


# THE USE OF CYBERTERRORISM IN THE ISRAEL-HAMAS WAR



نعمل بفضل الله بكل هدوء وثبات ، ونجد في الله قوتنا والنصر حليف المقاومة بإرادته وقدرته. نرفع رؤوسنا بثقة، مؤكداً أن العدو قد فشل بشكل كامل في مواجهة هجمات وحدة السايبر.  
#طوفان\_الأقصى\_الإلكتروني  
#وحدات\_السايبير\_المشتركة  
#العائدون

The Returnees - العائدون -   
12/16/23

SIMON  
WIESENTHAL  
CENTER



# INTRODUCTION

On October 7, 2023, during the Jewish Sabbath and festival of Simchat Torah, Hamas shocked the world by invading Israel from Gaza across multiple entry points. The results were devastating: the single largest one-day total of murdered Jews since the Nazi Holocaust. Hamas targeted civilian families, assaulted and kidnapped hundreds of other civilians who were taken hostage in Gaza. Evidence suggests that Hamas was preparing for a 'second phase' of assaults, targeting the people of Israel. In response to this unprecedented massacre of 1,200 Israelis and the kidnapping of others, Israeli forces invaded Gaza with the stated goal of destroying Hamas.

In the online sphere, the vicious attacks set off a wave of posts, images, memes, cyber terror attacks, and videos on social media, but also on the dark web and adjacent sites. The Simon Wiesenthal Center's (SWC) Digital Terrorism and Hate Project monitors the social media activities of over 7,000 groups, individuals, and online channels, many who support Hamas and other terrorist groups. This report will explore the explosion of cyberterrorist activity against Jewish and Israeli targets in the wake of October 7th and expose some of the key groups and actors that have caused significant disruption and threats to personal safety.

## WHAT IS CYBER-TERRORISM?

Cyber-attacks against Israel primarily target critical infrastructure, telephone and emergency contact systems, Homefront Command alert systems, energy, utilities, telecommunications, and transportation sectors. Nation-state actors, particularly from Iran, North Korea, Russia, China, and other supportive of the Palestinian terrorists, are significant perpetrators. They utilize tactics such as spear phishing, denial of service, data leaks, brute force attacks, and exploit known IT system vulnerabilities.

In addition, following the October 7th massacre in Israel, there has been a surge in cyberterrorist and cyber threat attacks against Jewish sites. The Antisemitism Cyber Monitoring System, operated by the Israeli Diaspora Affairs Ministry,

---

<sup>1</sup> <https://www.washingtonpost.com/national-security/2023/11/12/hamas-planning-terror-gaza-israel/>

<sup>2</sup> <https://cybernews.com/cyber-war/israel-redalert-breached-anonghost-hamas/>

<sup>3</sup> <https://www.washingtonpost.com/politics/2023/10/11/largest-cyberattack-its-kind-recently-happened-heres-how/>

reported that online calls for violence against Israel, Zionists, and Jews following the IDF Swords of Iron operation have increased by 1,200%.<sup>4</sup> In November 2023, Check Point Software Technologies reported, “We have seen an increase of approximately 20% in cyberattacks in Israel during the war, including more than 50% when it comes to attacks on the government sector. So far, we don’t see this increase elsewhere on a global level.”<sup>5</sup>



**Figure 1: The Returnees - Telegram**

countries like the United States and India also being targeted because of their support for Israel.<sup>9</sup>

Cyberterrorist groups have joined the fray, launching their own attacks on Israeli websites.<sup>6</sup> Notably, specific cyber threat actors have been identified, including: a Gaza-based actor known as Storm-1133 who has targeted Israeli energy, defense, and telecommunications sectors<sup>7</sup>; an Iran-linked group, Imperial Kitten, targeting the Middle East’s tech sector, including Israel<sup>8</sup>; and The Returnees, a hacker collective that has targeted both Israeli infrastructure and individual citizens. The cyberfront of the war has had a broader impact, with

<sup>4</sup><https://www.jpost.com/diaspora/antisemitism/article-768393>

<sup>5</sup><https://www.csoonline.com/article/1249135/cyberattacks-on-israel-intensify-as-the-war-against-hamas-rages-check-point.html>

