\[.\]com/check-ioc](https://www.threatstop[.]com/check-ioc)

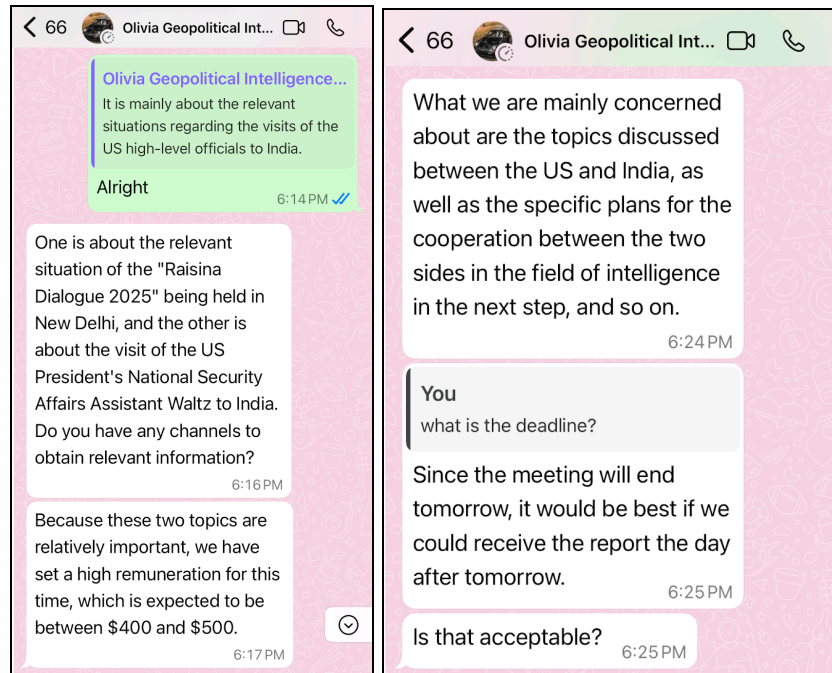
The job advertisement for the India-based role specifically sought individuals with active Top Secret/Sensitive Compartmented Information (TS/SCI) clearances; degrees in national security, international relations, political science, and other related fields; or those with government or military backgrounds with experience in high-stakes intelligence operations. The emphasis on specific qualifications indicates the actors were likely seeking individuals with privileged access to confidential or sensitive information regarding the Indian government's activities—either through direct intelligence or military experience or through contacts within government offices.

Although the job criteria appear to primarily appeal to specific professionals, the advertisement also seemed to cast a wider net. It sought those positioned near high-level diplomatic or defense events to gather actionable intelligence, regardless of security clearance—recognizing that physical proximity to critical discussions could provide valuable intelligence. The role also promised anywhere between USD 200 to USD

500 or more “per report” based on the intelligence acquired, which is a substantial payment structure in India. A report would likely include compiling a written document of exclusive insider details pertaining to foreign affairs or defense planning—including citing discussions among government officials or referencing confidential documents. ZeroFox has not verified the existence or contents of any intelligence report during this investigation.

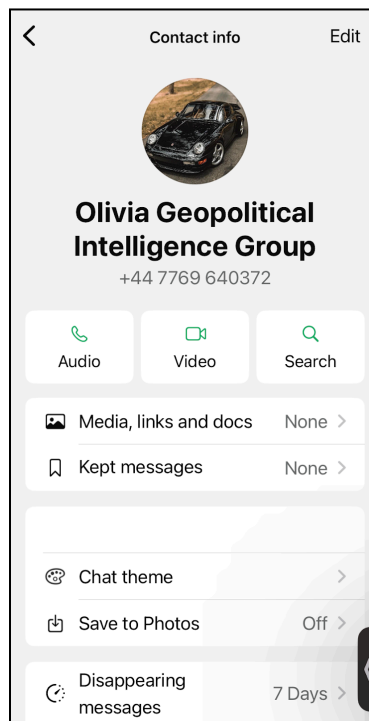
It is also unlikely that the applicant would be made explicitly aware of the true nature of the “job” or the tasks. It is likely that at no point in time would candidates be informed that they would be engaging in illegal or legally gray activities. The actors behind the operations were almost certainly not planning to reveal their identities. The operation was designed to appear legitimate by seeking geopolitical or risk advisory consultancy that would inform business clients.

