THREAT ANALYSIS

Recorded Future®

By Insikt Group®

December 11, 2025

Palestine Action: Operations and Global Network

Palestine Action's global network has very likely increased the scope and frequency of its operations following the group's 2025 designation as a terrorist organization in the United Kingdom.

The facilities of defense contractors, banks, insurance agencies, and logistics companies that provide services to Israel face heightened physical risks from Palestine Action's global network.

Palestine Action's global network uses common tactics, techniques, and procedures for sabotage, obstruction, and vandalism, aimed at causing economic disruption and damage to targeted entities.

Executive Summary

Palestine Action has almost certainly responded to its July 2025 designation as a terrorist organization in the United Kingdom (UK) by encouraging domestic violent extremists (DVEs) outside the UK with a nexus to the group to increase the scope and frequency of their operations, while abstaining from conducting or claiming attacks within the UK. Palestine Action's dual-track strategy, very likely intended to maintain pressure on the multinational companies they target while avoiding complications to their legal efforts to contest the UK designation in court, almost certainly poses persistent physical threats to private and public sector facilities in Western Europe, North America, and Australia.[1] Recent arrests of pro-Palestine Action protesters in the UK and events in the Israel-Hamas conflict have very likely prompted Palestine Action's global network to more frequently conduct militant direct actions on behalf of Palestine Action's interests.[2]

Palestine Action's global network consists of pro-Palestinian activist groups that share the UK branch's commitment to militant direct action and other core aspects of the group's operational profile — such as motivating ideologies, preferred targets, area(s) of operation, or tactics, techniques, and procedures (TTPs). The most popular TTPs within the network are almost certainly those that Palestine Action's UK branch has promoted or employed, including vandalizing the exterior of facilities with red paint or blunt instruments, obstructing facilities with "human chains" or large objects, and sabotaging valuable assets inside the perimeter of a facility. Defense contractors that provide services to Israel's government or military are almost certainly the primary target of the Palestine Action global network, although the network has also frequently targeted insurance agencies, banks and financial entities, and shipping companies.

[1] Insikt Group uses definitions of terrorism and violent extremism adapted from US Intelligence Community (IC) definitions, academic research, and open-source reporting.
[2] In this context, direct action refers to coordinated activities by an individual or group of individuals to achieve a political goal without the involvement of a higher authority or bureaucratic institution. Direct action covers a wide range of political activity and can take non-violent (such as protests, demonstrations, banner drops, boycotts, or strikes) or violent (such as attacks, sabotage, rioting, or insurrection) forms.

Key Findings

- Palestine Action's July 2025 terrorism designation in the UK very likely broadened the geographic scope of its operations and potential targets, as activist groups in its global network outside the UK almost certainly have greater freedom of maneuver.
- Since October 7, 2023, events in the Israel-Hamas conflict, especially expansions of Israeli military activity or reports of humanitarian crises in the Gaza Strip, have prefigured physical attacks with a nexus to Palestine Action.
- The facilities of Western European, North American, and Australian defense contractors, banks, insurance companies, international shipping and logistics service providers, and government agencies — particularly those with a perceived relationship to Israel — very likely face elevated physical risks from Palestine Action's global network.
- The most costly Palestine Action operations — some of which have caused several million dollars in damages to targeted organizations — very likely resulted from Palestine Action operatives breaching facilities' secure perimeters.
- In the short to medium term, Palestine Action militant direct action in the UK is very likely to maintain a lower operational tempo until the group either succeeds in its effort to rescind its terrorism designation or exhausts all legal avenues to do so.

Palestine Action: History and Terrorism Designation

Palestine Action was founded in the UK in July 2020 by Huda Ammori and Richard Loxton-Barnard, longtime UK-based activists in the pro-Palestinian and environmental movements, respectively. The almost certain core purpose of Palestine Action is to promote militant direct action by pro-Palestinian activists around the world, particularly those who aim to disrupt the operations of government agencies, defense contractors, and private companies that supply Israel or the Israel Defense Forces (IDF). Historically, the group's UK core has focused its efforts on targeting the Israeli multinational defense contractor Elbit Systems (Elbit), as well as its partners and subsidiaries. Like other domestic violent extremist (DVE) groups, Palestine Action and its individual global network groups very likely lack formal hierarchies, opting instead to function in the form of decentralized activist cells.

