Yet Another Diminishing Spark: Low-level Cyberattacks in the Israel-Gaza Conflict

Anh V. Vu
University of Cambridge
Cambridge Cybercrime Centre
anh.vu@cl.cam.ac.uk

Alice Hutchings
University of Cambridge
Cambridge Cybercrime Centre
alice.hutchings@cl.cam.ac.uk

Ross Anderson
University of Cambridge
and University of Edinburgh
ross.anderson@cl.cam.ac.uk

***Abstract*—We report empirical evidence of web defacement and DDoS attacks carried out by low-level cybercrime actors in the Israel-Gaza conflict. Our quantitative measurements indicate an immediate increase in such cyberattacks following the Hamas-led assault and the subsequent declaration of war. However, the surges waned quickly after a few weeks, with patterns resembling those observed in the aftermath of the Russian invasion of Ukraine. The scale of attacks and discussions within the hacking community this time was both significantly lower than those during the early days of the Russia-Ukraine war, and attacks have been prominently one-sided: many pro-Palestinian supporters have targeted Israel, while attacks on Palestine have been much less significant. Beyond targeting these two, attackers also defaced sites of other countries to express their war support. Their broader opinions are also largely disparate, with far more support for Palestine and many objections expressed toward Israel.**

1. Introduction

Cyber operations have been used in armed conflicts as part of 'hybrid' warfare [1], involving both high and low-level actors who have contributed to a digital confrontation in various ways. Since the Hamas attack on 7 October 2023 and the declaration of war, Israeli and Palestinian digital assets have been targeted, including distributed denial-of-service (DDoS) and website defacement attacks. For example, after the Jerusalem Post suffered a DDoS attack, geo-fencing measures were implemented to restrict access to users within Israel [2]. Media outlets in Israel and the Palestinian territories have also been targeted [3], with hundreds of journalists and media workers (unintentionally) killed [4]. This ongoing war introduces an opportunity to analyse cyberattack patterns and assess how they differ from other conflicts such as the invasion of Ukraine in 2022, given that both are major wars rooted in national aspirations but with different political contexts.

While nation-state attacks are widely highlighted in the news, the role of low-level cybercrime actors and volunteer hacktivists appears to have been under-reported. Our prior work [5] analysed 'nationalistic' activities in the Russia-Ukraine war that began in February 2022, revealing swift responses with immediate but short-lived peaks of online discussions, website defacements, and DDoS attacks targeting both countries. We take a similar approach to analyse the non-governmental low-level cyberattacks in the Israel-Gaza conflict, focusing particularly on web defacement and UDP amplification DDoS attacks. These attacks can be carried out by individuals who generally lack advanced technical skills but repurpose off-the-shelf tools and services. Despite their simplicity, these vectors are attractive during wartime as they can be executed at scale and may cause immediately noticeable effects by making digital infrastructure inaccessible or by 'painting' sites with unwanted messages and political propaganda.

Ethics and Data Availability. We received approval from our institutional ethics committee for data collection and analysis. We only scrape public content and refrain from gathering private data or data that requires authorisation. Our scraper maintains a reasonable pace to avoid burdening websites with unnecessary traffic [6]. All analyses are conducted collectively without disclosing individual information to prevent potential harm, aligning with the British Society of Criminology's Statement on Ethics [7]. All datasets and scripts are available through a data-sharing agreement with the Cambridge Cybercrime Centre.[1]

2. Cyber Operations in Armed Conflicts

Similar to Russia and Ukraine, Israel and Palestine have a long-standing antagonistic relationship dating back many years, with Israel possessing high defensive and offensive capabilities. Cyber operations by both state and non-state groups have been reported following the Hamas strike, including destructive attacks such as phishing emails used to deliver data wipers to Israeli organisations [8], DDoS attacks targeting Israeli websites that provide information to civilians [9], as well as ransomware and website defacements aimed at disrupting infrastructure and spreading political propaganda [10]. Iran has conducted hack-and-leak operations and phishing campaigns against Israeli and US entities, while Iranian infrastructure has also been targeted, with disruptions attributed to actors claiming to be retaliating for the conflict [11]. Resembling the IT Army of Ukraine, the IT Army of Palestine was formed in an ad-hoc manner to attract volunteer hacktivists to attack Israeli infrastructure. Though not publicly announced, the group primarily coordinates its activities and advertises its targets through a Telegram channel. However, its scale, operational capacity, and media coverage remain significantly more limited than those of the IT Army of Ukraine.

