

archive.today

webpage capture

Saved from <https://www.nytimes.com/2024/10/18/world/middleeast/anonymous-sudan-cy>

search

19 Oct 2024 09:47:08 UTC

All snapshots from host www.nytimes.com[history](#) [prior](#) [next](#)

Webpage

Screenshot

[share](#)[download .zip](#)[report bug or abuse](#)**The New York Times**[Middle East Crisis](#) | [LIVE Updates](#) [Hamas Leader Is Dead](#) [Who Was Yahya Sinwar?](#) [Drone Footage](#) [How Israel Killed Sinwar](#) [Cease-Fire Talks](#)

U.S. Indicts 2 Linked to Oct. 7 Cyberattack on Israeli Warning System

The Justice Department has accused two Sudanese brothers of cyberattacks on U.S. infrastructure as well as preventing possibly lifesaving alerts from reaching Israelis as the Hamas attack unfolded.

Listen to this article · 6:41 min [Learn more](#)

Share full article



An apartment complex in Ashkelon, Israel, that was hit by rockets fired by Hamas on Oct. 7, 2023. Tamir Kalifa for The New York Times

By [Michael Schwirtz](#)

Oct. 18, 2024

It was early morning on Oct. 7, 2023, and Hamas fighters had just breached the Israeli border, when Ahmed Omer, a young Sudanese man with an aptitude for computers, launched a different kind of attack.

Sitting at a computer, he mounted a long-distance cyberassault on the online early warning systems used in Israel to alert citizens to danger. The systems were briefly disabled, preventing potentially lifesaving warnings from reaching Israelis about [Hamas's deadly](#)

assault, in which about 1,200 people were killed and more than 200 abducted.

That was the case made against Mr. Omer and his brother, Alaa Omer, in a criminal indictment unsealed in California this week. “This was the most dangerous cyber group in terms of DDoS attacks in the world,” E. Martin Estrada, the United States Attorney for the Central District of California, said in a call with reporters.

The brothers are accused of running a group called Anonymous Sudan, which for the year it existed launched as many as 35,000 cyberassaults known as distributed denial of service, or DDoS, attacks. The attacks disrupted websites belonging to government agencies, including the F.B.I. and Justice Department, and to news agencies, such as The Washington Post and CNN, according to the indictment.

They also attacked hospitals in various countries.

The indictment outlines in detail actions against the United States, Israel and a number of other countries, including Denmark, France and Sweden. The California attorney’s office claims jurisdiction because the operation attacked American entities.

In February, the brothers shut down critical computer systems belonging to the Cedars-Sinai hospital in Los Angeles, causing emergency services to temporarily divert patients to other hospitals, according to the indictment. The brothers, who have been arrested and are in custody in an unspecified country, claimed at the time that the attack was in retaliation for Israel’s bombing of hospitals in Gaza.

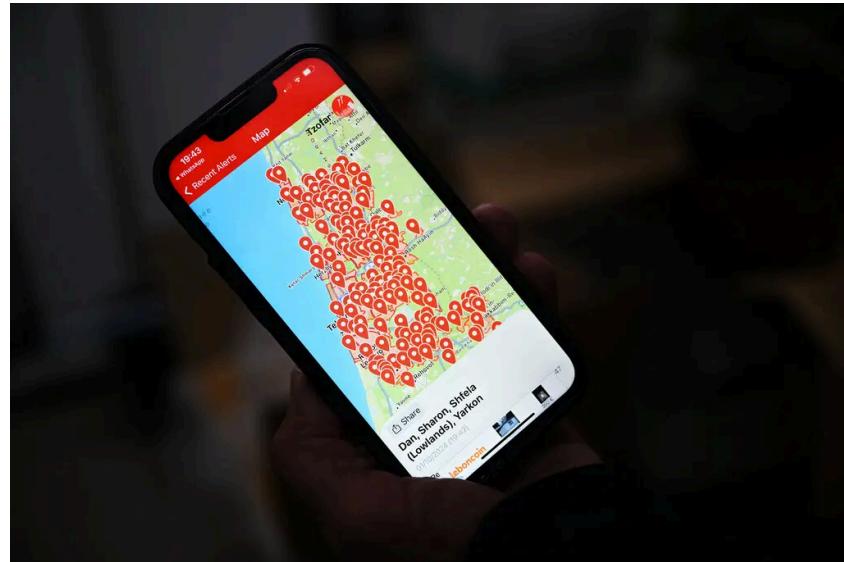
“Bomb our hospitals in Gaza, we shut down yours too, eye for eye,” they wrote on Telegram, the messaging app.

Their actions were so damaging, and potentially life-threatening, that prosecutors have included one charge against Ahmed Omer that carries a maximum sentence of life in prison, the first time the United States has threatened a cybercriminal with such punishment, according to Mr. Estrada.

“When you’re attacking hospitals, you’re putting lives in jeopardy, and this one certainly put lives in jeopardy,” Mr. Estrada said in the call with reporters.

The attacks on Israel were perhaps the most dramatic and damaging done by Anonymous Sudan, officials said.

In the hour after Hamas fighters launched their attack, first with rocket fire and then by breaching the Israeli border on foot and by paraglider, Anonymous Sudan targeted two private companies that provide online applications designed to alert Israeli users to danger.