<sup>6</sup><https://www.wired.com/story/israel-hamas-war-hackivism/>

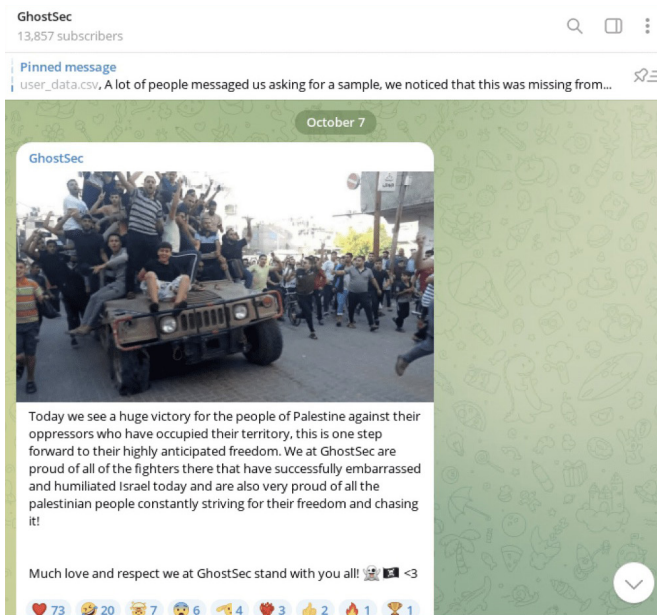
<sup>7</sup><https://techcrunch.com/2023/10/09/hackivism-erupts-in-response-to-hamas-israel-war/>

<sup>8</sup><https://thehackernews.com/2023/10/gaza-linked-cyber-threat-actor-targets.html>

<sup>9</sup><https://thehackernews.com/2023/11/iran-linked-imperial-kitten-cyber-group.html>



**Figure 2: AnonGhost (October 8) - Telegram**



**Figure 3: Ghostsec Cyber threat actor - Telegram**

Cyber-threats, cyber-attacks, and cyberterrorism against Israel is not a new phenomenon. However, the SWC monitored a significant uptick in activity by cyber threat actors both prior to, and post, October 7, 2023.

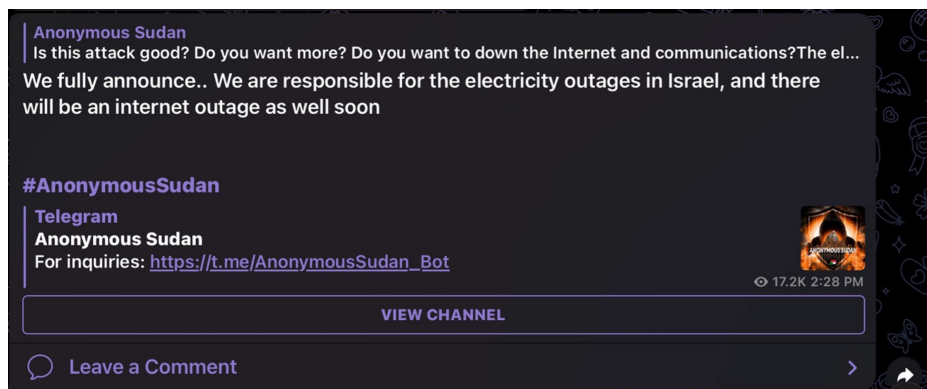
The SWC has identified at least 40 cyber terror entities that have participated and collaborated in cyber terror attacks targeting Israel. These groups and their collaborators have claimed responsibility for attacks against numerous Israeli internet domains. Some of these cyber terror groups regularly provide details of attacks they have conducted or information they have obtained. They have also shared graphic images and videos of the conflict as well as justification for their beliefs and actions.

It should be noted that the impact of cyberterror attacks on Israeli society during this war has been profound, having caused stress, anxiety, insecurity, and financial harm. Cyberterror attacks in Israel have led to service disruptions, physical damage, and even the risk of death or bodily injury, as a result of disruptions to the emergency telephone system. The psychological impact of cyber threats can rival those of traditional terrorism by instilling fear in civilian populations.<sup>10</sup>

<sup>10</sup>Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber terrorism. *The Bulletin of the atomic scientists*, 72(5), 284–291. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5370589/>

Some of the most prolific cyberterror actors are discussed herein:

## ANONYMOUS SUDAN



*Figure 4: Anonymous Sudan (April 2023) - Telegram*

denial-of-service (DDoS) attacks against targets in Israel, Sweden, Denmark, America,