Iran has also engaged in cyber and influence operations targeting Israel, employing online propaganda and

1. Our legal framework: https://cambridgecybercrime.uk/data.html

disruptive attacks in support of Hamas [12]. Israeli digital billboards were defaced to display Palestinian flags, fabricated war-related news, and political messaging [13] as part of a broader disinformation campaign [14]. The pro-Palestinian hacktivist group AnonGhost developed a malicious mobile app that mimicked a legitimate app used by Israeli citizens to receive real-time alerts about incoming airstrikes. This counterfeit application not only misled users with many false warnings but also covertly harvested sensitive personal information and activity logs [15].

The US has been actively cooperating with Israel on cyber initiatives [16]. Although Israel possesses strong cyber warfare capabilities, reports of cyberattacks on Palestinian targets have been limited, largely due to the region's minimal reliance on internet infrastructure. Shortly after the conflict started, Cloudflare observed that over half of all traffic to Palestinian websites were part of HTTP DDoS attacks [9]. Israel enforced a near-total telecommunications blackout for some time (some lasting an entire week), cutting off internet and telephone connections, which severely impacted critical services including medical operations [17]. A few days after the Hamas attack, internet accessibility in the Gaza Strip dropped to just 15% of pre-war levels [18]. Some pro-Israeli hacktivists have launched cyberattacks, allegedly disrupting Tehran's electrical grid and taking down the Gaza Now news site [19].

A comprehensive account of this conflict has been documented [20]. Some commentators have suggested that this 'cyberwar' has not caused significant harm compared to the physical battlefield, where human lives are at stake. Instead, cyber operations have primarily served as tools for espionage and political propaganda [21]. This conflict once again highlights the role of information operations in modern 'hybrid' warfare, where digital tactics complement traditional military actions. It offers an opportunity to analyse attack patterns and compare them to those seen in the Russia-Ukraine conflict, as both are major wars driven by national aspirations but set in different political contexts. While some industry reports have examined the attack landscape [9], [11], [12], academic studies on the role of low-level cybercrime actors in this ongoing conflict – both quantitative and qualitative – remain rather limited.

3. Methods and Datasets

We analyse the changing landscape of low-level cybercrime activities using quantitative datasets of both cyberattacks and online discussions, spanning from 1 August 2023 to 31 January 2024 – two months before and four months after the war commenced. As in our prior work [5], the most substantial changes occurred within six months, making this timeframe sufficient to draw the key narratives. All timestamps are normalised to UTC+0.

3.1. Datasets

We particularly focus on DDoS and website defacement attacks – two simple and measurable types of cyberattacks that can be launched by low-level cybercrime actors using existing tools and services. These attacks can be executed at scale and may cause immediately visible results during wartime, such as making websites inaccessible or taunting opponents with unwanted political propaganda.

Web Defacements. We analyse 105 432 web defacements within the period, as part of over 350k records shared by the Cambridge Cybercrime Centre [5] in a collection of the five most popular archives that defacers use to self-report attacks: ZONE-H, OWNZYOU, ZONE-XSEC, HAXOR-ID, and DEFACER-PRO. This dataset is self-reported (some actual defacements may be missing); however, combining the most prominent defacement archives provides a reasonably indicative picture. Its reliability and completeness have been comprehensively verified with semi-automatic validation, de-duplication and correction, while victims are identified based on country-code top-level domains (ccTLDs), IP geolocation, and the geolocation of their hosting Autonomous Systems (AS), excluding CDNs [5].

UDP Amplification DDoS Attacks. We use a DDoS attacks dataset gathered from a honeypot network of several dozen sensors set up worldwide since 2014 [22]. This honeypot simulates UDP protocols susceptible to reflective attacks, capturing packets sent by malicious actors but avoid redirecting the magnified traffic to the intended victims. An attack is defined as a flow of at least five packets to a victim, with the victim's country determined by IP and AS geolocation, excluding popular CDNs [5]. With UDP amplification, there is no source information. This dataset covers DDoS attacks caused by many low-level cybercrime actors, particularly booter users, but does not cover TCP-based and direct-path attacks. It has been used to measure booter activity following law enforcement takedown campaigns in 2018 [23] and 2022–2023 [24].

Underground Forum Posts. We analyse war-related discussions on one of the largest hacking forums, HACK FORUMS, as part of the CRIMEBB dataset [25]. This forum facilitates cybercrime discussion and trades among low-level actors, some of whom have faced criminal charges [26]. There are 80 threads containing at least one post having (case-insensitive) terms 'Israel', 'Palestine', 'Hamas', and 'Gaza' over the period: 67 related to Israel, 33 related to Palestine, 23 related to both countries, and three related to 'Hamas' or 'Gaza'. We subsequently extracted 742 posts from 16 highly relevant threads (with titles directly containing the keywords) and 173 posts having the keywords from the remaining 64 less relevant threads, compiling a total of 915 relevant posts made by 187 active users.

