



| Flash |

Geopolitical and Cyber Risks of Iranian Attack on Israel

F-2023-04-15b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Geopolitical

April 15, 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 11:30 AM (EDT) on April 15, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Geopolitical and Cyber Risks of Iranian Attack on Israel

> Key Findings

- On April 13, Iran launched a massive, yet calibrated, attack on Israel in retaliation for an earlier Israeli strike on an Iranian consulate in Syria.
- Negative economic, geopolitical, and supply chain effects have been muted because markets already factored in the strike, which came with a two-week warning and deliberately avoided mass casualties.
- An immediate Israeli response that would widen the Israel-Hamas war is unlikely, but limited strikes against military positions belonging to Iranian allies across the Middle East are well within the realm of possibility.
- Ahead of the retaliation, ZeroFox identified cyber threat actors forming alliances with both Israel and Iran, which could escalate to cyberattacks on organizations on each side of the conflict.
- An Israeli-backed cyberattack on Iran is less likely, as Israel has historically focused its targeting on threats to its physical security.

| Details

On April 13, 2024, Iran launched an unprecedented, large-scale missile and drone strike against Israel; it was the first direct attack on Israel from Iranian territory (as opposed to those initiated by Iranian proxies in the region). The attack almost certainly was in response to an Israeli strike on an Iranian diplomatic facility that killed several senior Islamic Revolutionary Guard Corps (IRGC) officials in Damascus on April 1, 2024.

- The strike included 170 Shahed-136/131 drones, 30 cruise missiles, and 120 ballistic missiles.¹ Lebanese Hezbollah, the Houthi movement in Yemen, and Shi'a Iraqi special groups participated in the attack as well. Iran also seized an Israeli-linked container ship in the Strait of Hormuz.²
- Ninety-nine percent of the missiles and drones launched were successfully intercepted by Israel and its allies before reaching their intended targets, and reporting indicates the incident caused no fatalities.

Following the attack, Iran issued a statement indicating that it deems the issue concluded. Iran appears not to have aimed at large civilian centers and also avoided attacking U.S. forces; it reportedly warned the United States of the strike through Turkey.³

In the short term, a smaller Israeli retaliation is likely, as the war cabinet threatened to “exact a price” against Iran.⁴ These efforts could potentially target proxy positions involved in the attack, such as those in Iraq and/or Syria.

- Israel's allies, including the United States and several European governments, are already strongly calling for Israel to declare the issue closed.⁵ President Joe Biden stated that the United States would not support an Israeli counterattack against Iran.⁶

| Supply Chains and Economic Impacts

Oil prices dropped in the immediate aftermath of the attack.⁷ Oil prices had been rising since Israel targeted the IRGC in Damascus on April 1 out of fear it would lead to Iranian

¹

[hXXps://www.usatoday\[.\]com/story/graphics/2024/04/15/us-israel-planes-missiles-iran-attack-maps/73316311007/](https://www.usatoday.com/story/graphics/2024/04/15/us-israel-planes-missiles-iran-attack-maps/73316311007/)

² [hXXps://www.bbc\[.\]com/news/world-middle-east-68806508](https://www.bbc.com/news/world-middle-east-68806508)

³

[hXXps://www.reuters\[.\]com/world/middle-east/iranian-notice-attack-may-have-dampened-escalation-risks-2024-04-14/](https://www.reuters.com/world/middle-east/iranian-notice-attack-may-have-dampened-escalation-risks-2024-04-14/)

⁴ [hXXps://www.cnn\[.\]com/2024/04/14/middleeast/israel-iran-attack-response-intl/index.html](https://www.cnn.com/2024/04/14/middleeast/israel-iran-attack-response-intl/index.html)

⁵

[hXXps://www.timesofisrael\[.\]com/european-allies-urge-israel-against-military-response-to-iran-as-war-cabinet-convenes/](https://www.timesofisrael.com/european-allies-urge-israel-against-military-response-to-iran-as-war-cabinet-convenes/)

⁶ [hXXps://www.axios\[.\]com/2024/04/14/biden-netanyahu-iran-israel-us-wont-support](https://www.axios.com/2024/04/14/biden-netanyahu-iran-israel-us-wont-support)

⁷

[hXXps://www.bloomberg\[.\]com/news/articles/2024-04-14/asian-stocks-set-to-fall-in-wake-of-iran-attack-market-s-wrap](https://www.bloomberg.com/news/articles/2024-04-14/asian-stocks-set-to-fall-in-wake-of-iran-attack-market-s-wrap)

retaliation that would widen the conflict. A broader conflict could see Iran close the Strait of Hormuz, through which 20 percent of the world's oil supply passes.⁸ More likely, there would be even more difficulty transporting oil by tanker ship in the Middle East, and Iran's oil production would be further sanctioned, pushing prices up even further.⁹

- The drop in prices reflects how much Iran's retaliation had already been factored into the price of oil and that the attacks were widely viewed as limited despite the large number of munitions fired at Israel.
- Expect energy prices to remain volatile for the coming weeks over the possibility of further retaliation from Israel.
- A sustained increase in energy prices would likely increase inflation globally and negatively impact the international economy through higher costs for manufacturing, trade, and travel. Even without a major Israeli retaliation, sustained elevated oil prices are likely through 2024.

The most significant impacts to supply chains will be for trade between Europe and Asia, which largely passes through the Middle East. The region's trade is already constrained due to Houthi attacks in the Red Sea. Iran's seizure of a container ship during the assault was likely meant to reinforce the threat Iran and its allies pose to global shipping.