*Figure 5: From Anonymous Sudan (Russia) - Telegram*

Anonymous Sudan is a pro-Palestinian, pro-Russian grassroots hacker group purporting to originate in Sudan. Since early 2023, they have participated in a variety of disruptive actions including distributed

Australia, and other countries where they believe anti-Muslim and anti-Palestinian activity takes place. DDoS attacks flood the targeted server with traffic, effectively eliminating its ability to operate. Anonymous Sudan is a multilingual, multiplatform entity. In April and May 2023, Anonymous Sudan enacted attacks against Israel's Iron Dome defense system. On October 7, 2023, pro-Palestine hacktivist group Team Bangladesh announced its support for Hamas and its alignment with Anonymous Sudan, using pro-Palestinian hashtags including #FreePalestine and #OpIsraelV2.



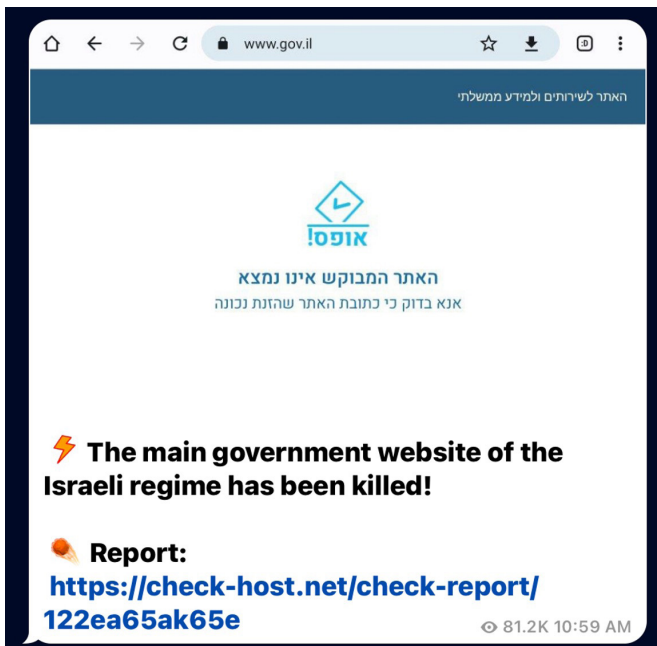
**Figure 6:**  
From Anonymous Sudan (Russia) - Telegram



## KILLNET

Killnet has recently united with Anonymous Sudan in its attacks against Israel. Killnet is multilingual, multiplatform entity. The Palestinian arm of Killnet was established on October 13, 2023. Hacker and cyberterror entities are often politically motivated and influenced, frequently aligning with state-sponsored cyber hacktivists. Killnet, via multilingual posts (English/ Russian/Arabic/ Hebrew), announced further intentions to target the Israeli government, and Anonymous Sudan issued similar threats (see figures 8 and 9).

**Figure 7: Killnet - Telegram**



**Figure 8:**  
*Killnet October 8 - Telegram*



**Figure 9:**  
*Anonymous Sudan - Telegram*

# GHOSTSEC

Ghostsec is a cyberthreat actor and hacktivist group which emerged as an offshoot of the infamous hacker group, Anonymous. Initially, the group focused on counterterrorism efforts and monitoring online activities associated with terrorism. They gained prominence following the 2015 Charlie Hebdo shooting in Paris and the rise of ISIS. Previously dedicated to thwarting, tracking, and disrupting ISIS-related online propaganda, they collaborated with law enforcement and intelligence agencies.<sup>11</sup> Ghostsec has now pivoted their activities to attacks against Israel. They have aligned with the interests of Hamas. Their activities have primarily impacted organizations they perceive as anti-Hamas. The campaign has targeted Israeli energy and defense sectors as well as entities affiliated with Fatah, a Palestinian political party based in the West Bank that is a rival to Hamas.

Uptycs.com, a cyber security company, lists these recent activities attributed to GhostSec:

- In May 2022, the HRVAC website in Israel was hacked, resulting in the release of personal and credential data.
- In June 2022, the hacker group targeted telecommunications and electricity industries with successful hacks.
- In July 2022, the focus of the attacks was on energy and sewage systems industries.
- In August 2022, military data and railway system API data were exposed in a data leak.
- In September 2022, PLC devices became the target of the attacks.
- In April 2023, the focus of the attacks was on the water pump Industry.
- In May 2023, unauthorized access to PLC devices resulted in a data leak.
- In October 2023, there was an attack on water pumps alongside the deployment of GhostLocker ransomware.
- During November 2023, this group continuously launched cyber-attacks on Israel in response to alleged war crimes.