Telegram Chats. One week after the Hamas strike, the Cyber Army of Palestine was established to support the 'digital frontline', mirroring the IT Army of Ukraine [5]. The most tangible outcome is two public Telegram channels, starting on 14 October 2023, to recruit volunteer hacktivists and coordinate attacks against Israeli digital assets. The primary channel is used solely by the admins to spread propaganda while offering training and attack tools, attracting over 13 000 subscribers (10–15 times less than the IT Army of Ukraine). The secondary channel is used by over 1 000 participants for social discussions, with announcements forwarded from the primary channel. Successful attacks are frequently showcased in both channels, with victims and domain names often promoted in Arabic; most are Israeli, but sometimes extend to Arab 'friends' such as Egypt. Using Telethon and official Telegram APIs, we collect both channels, with 189 admin announcements and 26k messages of over 3 000 users. Regular expressions are used to extract all targeted domains from the chats.

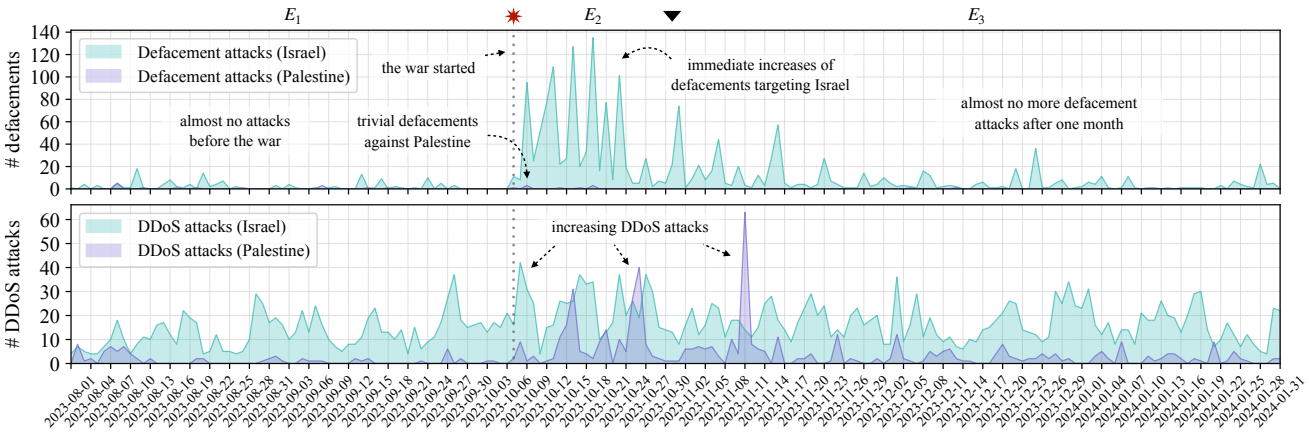

Figure 1: Number of self-reported defacements (top) and DDoS attacks (bottom) on Israel and Palestine over the period. Some attack levels escalated shortly after the war began but then rapidly dropped. The red star marks the Hamas strike.

Table 1: The significance of the impact on the number of daily defacements and DDoS attacks on Israel and Palestine.

Country and type of attacks	Statistical tests for the number of attacks per day				
	Kruskal-Wallis report	$\langle E_1, E_2 \rangle$	$\langle E_1, E_3 \rangle$	$\langle E_2, E_3 \rangle$	η^2
Israel (web defacements)	$H(2) = 62.33, p < .0001$	$p < .0001$	$p < .0001$	$p < .0001$	0.33
Palestine (web defacements)	$H(2) = 10.50, p < .01$	$p = .2007$	$p < .05$	$p < .01$	0.05
Israel (DDoS attacks)	$H(2) = 24.48, p < .0001$	$p < .0001$	$p < .01$	$p < .01$	0.12
Palestine (DDoS attacks)	$H(2) = 32.91, p < .0001$	$p < .0001$	$p < .001$	$p < .01$	0.17

3.2. Statistical Tests

Similar to our prior work [5], we test the significance of the impact resulting in different levels of attack counts and discussions by separating the period into three eras; E_1: before the Hamas strike, E_2: around one immediate following month from 7 October to 31 October 2024, and E_3: from 1 November 2023 to 31 January 2024. We then apply the unpaired non-parametric Kruskal-Wallis test (as the data distribution is not normal), with the null hypothesis that there is no significant difference between the three eras. If a difference is found, Dunn's post-hoc test is used to identify the pairs causing changes. Effect sizes are measured by η^2, ranging [0, 1]; $0 \leq \eta^2 < 0.01$: no effect; $0.01 \leq \eta^2 < 0.06$: small effect; $0.06 \leq \eta^2 < 0.14$: medium effect; and $0.14 \leq \eta^2 \leq 1$: large effect [27].

