



Flash

Conflict in Israel

F-2023-10-09a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Geopolitical, Military

October 9, 2023

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 12:00 PM (EDT) on October 9, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Conflict in Israel

| Executive Summary

Hamas' large-scale surprise incursion into Israel is unprecedented by numerous metrics; Israel's intelligence community and its Western allies must confront its worst intelligence failure in 50 years. The sophistication and effectiveness of Hamas' attack indicate significant international support, which went largely unnoticed—adding to the fear that will likely permeate Israeli society in the medium and long term. The government of Prime Minister Benjamin Netanyahu will be under heavy pressure to respond forcibly in order to regain a sense of security. Hamas is likely prepared for this, and the longer this conflict goes on, the more likely it will be to spread across the region. In the cyber arena, threat actors have already begun to pick sides in the conflict, indicating an increasingly adverse cybersecurity environment in the Middle East. Travel across the region, particularly to and from Israel and the Palestinian territories, will be severely impacted as long as this stage of the conflict persists.

| Analyst Commentary

On October 7, 2023, Hamas, the militant organization that controls the Gaza Strip, launched a large-scale, surprise assault against Israeli communities bordering the enclave. The multi-pronged attack, which included thousands of rockets fired into Israel as well as ground, air, and water-based assaults, has resulted in the deaths of at least

800 Israelis, with over 2,200 wounded.¹ Dozens of foreign and dual nationals have also reportedly been killed and wounded.² Additionally, Hamas claims to have abducted at least 100 civilians and Israeli military personnel.³ Islamic Jihad, a smaller militant group operating in the Gaza Strip, also asserted that the group is in possession of 30 hostages.⁴ As of afternoon hours local time on October 9, 2023, Israeli military officials stated that the Israeli Defense Forces (IDF) successfully regained control of the besieged communities in southern Israel. However, they also warned that scattered militants may remain in the area amid reports of sporadic fighting on the Israeli side of the Gaza border fence.⁵

In response to the incursion, Israeli warplanes continue to strike Hamas targets within the Gaza Strip. According to Palestinian health authorities, at least 560 people have been killed in the retaliatory strikes, with a further 2,900 wounded.⁶ Israeli forces are also in the midst of implementing a “full siege” of the enclave, staging large numbers of troops near the border fence, as well as cutting off electricity and water supplies.⁷

Smaller-scale fighting has also been seen on Israel’s northern border with Lebanon. On October 8, 2023, Israeli troops and Hezbollah militants exchanged rocket fire.⁸ Israeli forces also claimed to have killed several “armed infiltrators” from Lebanon on October 9, 2023. However, Hezbollah denied a role in the incident.⁹

¹

[hXXps://www.timesofisrael\[.\]com/death-toll-from-hamas-onslaught-passes-600-over-100-kidnapped-as-israel-s-trikes-gaza/](https://www.timesofisrael.com/death-toll-from-hamas-onslaught-passes-600-over-100-kidnapped-as-israel-s-trikes-gaza/)

² [hXXps://www.washingtonpost\[.\]com/world/2023/10/08/american-dead-israel-hamas-foreign-national/](https://www.washingtonpost.com/world/2023/10/08/american-dead-israel-hamas-foreign-national/)

³ [hXXps://www.jpnn\[.\]com/breaking-news/article-762037](https://www.jpnn[.]com/breaking-news/article-762037)

⁴ [hXXps://www.politico\[.\]com/news/2023/10/08/israelis-held-hostage-gaza-00120542](https://www.politico.com/news/2023/10/08/israelis-held-hostage-gaza-00120542)

⁵

[hXXps://www.timesofisrael\[.\]com/liveblog_entry/idf-spokesperson-says-military-has-regained-control-of-all-gaza-border-towns-but-terrorists-may-remain/](https://www.timesofisrael.com/liveblog_entry/idf-spokesperson-says-military-has-regained-control-of-all-gaza-border-towns-but-terrorists-may-remain/)

⁶ [hXXps://twitter.com/MOH_PR/status/1711353191617397076](https://twitter.com/MOH_PR/status/1711353191617397076)