---

<sup>11</sup><https://www.uptycs.com/blog/ghostlocker-ransomware-ghostsec>





*Figure 10: Ghostsec - Telegram*

## CYB3R DRAGONZ

Little is known about the provenance of cyber threat actor Cyb3r Drag0nz. In early October, they posted a survey to their Telegram channel asking users which country they should support. 83% of 392 respondents voted for "Palastine [sic]", and 17% for Israel.



*Figure 11: Cyb3r Drag0nz - Telegram*



Figure 12: Cyb3r Drag0nz - Telegram



Figure 13: Cyb3r Drag0nz - Telegram

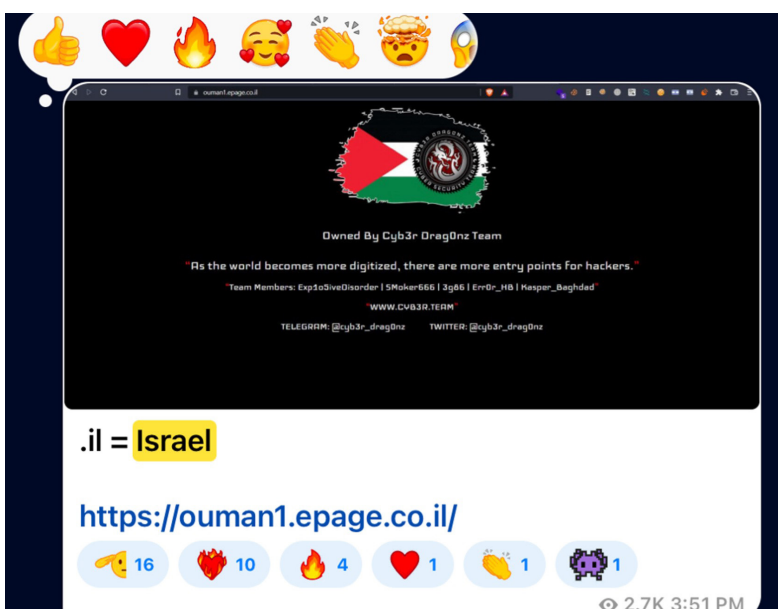


Figure 14: Cyb3r Drag0nz - Telegram

Pro-Palestinian cyber terror groups have also targeted Israeli citizens and sympathizers. Personal information has been leaked, with supporters and sympathizers being encouraged to target social media accounts to harass users with pro-Palestinian messages.

## PRO-ISRAEL EFFORTS:

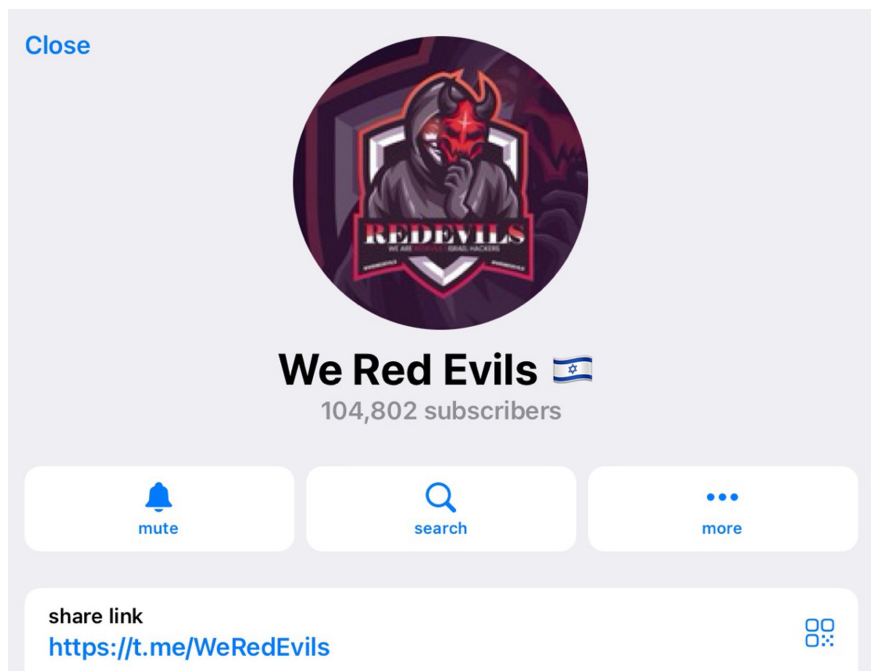
Multiplatform Garuna Ops has aligned itself with Israel and in the process has also committed numerous attacks against Yemeni, Bangladeshi and some Palestinian interests. They have publicly stated that they would commit attacks against any government or country which displays support for Hamas and Palestine.