Subsequent communications with the campaign operatives exposed highly specific and unusual instructions. Communications were managed by a “project manager” identified simply as “Olivia,” who claimed to be based out of Singapore, but used a UK country code mobile number. In WhatsApp communications, Olivia gave clear instructions to get “specific plans for the cooperation between the two sides (U.S. and India) in the field of intelligence in the next step...,” which very likely alludes to an intent to acquire confidential and sensitive documents on intelligence-sharing between two countries. The instruction was akin to coercing the target to commit an illegal act by gathering and sharing top secret information pertaining to national security without having explicit government clearance. The nature of the task is also very likely beyond the scope of usual geopolitical risk consultancy.



## WhatsApp communication by Olivia

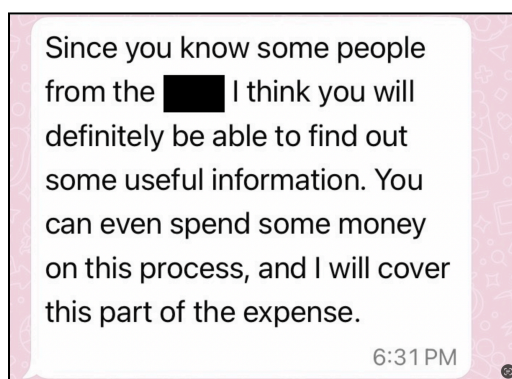
Source: ZeroFox Intelligence



## Olivia's contact number, which begins with a UK country code

Source: ZeroFox Intelligence

Olivia also suggested using money to extract exclusive information on intelligence sharing plans—implying a push to use bribes to gain classified information. Furthermore, all interactions were confined to text-only—initially via email and then exclusively on WhatsApp (with disappearing messages turned on)—with campaign operatives consistently evading voice or video call requests, highlighting the emphasis on anonymity and intent to mask true affiliations.



### **WhatsApp message encouraging the use of bribes to gather information**

*Source: ZeroFox Intelligence*

Between January and March 2025, campaign actors tasked the target with collecting sensitive information regarding three specific diplomatic events between India and the United States: India's External Affairs Minister (EAM) S Jaishankar's visit to the United States for Donald Trump's presidential inauguration, U.S. Director of National Intelligence (DNI) Tulsi Gabbard's New Delhi visit and participation in the Raisina Dialogue 2025, and then-U.S. National Security Advisor (NSA) Mike Waltz's scheduled visit to India (the visit was later cancelled). The tactical goal of the operation was likely to gather information pertaining to events happening behind closed doors, which is not publicly disclosed but is likely to be known to support staff and other administrative personnel in close physical proximity to high-ranking officials. Any data points collected via this operation were very likely to support information already gathered via more conventional monitoring methodologies and paint a clearer picture of decisions taken with regards to these three events.

The campaign actors likely sought this information to gain strategic advantages over the target nation's defense planning or international negotiations that could be exploited to

prepare countermeasures or influence outcomes. While the TTPs were observed and documented, ZeroFox could not verify if any actual intelligence or information was shared with the campaign actors or if the operation was successful.

## **A Tactic Reported Globally: Incidents in the United States and Europe**

The campaign observed in India has multiple parallels with those reported in the United States and Europe. On May 16, 2025, a report linked U.S. job advertisements seeking “Recently Laid-Off U.S. Government Employees” to a “network” whose tactics resembled previous Chinese intelligence operations.<sup>3</sup> The tactics involved posing as legitimate consultancies based outside of China, posting job ads explicitly targeting former federal employees with security clearances, and using email addresses and phone numbers appearing to be from Singapore or the United States but overlapping with other entities with links to China. The report also uncovered that the network, consisting of five companies, was using the same Chinese-owned server to host their websites. This very likely indicated that the websites or organizations were not independently run but rather were operated by a single entity—or in this case, an intelligence unit. Subsequent to their research and investigation, the non-profit behind the report, Federation for Defense of Democracies (FDD), linked the job advertisements to a Chinese intelligence operation that followed similar patterns observed in earlier cases.