⁷ [hXXps://www.cnn\[.\]com/2023/10/09/middleeast/israel-gaza-hamas-fighting-monday-intl-hnk/index.html](https://www.cnn.com/2023/10/09/middleeast/israel-gaza-hamas-fighting-monday-intl-hnk/index.html)

⁸ [hXXps://www.newarab\[.\]com/news/hezbollah-and-israel-exchange-rocket-fire-amid-hamas-attack](https://www.newarab.com/news/hezbollah-and-israel-exchange-rocket-fire-amid-hamas-attack)

⁹

[hXXps://www.reuters\[.\]com/world/middle-east/israel-retaliates-after-hamas-attacks-deaths-pass-1100-2023-10-09/](https://www.reuters.com/world/middle-east/israel-retaliates-after-hamas-attacks-deaths-pass-1100-2023-10-09/)

| Historical Context

In 2005, Israeli forces unilaterally withdrew from Gaza. A year later, Hamas won the 2006 Palestinian Legislative election and subsequently violently ejected rival Fatah forces in 2007.¹⁰ Since this time, conflicts in and around the Gaza Strip have become a regular occurrence, including a 22-day Israeli invasion in December 2008 and January 2009 and the 2014 Gaza War, which also saw an Israeli ground invasion.¹¹ While cross-border attacks launched by Palestinian militants have occasionally occurred,¹² they have been limited in scope, making this current fighting unprecedented in the conflict's history.

| Cyber

Threat actors have already been observed picking sides in the conflict, indicating an increasingly adverse cybersecurity environment in the Middle East. Attacks targeting both Israel and Palestine perpetrated by hacktivist groups and state-sponsored threat actors have occurred since Hamas' attack and Israel's subsequent declaration of war. Distributed denial-of-service (DDOS) attacks were reportedly the most frequently utilized attacks by groups so far. While a majority of the hacktivists' claims are unsubstantiated, major hacktivist organizations, like Anonymous Sudan and Killnet, have executed disruptive attacks in the past.¹³

Hacktivist group Anonymous Sudan was allegedly the first to target Israel's warning systems, followed by the Israeli Jerusalem Post media outlet; its website is currently not available.¹⁴ Cyber Av3ngers targeted critical infrastructure in Israel, such as energy grids and power plants, and were reported to have taken down a website.¹⁵ The hacktivist group Killnet also attested to taking down Israeli websites. Meanwhile, other groups, such as the Cyber Force and ThreatSec, launched initiatives targeting Palestinian government

¹⁰ [hXXps://www.theguardian.com/world/2007/jun/15/israel4](https://www.theguardian.com/world/2007/jun/15/israel4)

¹¹ [hXXps://www.reuters.com/world/middle-east/conflict-between-israel-palestinians-gaza-2023-10-07/](https://www.reuters.com/world/middle-east/conflict-between-israel-palestinians-gaza-2023-10-07/)

¹²

[hXXps://www.washingtonpost.com/world/middle-east/gunmen-attack-israeli-bus-near-egypt-border/2011/08/18/gIQAAtFf8MJ_story.html](https://www.washingtonpost.com/world/middle-east/gunmen-attack-israeli-bus-near-egypt-border/2011/08/18/gIQAAtFf8MJ_story.html)

¹³ [hXXps://www.securityweek.com/hackers-join-in-on-israel-hamas-war-with-disruptive-cyberattacks/](https://www.securityweek.com/hackers-join-in-on-israel-hamas-war-with-disruptive-cyberattacks/)

¹⁴ [hXXps://twitter.com/Jerusalem_Post/status/1710898092055068889](https://twitter.com/Jerusalem_Post/status/1710898092055068889)

¹⁵ [hXXps://twitter.com/FalconFeedsio/status/1711033041827828087](https://twitter.com/FalconFeedsio/status/1711033041827828087)

infrastructure, with members of ThreatSec announcing that it had compromised the internet in Gaza.¹⁶