4. The Evidence of Cyberattacks

This section outlines the evolving landscape of defacement and DDoS attacks targeting both sides. Figure 1 presents the number of attacks per day over the period, while Table 1 details the statistical (in)significance of the effect.

4.1. Website Defacement Attacks

There is evidence of defacement attacks on Israeli websites. While Palestine suffered only 25 attacks by 18 defacers, we see 1 791 attacks on Israel by 439 defacers. There were almost no web defacements targeting Israel in the preceding weeks, with attacks beginning just a few hours after the Hamas attack then escalated quickly (see Figure 2). A small spike occurred on 7 October; the next big one was two days later, following Israel's declaration of war, with around 100 attacks (69 at 10 PM); the peak of nearly 140 attacks was on 19 October. Kruskal-Wallis test indicates a statistically significant effect on the number of daily defacements against Israel pre-war versus post-war, with a large effect size (0.33), suggesting that the conflict is highly associated with the outbreak of attacks on Israel. There is no difference in defacement on Palestine between E_1 and E_2, primarily due to the small sample size.

These outbreaks exhibit some similarities to the cyber-attack patterns observed during the Russia-Ukraine conflict, as documented in prior work [5], see Figure 3. The surges in attacks occurred quickly, while the defacer peaks lagged by a few days, presumably as more defacers joined in. Participation then dropped steadily, with only around five attackers still active after three weeks – following the pattern in the Russia-Ukraine conflict. Offensive activity against Israel (both attacks and attackers) was significantly less than that against Russia but more than that against Ukraine. While attacks targeted both sides in the Russia-Ukraine conflict, the Israel-Gaza war has been mostly one-sided, with no substantial attacks against Palestine so far.

Defacement Motives. Defacers are highly centralised: the 10 most active accounted for 55.67% of attacks; with one contributing 16.46%. This aligns with 'offender concentration' – a well-established criminological regularity; for example, just 1% of repeat offenders were responsible for 57.8% of repeat defacements [28], and a small number of forum members are involved in the majority of contractual transactions on a cybercrime market [29]. We analyse messages left on defaced pages, considering a political sentiment to be supporting one side if a support/objection is expressed. Signatures without a clear war-related statement are considered self-aggrandisement, and are marked

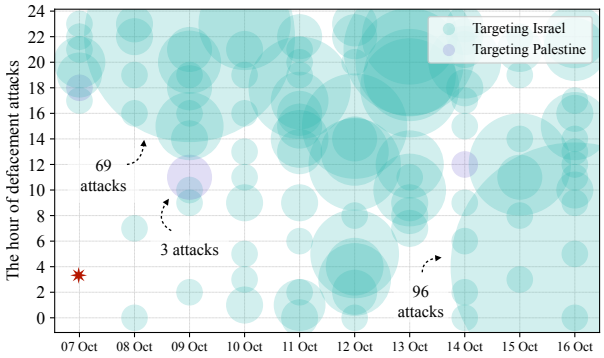

Figure 2: The number of website defacement attacks targeting Israel and Palestine, broken down hour by hour. The red star marks the Hamas attack on 7 October 2023.

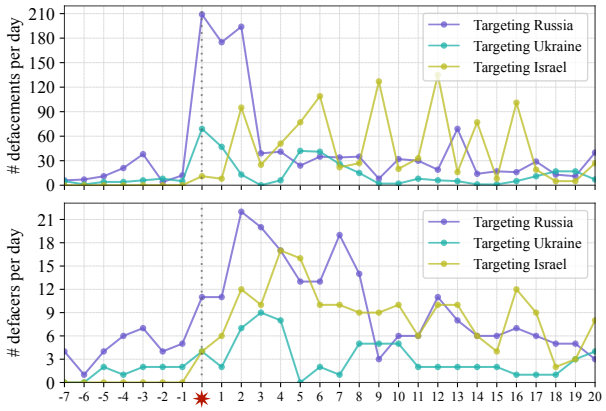

Figure 3: Defacements (top) and defacers (bottom) targeting Israel around 7 October 2023, in comparison with those seen with Russia and Ukraine in February 2022 [5].