Palestine Action very likely distinguishes between elements of the organization that focus on non-violent direct actions — such as protests, demonstrations, and political activity — and the organization's covert cells dedicated to militant direct action. On August 2, 2023, the group announced the creation of "Palestine Action Underground," its label for the group's "covert missions," and stated that its future militant direct actions would target "any business found to be collaborating with Elbit via their research, technology, consultation, labour, components, or any other service."[3] A March 2025 unclassified intelligence assessment from the UK's Joint Terrorism Assessment Center (JTAC) reported that between July 2020 and March 2025, Palestine Action "conducted over 385 direct actions" in the UK, including both non-violent and militant direct actions. These actions have occurred throughout the UK, supporting JTAC's assessment that the group has cells throughout the country, but police in the UK have reported higher degrees of Palestine Action-related activity in Greater London, as well as "Staffordshire, Greater Manchester, Leicestershire, Metropolitan, Kent, and Avon and Somerset."

The frequency and scope of Palestine Action's operations in the UK almost certainly increased following the October 7, 2023, Hamas attack in Israel and the subsequent Israel-Hamas war in the Gaza Strip. **Figure 1** (below) shows references in the Recorded Future Intelligence Operations Platform to incidents of sabotage or vandalism in the UK involving Palestine Action between its 2020 founding and 2025 terrorism designation, annotated with significant events during the post-October 2023 Israel-Hamas conflict. In many instances, Palestine Action's operations followed major developments in this conflict, such as expansions of Israeli military activity in the Gaza Strip or elsewhere in the Middle East, reports of humanitarian crises in Gaza, or the deaths of senior Hamas, Palestinian Islamic Jihad (PIJ), or Hezbollah figures in targeted airstrikes.

[3] Source document held by Insikt Group.