*Figure 15: Garuna Ops (October 7, 2023) - X (formerly Twitter)*

# WE RED EVILS

We Red Evils is a fledgling multiplatform Israeli hacker group that emerged in October 2023. The group has become known for its attacks targeting pro-Palestinian and pro-Hamas countries and sites. They have successfully breached the systems of those affiliated with the Iranian Revolutionary Guards Corps and impacted the power grid and infrastructure in Iran.



**Figure 16:** We Red Evils - Telegram



**Figure 16:** We Red Evils - X (formerly Twitter)

## CONCLUSION

Cyberterrorism is playing a significant role in the war between Israel and Hamas, with Hamas and its backers exploiting vulnerabilities in Israel's technology-reliant defense systems.<sup>12</sup> In planning the October 7th massacre, Hamas researched areas with minimal camera coverage, and then used drones to drop grenades, disrupting Israel's surveillance apparatus, increasing the deadly nature of their attacks.<sup>13</sup>

Hacker and cyberterror attacks by nation-state groups and actors via proxy-attacks (inspired by Iran and others) against Israeli critical infrastructure such as media, energy, utilities, telecommunications, and transportation have grown exponentially.<sup>14</sup> While the observed cyberterror tactics are not assessed to be highly sophisticated, they have been disruptive, and it is likely more sensitive information is being shared in closed channels. Despite their lack of sophistication, these attacks are highly effective in spreading fear.<sup>15</sup> The impact of cyberterrorism on Israeli society is multifaceted, affecting both the psychological well-being of individuals and the public's confidence in institutions tasked with keeping them safe.<sup>16</sup> The psychological effects of cyber threats can be very severe, inducing stress, anxiety, and insecurity.<sup>17</sup>

The threats from cyberterrorism are also significant for highly digitalized economies like Israel. The post October 7th rise in cyberattacks has also seen an increase in cyber operations and threats against Jewish, Muslim, and Arab-American communities and institutions.<sup>18</sup> The cyberterrorism and cyber warfare components of this war have added a new dimension in this conflict, demonstrating the increasing importance of cybersecurity in modern warfare<sup>19</sup>. Mitigating or eliminating cyber-terrorism in both this war and the larger global situation in the 21st century will take an international, "all hands on deck" approach, utilizing the technological resources and assets from targeted countries and their allies.

The SWC continues to monitor and report on the activities of cyber terrorists and the threats they pose to Israel and Jewish communities and institutions.

---

<sup>12</sup><https://www.washingtonpost.com/world/2023/10/17/israel-hamas-war-reason-explained-gaza/>  
<https://www.politico.com/news/2023/10/10/israel-hamas-technology-failure-00120667>

<sup>13</sup><https://www.politico.com/news/2023/10/15/hackers-israel-hamas-war-00121593>  
<https://www.politico.com/news/2023/10/10/israel-hamas-technology-failure-00120667>

<sup>14</sup><https://cloudsecurityalliance.org/blog/2022/09/26/the-ongoing-cyber-threat-to-critical-infrastructure/>

<sup>15</sup><https://www.securityweek.com/cyberterrorist-attacks-unsophisticated-effective-former-fbi-agent/>

<sup>16</sup><https://academic.oup.com/cybersecurity/article/3/1/49/2999135>

<sup>17</sup>Ibid.

<sup>18</sup><https://homeland.house.gov/wp-content/uploads/2023/11/2023-11-15-HRG-Testimony.pdf>

<sup>19</sup><https://www.politico.com/news/2023/10/15/hackers-israel-hamas-war-00121593>