as financially motivated if there are adverts for hacking services e.g., '*contact for shells*'. Among 1 816 defacements on Israel and Palestine, 221 are self-aggrandisement (12.17%). Only one supports Israel, but 559 defaced Israeli sites in support of Palestine (30.78%) with hashtags #opisrael, #savegaza, #freepalestine, and #savepalestine. That proportion is much higher than what was seen in the Russia-Ukraine conflict, where only around 7% of attacks explicitly expressed support for either side [5]. We see two are financially motivated, and three expressing warlike sentiment but without a clear supporting side. Beyond defacing Israeli and Palestinian sites, defacers also targeted sites of other countries to express their support or objection to the war. The majority of messages left on the defaced pages similarly show strong support for Palestine, suggesting that the wider opinion is also largely one-sided.

Choice of Targets. There is little evidence of successful defacements against high-profile targets; most victims are corporate, with 1 384 attacks (76.21%) against businesses under .co.il, 61 attacks (3.36%) targeting organisations under .org.il, and 16 attacks (0.88%) targeting educational websites. The few notable compromised targets include an Israeli housing association, partly exploited on 13 October 2023, a subdomain of the Israel Defense Forces under .idf.il, and 16 subdomains of the largest public college in Israel. Regarding Palestinian targets, we see only 25 .ps reported victims. The rest are under generic ccTLDs: .com (262), .net (22), .org (11), .biz (4), .club (3), .art (1), and 22 unidentifiable IP addresses. As in the Ukraine war, most defacements are strategically unimportant, as defacers usually employ off-the-shelf tools and scan pre-defined ccTLDs to find vulnerable targets for mass defacements.

4.2. UDP Amplification DDoS Attacks

The war appears to be closely linked to a gradual surge in DDoS attacks targeting Palestine, which was almost zero prior to 7 October 2023. The attack counts gradually rose to about 30–40 per day, peaking at over 60 on 11 November 2023. This increase was short-lived, subsiding significantly after one month. There was a slight uptick of 40 attacks targeting Israel per day on 8 October 2023 (one day after the war commenced), however its correlation with the conflict was visually unclear as there have been consistent attacks against Israel for the previous two months. Kruskal-Wallis test confirms a statistically significant effect on the number of daily DDoS attacks against Israel and Palestine pre-war versus post-war, with medium and large effect sizes (0.12 and 0.17), suggesting that the conflict is likely associated with these increases.

DDoS attacks targeting Israel seem more enduring than those against Palestine. During the period, the total attacks on Israel captured by the honeypot – which covers UDP-based but not TCP-based and direct-path attacks – was five times higher to those hitting Palestine (over 3 000 vs 600). These volumes, however, have been an order of magnitude less (15–20 times) compared to the scale observed in the Russia-Ukraine conflict, where around 600 attacks per day were recorded using the same dataset [5].

5. The Hacking Community Reactions

Discussions on HACK FORUMS. There was an immediate increase in posts related to the conflict on HACK FORUMS from near zero to around 270 per day as the war escalated (see Figure 4). This surge peaked at a higher level but tailed off much faster than those previously seen in the Russia-Ukraine conflict (which peaked at around 140 but lasted for a few weeks [5]), indicating a more short-lived effect. Kruskal-Wallis tests confirm the significance $H(2) = 80.32, p < .0001$, with a very large effect size $\eta^2 = 0.43$. Pairwise post-hoc tests for $\langle E_1, E_2 \rangle$ and $\langle E_2, E_3 \rangle$ are highly significant ($p < .0001$), so is $\langle E_1, E_3 \rangle$ ($p < .001$). This suggests genuine effects on the hacking community discussions associated with the conflict, with notable shifts particularly from E_1 to E_2 and E_2 to E_3.

The number of posting users shows a similar pattern, peaking two days after the Hamas strike. Kruskal-Wallis test reports $H(2) = 78.07, p < .0001$ with a large effect size $\eta^2 = 0.42$. Pairwise post-hoc tests for $\langle E_1, E_2 \rangle$ and $\langle E_2, E_3 \rangle$ are highly significant ($p < .0001$), so is $\langle E_1, E_3 \rangle$ ($p < .001$). This evidence again suggests significant changes correlated with the war; both the number of posts and users increased sharply, but lagged two days after the Hamas strike – similar to the defacement activity.