The group Libyan Ghosts has also reportedly been targeting websites in Israel.¹⁷ The YourAnonTI3x hackers group has claimed to have targeted multiple websites in Israel.¹⁸ Security researchers reported on X (formerly known as Twitter) that the group Killnet began a massive cyberattack on all Israeli government systems.¹⁹ The X account Anonymous also reported that the groups Anonymous Sudan, KillNet, and Moroccan Black Cyber have officially launched a cyber war against the Israeli government.²⁰ Lastly, the group Storm-1133 has also been reported to be targeting Israeli energy, defense, and telecom; the group has been attributed as being close to Hamas.^{21 22}

ZeroFox researchers have observed multiple actors organizing credential dumps via various channels targeting the Israeli government and private industry. These actors have been observed sharing credential dumps among multiple groups to increase attack spread.

Data leaked 🔥🔥 by AnonOne on one of the Israeli Ministry of Defense's deep web sites following the hack that occurred today from the Storm-1133 group.

Threat Actors Sharing Credential Dumps

Source: ZeroFox Internal Collections

¹⁶ [hXXps://www.theregister\[.\]com/2023/10/09/hackivism_middle_east/](https://www.theregister.com/2023/10/09/hackivism_middle_east/)

¹⁷ [hXXps://twitter\[.\]com/FalconFeedsio/status/1711198577417224214](https://twitter[.]com/FalconFeedsio/status/1711198577417224214)

¹⁸ [hXXps://twitter\[.\]com/YourAnonTI3x](https://twitter[.]com/YourAnonTI3x)

¹⁹ [hXXps://twitter\[.\]com/aliifill/status/1711038069778854239](https://twitter[.]com/aliifill/status/1711038069778854239)

²⁰ [hXXps://twitter\[.\]com/YourAnonOne/status/1711374825128653310](https://twitter[.]com/YourAnonOne/status/1711374825128653310)

²¹ [hXXps://thehackernews\[.\]com/2023/10/gaza-linked-cyber-threat-actor-targets.html](https://thehackernews[.]com/2023/10/gaza-linked-cyber-threat-actor-targets.html)

²² [hXXps://cybernews\[.\]com/cyber-war/microsoft-names-hamas-linked-group-targeting-israel/](https://cybernews[.]com/cyber-war/microsoft-names-hamas-linked-group-targeting-israel/)

```
.il-2474.txt  
Israel gov sites logins  
You can login do what ever you want 🤖  
  
F*ck Israel ❌  
  
Banks, companies,gov logins include!
```

Threat Actors Sharing Credential Dumps*Source: ZeroFox Internal Collections*

Concentrated cyberattacks are likely to continue as the conflict between Israel and Palestine escalates and may worsen. Cyberattacks, particularly DDoS attacks, will continue to affect companies based in Israel and Palestine. Media outlets, as well as government websites and infrastructure, are popular targets of threat actors during periods of political upheaval.²³

| Travel

Several international airlines have reportedly suspended flight services with Tel Aviv over the weekend or until further notice, impacting hundreds of flights. Israel's national carrier, El Al, was the exception, adding more flights to bring reservists back worldwide to assist in troop mobilizations. However, while regulators—including the U.S. Federal Aviation Administration, the European Union Aviation Safety Agency, and Israel's aviation authority—urged airlines to use caution in the region's airspace, they refrained from suspending flights.

²³ [hXXps://www.securityweek\[.\]com/hackers-join-in-on-israel-hamas-war-with-disruptive-cyberattacks/](https://www.securityweek.com/hackers-join-in-on-israel-hamas-war-with-disruptive-cyberattacks/)