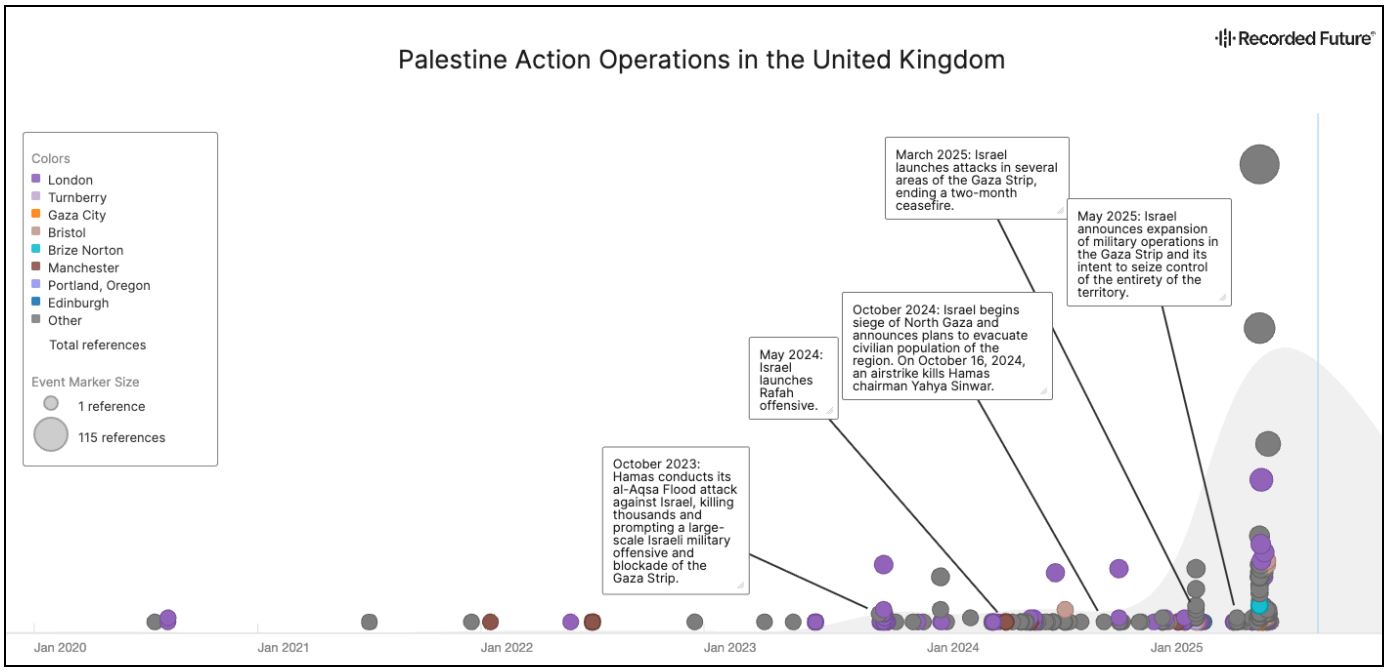

***Figure 1**: References to Palestine Action operations in the UK in the Recorded Future Intelligence Operations Platform alongside key developments in the Israel-Hamas conflict (Source: Recorded Future)*

The culmination of Palestine Action's direct action campaign in the UK was a June 20, 2025, operation in which several of the group's members illegally breached the Royal Air Force (RAF) Brize Norton base in Oxfordshire, sprayed paint into the engines of two RAF Airbus A330 Multi Role Tanker Transport (MRTT) aerial refueling aircraft, and damaged the jets with crowbars. In total, the attack caused over seven million pounds ($9.5 million) in damages and prompted calls for UK law enforcement agencies to crack down on Palestine Action. Three days after the attack, UK Home Secretary Yvette Cooper announced the Home Office's intent to proscribe Palestine Action under the UK's Terrorism Act 2000. The UK Parliament approved the proscription with votes on July 2 and 3, 2025, and Palestine Action was officially designated a terrorist organization in the UK on July 5; this status prohibits individuals from joining, fundraising, or expressing support for Palestine Action, with legal penalties as severe as fourteen years in prison for being convicted of being a Palestine Action member.

Palestine Action has almost certainly pursued a dual-track strategy in response to its designation in the UK, abstaining from major sabotage operations in the UK while inciting its global network to conduct these operations outside of the country. Insikt Group is not aware of significant incidents of sabotage connected to Palestine Action in the UK since its proscription. Instead, the group has attempted to legally challenge the ban and garner public support for its cause through a series of unlawful (due to Palestine Action's proscription) but well-attended protests in which several thousand demonstrators have been arrested for expressing support for Palestine Action.

However, the organization's international network outside the UK has almost certainly taken responsibility for Palestine Action's direct action campaigns, targeting defense contractors, militaries, and other industries perceived to be supporting Israel with sabotage, vandalism, and other disruptive

physical threat activities despite the UK terrorism designation. In August 2025, Palestine Action's official website deleted all of its content and posted a statement (**Figure 2**) claiming that "the website has been transferred to others in the global movement who are not active in Britain or British nationals." The website now provides two ways for individuals to contribute to the organization: through its Monero (XRP) cryptocurrency wallet or through the website of its Italian franchise, Palestine Action Italia (also known as Palestina Libera). On September 8, 2025, a Palestine Action Global social media account began posting and announced the launch of the "Palestine Action Global" platform, indicating the organization's belief that "Palestine Action is a global network taking direct action against the Israeli war machine."