This increased activity is notable as the overall HACK FORUMS activity remained stable at this time. However, this rise is trivial compared to the HACK FORUMS size of around 10k posts per day. We did not see forum users

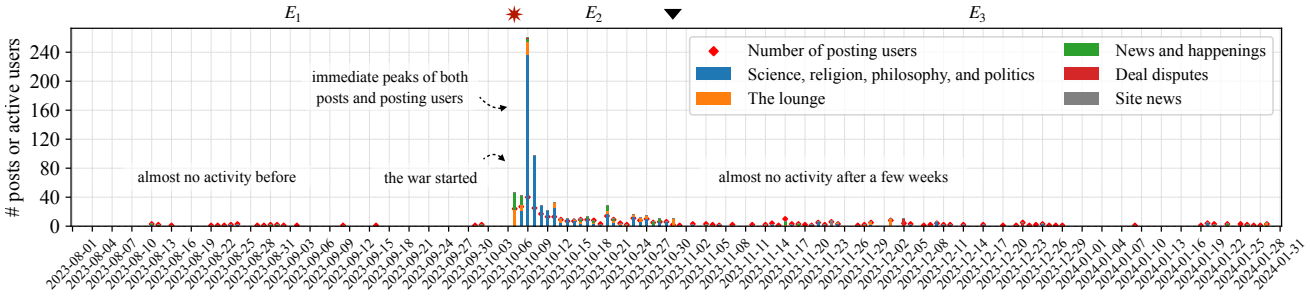

Figure 4: Daily posts and posting users on HACK FORUMS mentioning Israel and/or Palestine (top five subforums).

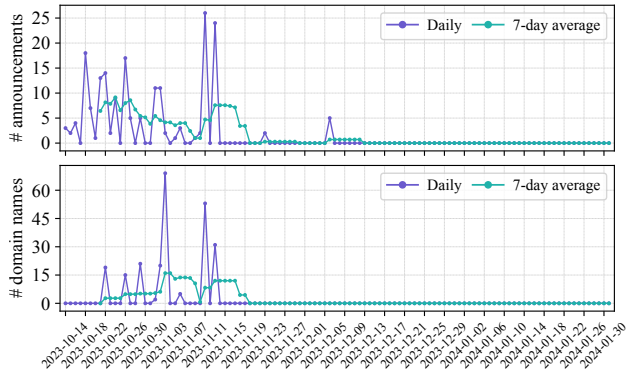

Figure 5: Number of daily announcements and domain names targeted by the Cyber Army of Palestine group.

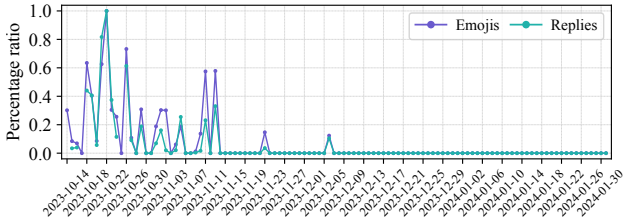

Figure 6: The user engagement (daily) in the Cyber Army of Palestine channel. Values are min–max normalised.

discussing ways to attack either country. Posts are highly centralised: 96.39% belong to the top five popular subforums. The biggest subforum, *'science, religion, philosophy, and politics'*, accounts for 68.63%, and the second biggest, *'the lounge'*, accounts for 12.90%. The primary discussion on 7 October was general chats and *'news and happenings'*, but shifted to *'science, religion, philosophy, and politics'* in the following days, while other boards exhibited trivial activity. Interest then declined, dwindling to around 10 posts per day after a week and almost zero after two weeks, suggesting that while users were highly active on 9 October 2023, their engagement waned over time and returned to the previous levels, presumably as they lost interest. This short-lived nature is in line with evidence seen from web defacement and DDoS attacks.

The Cyber Army of Palestine. There was a high level of activity in the first month following the channel's inception, peaking at around 25 announcements per day but rapidly dwindling to near zero in subsequent periods (see Figure 5). All promoted targets were domains with no associated IP addresses – unlike the IT Army of Ukraine channel, where our prior work found domains are often associated with IP addresses [5]. Targets were not posted until the second week, peaking at 70 on 3 November 2023. However, as the number of announcements tailed off, the promoted targets also dwindled. The decline in activity extended beyond just the operators; subscribers also exhibited diminishing engagement over time (see Figure 6). While they actively engaged with announcements during the first month, the number of reactions declined rapidly following the absence of new announcements. We believe the patterns indicate a clear loss of interest from both operators and subscribers. This decline was even more rapid than the declining interest observed with the IT Army of Ukraine [5], which sustained a prolonged tail of announcements and promoted targets in the two months following the invasion. We do not perform statistical tests on the Telegram chat data, as this channel was established after the conflict, and thus pre-war records are unavailable.