Africa	Royal Air Maroc canceled flights to and from Tel Aviv on Saturday and Sunday. The company offered support to passengers holding tickets to and from Tel Aviv Ben Gurion airport with travel dates up to October 13. ²⁴
Americas	On Sunday, U.S. air carriers United Airlines, Delta Air Lines, and American Airlines suspended direct flights following the FAA's caution advisories. ²⁵ Reportedly, United suspended services "until conditions allow them to resume." Air Canada canceled flights to and from Tel Aviv "until further notice." ²⁶
Asia	Cathay Pacific canceled its Tuesday and Thursday flights between Hong Kong and Tel Aviv and said it would provide further updates regarding its next scheduled service. Korean Air canceled its Monday flight between Incheon and Tel Aviv, and it expects future flights to be irregular.
Europe	- In Germany, flight operations at the Hamburg Airport were completely stopped on Monday due to a threat of attack on a plane from Tehran. Operations resumed two hours later after local federal police checked the plane without results.²⁷ Lufthansa has decided to suspend its regular flights to and from Tel Aviv up to and including October 14.²⁸ - Air France KLM suspended flights without providing a time frame. Its unit Transavia France canceled two flights on Monday and said it would provide a further update later in the evening.²⁹ - Spain-based Air Europa said it would be monitoring the situation and would be ready to delay or cancel flights if needed. Iberia Airlines, owned by IAG, canceled flights to Israel during the weekend and reported operating only one on Monday. IAG-owned Vueling also canceled flights from Barcelona to Tel Aviv. Although the carrier will resume daily round trips from Monday evening, it will monitor the situation for possible delays and cancellations. - Britain's easyJet halted flights with Tel Aviv on Sunday and Monday and said it would adjust the timing of flights in the next few days. Ryanair canceled all flights to and from Tel Aviv through Wednesday. Virgin Atlantic said its flights between London Heathrow and Tel Aviv could face delays or cancellations. - Italy's ITA and Greece's Aegean Airlines have canceled their flights to and from Tel Aviv until Oct. 10.³⁰³¹ Portugal's TAP canceled flights to and from Tel Aviv scheduled for Sunday and Monday. Finnish carrier Finnair and Hungarian Wizz Air suspended flights until further notice. - Air Malta canceled two return trips on Monday and Wednesday, saying it would continually adjust its schedule as needed. Poland's LOT said flights from Tel Aviv may be delayed or canceled in the upcoming days.³² Bulgaria Air canceled a return flight to Tel Aviv on Monday and Tuesday, but it said a flight to and from Tel Aviv on Thursday was scheduled to operate as planned.
Middle East	Etihad Airways canceled flights between Abu Dhabi and Tel Aviv on Monday and Tuesday. ³³ Gulf Air canceled all flights to Tel Aviv until Oct. 14. ³⁴

²⁴ [hXXps://www.royalairmaroc\[.\]com/us-en/information/delays-and-disruptions](https://www.royalairmaroc.com/us-en/information/delays-and-disruptions)

²⁵

[hXXps://www.reuters\[.\]com/world/several-airlines-suspend-tel-aviv-flights-until-conditions-improve-2023-10-08/](https://www.reuters.com/world/several-airlines-suspend-tel-aviv-flights-until-conditions-improve-2023-10-08/)

²⁶ [hXXps://www.aircanada\[.\]com/ca/en/aco/home/book/travel-news-and-updates/2023/civil-unrest-israel.html#/](https://www.aircanada.com/ca/en/aco/home/book/travel-news-and-updates/2023/civil-unrest-israel.html#/)

²⁷

[hXXps://www.bild\[.\]de/news/2023/news/verkehr-eingestellt-anschlagsdrohung-am-flughafen-hamburg-85685510.bild.html](https://www.bild.de/news/2023/news/verkehr-eingestellt-anschlagsdrohung-am-flughafen-hamburg-85685510.bild.html)

²⁸ [hXXps://www.lufthansa\[.\]com/xx/en/flight-information](https://www.lufthansa.com/xx/en/flight-information)

²⁹ [hXXps://www.transavia\[.\]com/en-EU/flight-status/search/](https://www.transavia.com/en-EU/flight-status/search/)

³⁰ [hXXps://www.ita-airways\[.\]com/en_il/fly-ita/news-and-activities/news/tel-aviv-airport.html](https://www.ita-airways.com/en_il/fly-ita/news-and-activities/news/tel-aviv-airport.html)

³¹ [hXXps://en.aegeanair\[.\]com/](https://en.aegeanair.com/)

³² [hXXps://www.lot\[.\]com/pl/en/situation-in-israel](https://www.lot.com/pl/en/situation-in-israel)