- In the immediate lead-up to and during the attack, the airspace over a large portion of the Levant was closed to traffic, with numerous airlines adjusting and canceling routes in the region. Particularly affected were services at Israel's Ben Gurion Airport (TLV), Jordan's Queen Alia International Airport (AMM), and Lebanon's Rafic Hariri International Airport (BEY).¹⁰ The possibility of a wider war threatens air freight, another already costly alternative to sea shipping via the Suez Canal and the Red Sea.

⁸ [hXXps://www.eia\[.\]gov/todayinenergy/detail.php](https://www.eia.gov/todayinenergy/detail.php)

⁹ [hXXps://www.ft\[.\]com/content/b3faef5-b68f-4a35-a54f-1305afda1483](https://www.ft.com/content/b3faef5-b68f-4a35-a54f-1305afda1483)

¹⁰ [hXXps://www.cnn\[.\]com/2024/04/13/jordan-israel-close-airspace-amid-report-of-drone-attack-from-iran.html](https://www.cnn.com/2024/04/13/jordan-israel-close-airspace-amid-report-of-drone-attack-from-iran.html)



Flightradar24 over the Middle East on April 14, 2024, after Iran launched strikes towards Israel

Source:

<https://www.cnn.com/2024/04/13/jordan-israel-close-airspace-amid-report-of-drone-attack-from-iran.html>

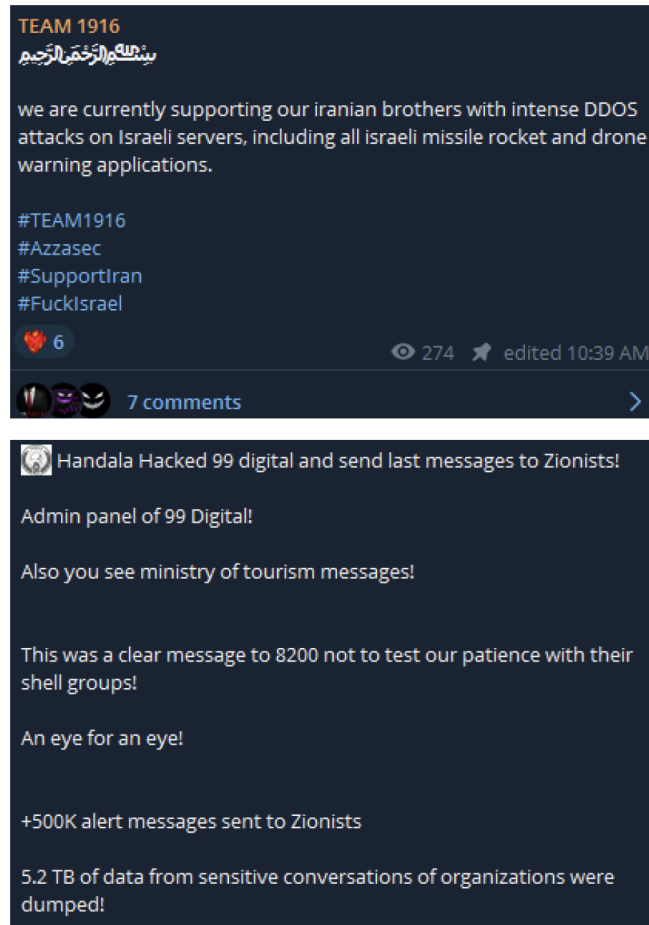
Cyber

The cyber threat to organizations operating in the region will very likely increase in the coming weeks. ZeroFox anticipates that high-profile organizations in Israel, Jordan, Iran, and Lebanon will very likely face an increased threat from state-linked entities and cybercriminals on both sides of the divide. It is unlikely countries further afield will see a notable increase in threat.

Before Iran's retaliatory missile launches on April 13, ZeroFox had observed a rise in cyberwar alliances backing Iran ahead of its expected retaliation against Israel for the April 1 strike that killed IRGC officials. While cyber threat actors may escalate their attacks against high-profile organizations on either side of the conflict, entities on the Israeli side are more likely to be targeted, as Israel may retaliate against Iran for this weekend's strike in the short term and is likely to continue its military hostilities with Hamas inside Gaza.

- The threat actor groups Mysterious Team Bangladesh, Sylhet Gang, and Red Evil have claimed to target Jordan for supporting Israel.

- Threat actor group Team Insane Pakistan has offered to support Iran, while Handala and Team 1916 have targeted Israel's digital infrastructure in support of Iran.
- Handala had earlier threatened Israel's Iron Dome Missile Defense System if Israel went ahead with its incursion into Rafah.¹¹



Samples of pro-Iranian cyber threat actors announcing plans to stage cyber operations in support of Iran

Source: ZeroFox Intelligence

Israel is more likely to respond militarily than through cyber domains. Israel's targeting of Iranian proxy groups in Iraq, Syria, Gaza, and Lebanon has historically focused on military targets that pose a risk to Israel's security. At the moment, the threat posed by well-armed militia groups near Israel's borders presents greater security risks than cyber

¹¹ ZeroFox Flash Report from March 6, 2024, titled "Threat Actors Target Israel over Possible Rafah Incursion"

threat actors backing Iran or Hamas, who are mainly engaged in website defacements and distributed denial-of-service (DDoS) attacks.

| Conclusion

Given Western pressure and the lack of fatalities associated with the April 13 attack, the response from the Israeli government will likely remain limited and designed to avoid further escalation. However, at least one Israeli report has indicated that Prime Minister Benjamin Netanyahu may threaten to maintain “tit-for-tat” attacks unless the United States and other countries back down from insisting that the conflict in the Gaza Strip must eventually lead to a two-state solution.¹² Regardless, the conflict between Israel and Tehran has now reached its most dangerous point in decades, creating serious risks in the cybersecurity and supply chain environments.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
12 hXXps://www.timesofisrael.com/war-cabinet-said-to-favor-hitting-back-at-iran-but-divided-over-when-and-how/ 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.

| 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%