In a previous instance, a Singaporean national working for Beijing's intelligence services was arrested in the United States for using LinkedIn to recruit government and military employees with security clearances under the guise of a fake consulting company.<sup>4</sup> Instances of job platforms being used to recruit potential intelligence sources have also been reported in Germany and the United Kingdom, among other countries, and were linked to Chinese espionage campaigns by the respective nations' authorities. In 2017, Germany's intelligence agency, Bundesamt für Verfassungsschutz (BfV), reported that China was using LinkedIn to recruit Germans as spies to gather information on officials

---

3

[hXXps://www.fdd\[.\]org/analysis/2025/05/16/fdd-uncovers-likely-chinese-intelligence-operation-targeting-recently-laid-off-u-s-government-employees/](https://www.fdd.org/analysis/2025/05/16/fdd-uncovers-likely-chinese-intelligence-operation-targeting-recently-laid-off-u-s-government-employees/)

4

[hXXps://www.justice\[.\]gov/archives/opa/pr/singaporean-national-sentenced-14-months-prison-acting-united-states-illegal-agent-chinese](https://www.justice.gov/archives/opa/pr/singaporean-national-sentenced-14-months-prison-acting-united-states-illegal-agent-chinese)

and politicians.<sup>5</sup> Similarly, in 2023, the United Kingdom's MI5 revealed that Chinese state actors were using LinkedIn to approach nearly 20,000 British nationals in an attempt to steal industrial or technological secrets.<sup>6</sup>

The tactics that were observed in the U.S. and European instances were also seen in the campaign observed in India. From seeking targets with security clearances and defense exposure to actors claiming to be based outside of China (such as in Singapore) to the use of online job platforms for recruitment, the patterns point towards established actions of a Chinese intelligence operation.

## **Assessment**

This incident likely underscores online job platforms being exploited as initial access vectors in the conducting of espionage campaigns. Part of such campaigns' tactics are likely to include the social engineering of citizens—especially those with access to sensitive information—in order to recruit them as informants. This type of operation likely indicates how national security threats are facilitated by the malicious use of everyday platforms. By conducting espionage leveraging social media platforms, adversaries are likely able to reach out to more targets, without the need for extensive resources. The unconventional espionage tactic is also very likely to have a psychological impact by blurring the lines between an insider and outsider threat, creating uncertainty within the diplomatic community.

These operations very likely pose a reputational threat to the entities that they seek to impersonate, and those whose communication channels are spoofed using phishing-style tradecraft. The India-based incident outlined in this report sheds light on how a likely compromised employer job account can be misused by malicious actors, including nation-state entities, when left unaddressed or dormant.

---

<sup>5</sup> [hXXps://www.bbc\[.\]com/news/world-europe-42304297](https://www.bbc.com/news/world-europe-42304297)

<sup>6</sup>

[hXXps://www.theguardian\[.\]com/uk-news/2023/oct/17/up-to-20000-britons-approached-by-chinese-agents-on-linkedin-says-mi5-head](https://www.theguardian.com/uk-news/2023/oct/17/up-to-20000-britons-approached-by-chinese-agents-on-linkedin-says-mi5-head)

These operations are likely to maintain persistence across regions by leveraging multiple job platforms and identities, enabling a resurgence even if one gets taken down. The IP addresses associated with such operations are likely to be linked to either adversarial nation's servers or APT infrastructure—known or unknown. Additionally, to date the targeted countries indicate the actors behind this campaign have an interest in U.S.-allied nations, which suggests the existence or future emergence of such operations in those nations.

## **Recommendations**

The discovery of online espionage campaigns being operated under the guise of consultancy jobs reveals an intelligence-gathering tactic that has been attributed to Chinese state-sponsored entities in various instances.

- Security agencies should monitor suspicious job advertisements on various online job platforms, big and small—especially those seeking candidates with security clearances.
- The IP addresses and domains of the suspicious entities should be flagged for widespread knowledge. Zeroing in on the technical infrastructure of espionage-linked IP addresses is likely to help dismantle future operations and reduce their persistence.
- Targeted groups and at-risk professionals should be made aware of such espionage campaigns and treat “consultancy” offers with skepticism, as well as be advised of the legal risks of providing the type of “insider information” sought.
- Firms should monitor whether their branding is being misused on multiple social media and online job platforms.

## | Appendix A: Traffic Light Protocol for Information Dissemination

|                                | <b>Red</b>   | <b>Amber</b>   |
|--------------------------------|--|--|
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:RED</b> 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. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.   |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> 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.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                                | <b>Green</b>   | <b>Clear</b>   |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.  |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> 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%         |