³³ [hXXps://www.etihad\[.\]com/en/manage/flight-tracker](https://www.etihad.com/en/manage/flight-tracker)

³⁴ [hXXps://www.gulfair\[.\]com/en/](https://www.gulfair.com/en/)

Forward Look

The conflict could potentially widen to include other regional actors. According to senior Hamas officials, Iran reportedly played a crucial role in the planning and execution of the incursion.³⁵ If true, Tehran could also pressure Hezbollah, its proxy in Lebanon, to escalate attacks against Israel, threatening a multi-front war. Iran could also be targeted with increased sanctions, potential cyberattacks, or even military retaliation for its purported role in the attack. Renewed sanctions against Iran will worsen supply chain disruptions, especially along energy supply lines.

Regardless, the fighting in the Gaza Strip shows no signs of abating in the near term. Rocket fire continues to strike Israel's main urban centers.³⁶ Meanwhile, Israel has officially declared war and is amassing troops for a potential land invasion amid a call-up of 300,000 soldiers, the largest in the country's history.³⁷³⁸ Any Israeli incursion into the Gaza Strip will be costly, given the enclave's difficult urban fighting environment and Hamas' likely extensive military preparations.

Another avenue through which the conflict may persist is the resolution of the hostage situation. Hamas stated that the group would like to exchange their Israeli hostages for "all Palestinian prisoners in Israeli jails."³⁹ However, afraid of the precedent it would set, the Israeli government may refuse to negotiate⁴⁰ or pay that high of a price, instead favoring military operations aimed at securing their release, something which could extend the conflict in some form for months if not years.

³⁵ [hXXps://www.wsj.com/world/middle-east/iran-israel-hamas-strike-planning-bbe07b25](https://www.wsj.com/world/middle-east/iran-israel-hamas-strike-planning-bbe07b25)

³⁶

[hXXps://www.timesofisrael.com/liveblog_entry/woman-critically-injured-man-seriously-hurt-in-rocket-strikes-near-jerusalem/](https://www.timesofisrael.com/liveblog_entry/woman-critically-injured-man-seriously-hurt-in-rocket-strikes-near-jerusalem/)

³⁷

[hXXps://www.aljazeera.com/news/2023/10/7/world-is-watching-fears-grow-of-a-massive-gaza-invasion-by-israel](https://www.aljazeera.com/news/2023/10/7/world-is-watching-fears-grow-of-a-massive-gaza-invasion-by-israel)

³⁸

[hXXps://www.bloomberg.com/news/articles/2023-10-09/israel-is-mobilizing-300-000-reservists-in-largest-ever-call-up](https://www.bloomberg.com/news/articles/2023-10-09/israel-is-mobilizing-300-000-reservists-in-largest-ever-call-up)

³⁹

[hXXps://www.aljazeera.com/news/2023/10/9/dozens-of-israelis-being-held-hostage-by-hamas-israeli-military-says](https://www.aljazeera.com/news/2023/10/9/dozens-of-israelis-being-held-hostage-by-hamas-israeli-military-says)

⁴⁰

[hXXps://www.timesofisrael.com/liveblog_entry/israeli-official-denies-report-of-qatar-mediated-negotiations-for-prisoner-swap/](https://www.timesofisrael.com/liveblog_entry/israeli-official-denies-report-of-qatar-mediated-negotiations-for-prisoner-swap/)

On the diplomatic front, the fighting is likely to cool regional rapprochement efforts, including a normalization agreement between Israel and Saudi Arabia that was reportedly near completion before Hamas' attack.⁴¹ It may also isolate Israel in the region, at least temporarily, by forcing Arab nations to show solidarity with the Palestinian cause—a possible *raison d'être* for the invasion.

⁴¹

[hXXps://www.economist\[.\]com/middle-east-and-africa/2023/09/24/america-israel-and-saudi-are-at-the-cusp-of-a-deal](https://www.economist.com/middle-east-and-africa/2023/09/24/america-israel-and-saudi-are-at-the-cusp-of-a-deal)

| 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%