The Tzofar - Red Alert app showing alerts for incoming rockets, this month. Leon Neal/Getty Images

A representative from one application, Tzofar - Red Alert, confirmed that the company had “suffered from a major DDoS attack to our services” in the early hours of Oct. 7, which made it difficult to access the company website. Users continued to receive alerts to the mobile app without interruption, said the company representative, who requested anonymity to discuss internal company matters.

“We are currently targeting some critical endpoints in the alert systems of Israel,” Anonymous Sudan posted to its Telegram channel on Oct. 7. “Glory to the Palestinian Resistance, we are with you.”

The group also targeted The Jerusalem Post, according to the indictment. Starting the morning of Oct. 8, the Israeli English-language daily reported [in an online post](#) that “multiple cyber attacks” caused “our site to crash.”

Middle East Crisis: Live Updates ›

Updated 2 hours ago

- [Here are the latest developments.](#)
- [What will happen to Yahya Sinwar's body?](#)
- [Some of the items Israel said it found near Sinwar: Mentos, a map, an expired passport.](#)

The indictment gives no indication that the brothers coordinated with members of Hamas during the attack. Only a few senior Hamas leaders knew the full extent of the operation before it began.

But the speed with which Anonymous Sudan responded — the first cyber attack on the alert system came less than 30 minutes after

the border was breached — underscored the skill and speed of its operation, experts said.

A group calling itself Anonymous Sudan appeared on the Telegram messaging app in January 2023. Despite the name, cybersecurity researchers long believed that the group served as a front for Russian cybercriminals.

For a time, the group posted in the Russian language. And within a month of its creation, Anonymous Sudan announced a partnership with REvil and Killnet, two of the most prominent Russian cybercriminal groups, and took part in joint attacks on Ukrainian computer systems.

Eventually, the group began publishing comments in Arabic and choosing targets that seemed to reflect a pan-Islamist viewpoint, said Ian Gray, the vice president for cyberthreat intelligence operations at Flashpoint, a cybersecurity company. Mr. Gray said that there was no indication that Anonymous Sudan had any connection to state actors, though the Russian cybercriminal groups with whom the group interacted have ties to Russia's security services.

"Any overlap between Anonymous Sudan and pro-Kremlin threat actors appears to be ideological and not based on national origin," Mr. Gray said.

It is not clear when the brothers might be extradited to the United States for trial, if ever. Mr. Estrada said that they were in custody outside the United States and had been interrogated by the F.B.I. He would not say the country where they were being held.

The group's attacks against Israel did not begin on Oct. 7. Earlier in the year, Anonymous Sudan launched attacks on a utilities provider, on the Israeli military and on the country's Supreme Court, according to the indictment and to cybersecurity researchers who have followed the group.

In May 2023, according to Flashpoint, the group launched an attack on Israel's Iron Dome defense system at the time of a rocket attack from Gaza. In that attack, 16 rockets were able to get past Israeli defenses, a larger than normal number, Flashpoint said in an internal report sent to The New York Times.

In one of their messages on Telegram from that time, Anonymous Sudan warned that it would coordinate with Hamas in future attacks.

"We are now playing with Israel again," the group wrote. "The strong strikes will be when there is a missile attack from Gaza."

Michael Schwirtz is an investigative reporter with the International desk. With The Times since 2006, he previously covered the countries of the former Soviet Union from Moscow and was a lead reporter on a team that won the 2020 Pulitzer Prize for articles about Russian intelligence operations. [More about Michael Schwirtz](#)

See more on: [U.S. Justice Department](#), [Israel-Hamas War News](#), [Hamas](#), [Federal Bureau of Investigation](#)[Share full article](#)**More in Middle East**

Israel Defense Force, via Associated Press

Sinwar's Final Moments: On the Run, Hurt, Alone, but Still Defiant

Image by Samar Abu Elouf for The New York Times

Surprise Battlefield Encounter Led to Hamas Leader's Death

Discovery's Expedition Unknown

In Jordan, a 'Stunning' Discovery Under Petra's Ancient Stone

Samar Abu Elouf for The New York Times

Yahya Sinwar, Leader of Hamas, Is Dead**Trending in The Times****A Weary Trump Whips Up Anger in Atlanta****Montana Camper Was the Victim of a Brutal Homicide, Not a Bear, Sheriff Says****Prediction Markets Tell a Different Story From the Polls****In Montauk, N.Y., an \$18 Million Listing for a Secluded Stone House****Sex, Horses and Stately Homes: Bringing a Naughty British Romance to TV****Don't Fall in Love With This Watch. It's Already Sold Out.****2 Triathletes Dead at World Championships, Organizers Say****Why Are People Wearing Bedroom Slippers on City Streets?****What We Know About Liam Payne's Death****Trump Among New York's Elites at a Charity Dinner: It Got Awkward****Editors' Picks**

Rozette Halvorson for The New York Times

Has a Celebrity Interview Made You Cringe? It Was Probably Hers.

Beau Grealy

Are They Not Famous, or Are You in a Bubble?**The New York Times**[Go to Home Page >](#)**NEWS****ARTS****LIFESTYLE****OPINION****MORE**

© 2024 The New York Times Company

NYTCo

Contact Us

Accessibility

Work with us

Advertise

T Brand Studio

Your Ad Choices

Privacy Policy

Terms of Service

Terms of Sale

Site Map

Help

Subscriptions

[Manage Privacy Preferences](#)