6. Concluding Remarks

The role of low-level cybercrime actors in the Israel-Gaza conflict appears to have resembled the timely but short-lived activity in the Russia invasion of Ukraine [5]. These actors were quickly influenced by the war and changed their behaviour, but their interest waned after a few weeks, with both attack levels and war-related discussions gradually dropping. While armed conflicts may be rooted in different ideologies and political contexts, the observed behaviours may also hold in other analogous situations.

Both types of attacks this time were at a much lower intensity than those in the Russia-Ukraine conflict, presumably as Russia and Ukraine have a far longer history of information operations, with substantial offensive capacities [30], and are among the most active cybercrime hubs globally [31]. Another contrast is that cyberattacks this time were predominantly one-sided: we see many more defacement and DDoS attacks on Israeli than on Palestinian targets, similar to the industry's view on application-layer DDoS attacks [9]. One significant caveat for this disparity may be the relatively low level and criticality of Internet infrastructure in Palestine, which has far fewer sites than Israel, many of which are hosted on overseas cloud services. The defensive capability, attack surface, and resources are also largely unequal between the two.

There may also be a difference in how people react to the conflict, with multiple reports of rising antisemitic and Islamophobic content online. There is a highly skewed picture of online social media supporting the two sides, with many pro-Palestinian messages spread compared to

pro-Israeli content. For instance, hashtags such as #StandWithPalestine and #PrayforPalestine attracted billions of views, while #StandWithIsrael and #PrayforIsrael generated just a few hundred million on TikTok [32]. Although this disparity may be partly influenced by complex content recommendation systems, the same picture is also observed in cyberattacks, messages left on defaced websites targeting Israel and Palestine, and also in the broader expressions in defacement attacks targeting other countries.

Our future work will incorporate more recent events. For example, on 1 April 2024, Israel conducted airstrikes on Iranian targets in Syria, killing the highest-ranking Iranian military official. The period from 15 January 2025 to 18 March 2025 (marked by ceasefires) and the surprise attack on the Gaza Strip on 18 March 2025 (ended the ceasefires), will also be measured. Comparisons with other conflicts, such as the long-standing China-Taiwan dispute and those in the Middle East, which present unique sociopolitical complexities, could offer broader insights into the interplay between conflict, cybercrime, and extremism.

Acknowledgments

We thank Richard Clayton and our colleagues at the Cambridge Cybercrime Centre for their useful feedback. All reviews for this paper are available at https://github.com/wacco-workshop/WACCO/tree/main/WACCO-2025. This study is supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 949127).

References

[1] Frank G. Hoffman. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies, 2007. https://rb.gy/2u7fpo.

[2] The Jerusalem Post. Hackers Hit United Hatzalah, Aid Group Treating Wounded Israelis. https://rb.gy/dtl7w1, 2023.

[3] Oxford Analytica. Cyberattacks on the Middle East Will Continue to Rise. *Emerald Expert Briefings*, 2024. DOI:10.1108/OXAN-DB291422.

[4] Committee to Protect Journalists. Journalist Casualties in the Israel-Gaza War. https://rb.gy/hjzftg, 2025.

[5] Anh V. Vu, Daniel R. Thomas, Ben Collier, Alice Hutchings, Richard Clayton, and Ross Anderson. Getting Bored of Cyberwar: Exploring the Role of Low-Level Cybercrime Actors in the Russia-Ukraine Conflict. In *Proceedings of the ACM World Wide Web Conference (WWW)*, 2024. DOI:10.1145/3589334.3645401.

[6] Lydia Wilson, Anh V. Vu, Ildiko Pete, and Yi Ting Chua. Identifying and Collecting Public Domain Data for Tracking Cybercrime and Online Extremism. In *Open-Source Verification in the Age of Google*. World Scientific, 2024. DOI:10.1142/9781800614079_0015.

[7] British Society of Criminology. Statement of Ethics. https://rb.gy/ldwfkl, 2015.

[8] Bleeping Computer. ESET Partner Breached to Send Data Wipers to Israeli Orgs. https://rb.gy/0zj5zz, 2024.

[9] Cloudflare. Cyber Attacks in the Israel-Hamas War. https://rb.gy/czdpjh, 2023.

[10] The Record. Attacks on Israeli Orgs 'More Than Doubled' Since October 7. https://rb.gy/wwmwg2, 2024.

[11] Google. Tool of First Resort: Israel-Hamas War in Cyber. https://rb.gy/45b4yz, 2024.

[12] Microsoft. Iran Surges Cyber-Enabled Influence Operations in Support of Hamas. https://rb.gy/ion04y, 2024.

[13] Business Insider. Hackers Infiltrated Israeli Smart Billboards to Post Pro-Hamas Messages. https://rb.gy/dtfyhd, 2023.

[14] Reuters. Disinformation Surge Threatens to Fuel Israel-Hamas Conflict. https://rb.gy/oinh39, 2023.

[15] Cloudflare. Malicious "RedAlert - Rocket Alerts" Application Targets Israeli Phone Calls, SMS, and User Information. https://rb.gy/tu8m25, 2023.

[16] Nextgov/FCW. US Cyber Agencies in 'Very Close Contact' With Israel After Unprecedented Hamas Attacks. https://rb.gy/xk22yn, 2023.

[17] CNN News. Gaza Communications Blackout, the Longest of the War, Hits One-Week Mark. https://rb.gy/2axuic, 2024.

[18] Internet Outage Detection & Analysis (IODA). Internet Connectivity for Gaza Strip. https://rb.gy/x1un70, 2023.

[19] Israel National News. 'Don't Play With Fire': Israeli Hackers Claim to Have Disabled Tehran Electrical Grid. https://rb.gy/ucgprr, 2023.

[20] Péter Selján. The 7 October Hamas Attack: A Preliminary Assessment of the Israeli Intelligence, Military and Policy Failures. *Academic and Applied Research in Military and Public Management Science*, 2024. DOI:10.32565/AARMS.2024.1.5.

[21] The Conversation. A Look Inside the Cyberwar Between Israel and Hamas Reveals the Civilian Toll. https://rb.gy/wxzdwv, 2024.

[22] Daniel R. Thomas, Richard Clayton, and Alastair R. Beresford. 1000 Days of UDP Amplification DDoS Attacks. In *Proceedings of the APWG Symposium on Electronic Crime Research (eCrime)*, 2017. DOI:10.1109/ECRIME.2017.7945057.

[23] Ben Collier, Daniel R. Thomas, Richard Clayton, and Alice Hutchings. Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks. In *Proceedings of the ACM Internet Measurement Conference (IMC)*, 2019. DOI:10.1145/3355369.3355592.

[24] Anh V. Vu, Ben Collier, Daniel R. Thomas, John Kristoff, Richard Clayton, and Alice Hutchings. Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services. In *Proceedings of the USENIX Security Symposium (USENIX Security)*, 2025. https://rb.gy/4nkvvv.

[25] Sergio Pastrana, Daniel R. Thomas, Alice Hutchings, and Richard Clayton. CrimeBB: Enabling Cybercrime Research on Underground Forums at Scale. In *Proceedings of the ACM World Wide Web Conference (WWW)*, 2018. DOI:10.1145/3178876.3186178.

[26] Sergio Pastrana, Alice Hutchings, Andrew Caines, and Paula Buttery. Characterizing Eve: Analysing Cybercrime Actors in a Large Underground Forum. In *Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*, 2018. DOI:10.1007/978-3-030-00470-5_10.

[27] Jeremy Miles and Mark Shevlin. *Applying Regression and Correlation: A Guide for Students and Researchers*. Sage, 2000. https://rb.gy/1hi361.

[28] Asier Moneva, E. Rutger Leukfeldt, Steve G.A. Van De Weijer, and Fernando Miró-Llinares. Repeat Victimization by Website Defacement: An Empirical Test of Premises From an Environmental Criminology Perspective. *Computers in Human Behavior*, 2022. DOI:10.1016/J.CHB.2021.106984.

[29] Anh V. Vu, Jack Hughes, Ildiko Pete, Ben Collier, Yi Ting Chua, Ilia Shumailov, and Alice Hutchings. Turning Up the Dial: the Evolution of a Cybercrime Market Through Set-Up, Stable, and Covid-19 Eras. In *Proceedings of the ACM Internet Measurement Conference (IMC)*, 2020. DOI:10.1145/3419394.3423636.

[30] Margarita Jaitner. Russian Information Warfare: Lessons From Ukraine. In *Cyber War in Perspective: Russian Aggression against Ukraine*. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2015. https://rb.gy/ywkisg.

[31] Jonathan Lusthaus, Miranda Bruce, and Nigel Phair. Mapping the Geography of Cybercrime: A Review of Indices of Digital Offending by Country. In *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2020. DOI:10.1109/EuroSPW51379.2020.00066.

[32] Politico. Does Social Media Favor Palestine Over Israel? https://rb.gy/z0nwsu, 2023.