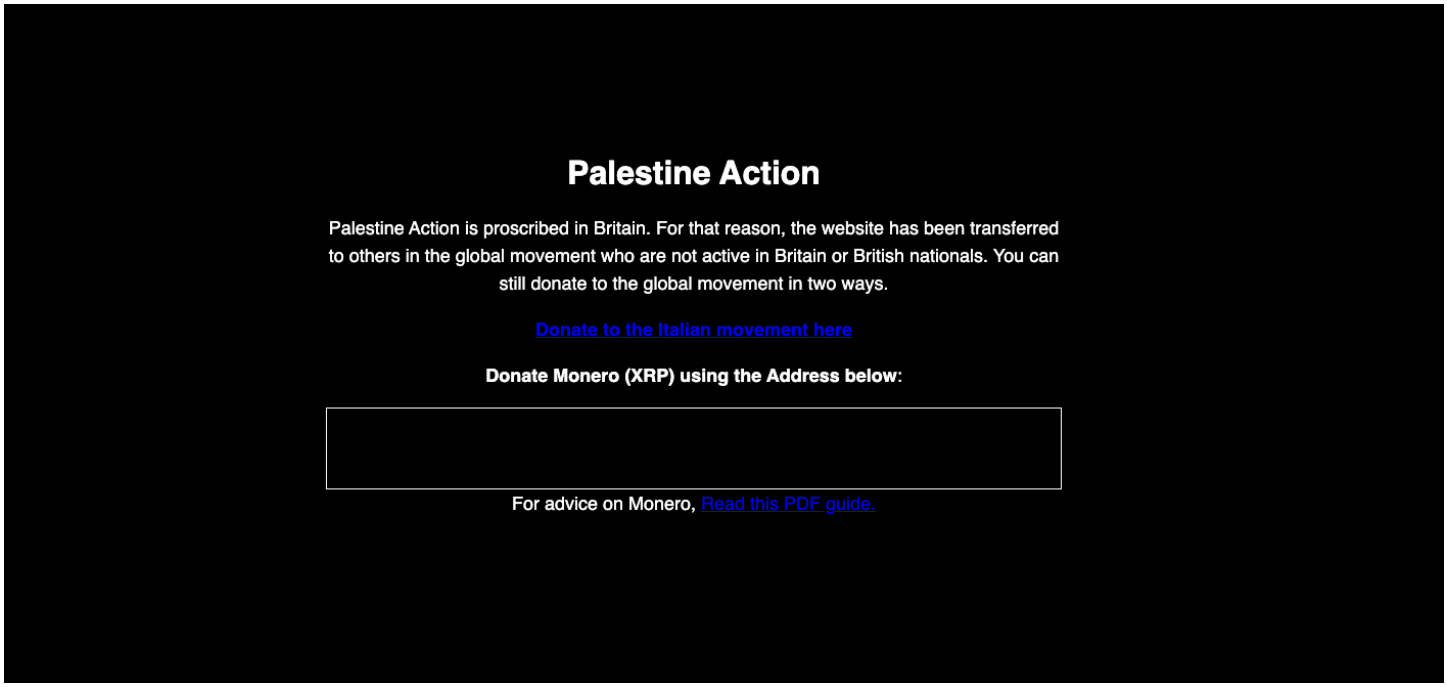

Figure 2: *Statement on Palestine Action website with cryptocurrency wallet information and link to Italian franchise (Source: Palestine Action)*[4]

Groups in Palestine Action's network in North America, Europe, and Australia — as detailed below — are very likely to increase their operational tempo in response to the UK proscription of Palestine Action and ongoing developments in the Israel-Hamas conflict. In the short term, the frequency of direct action conducted by groups in Palestine Action's global network is likely to outpace the parent organization in the UK, as it is likely to continue its *de facto* moratorium on sabotage and vandalism while it attempts to legally appeal its proscription. Nevertheless, Palestine Action will very likely attempt to continue providing support to its international network through organizing trainings for activists, sharing instructional material, and using its platform to advertise the activities of the network around the world.

[4] Image redacted to remove cryptocurrency wallet address.

Palestine Action's Tactics, Techniques, Procedures, and Targets

Palestine Action's UK branch and its global network almost certainly rely on standard operating procedures for conducting attacks against facilities to disrupt the business operations of their intended targets. Specifically, DVEs associated with the group almost certainly prefer TTPs for attacks that are described in Palestine Action's 2023 instructional guide to carrying out militant direct actions in support of the group's objectives.[5] Namely, Palestine Action and its global network have frequently and repeatedly used the same vandalism, physical obstruction, and sabotage TTPs in operations, as described in the following section. DVEs with a nexus to Palestine Action very likely select which TTP to employ in operations based on their level of access to the targeted facility in question, conducting more destructive and sophisticated attacks when they are able to gain interior access.

Across the globe, Palestine Action and similar groups' almost certainly primary targets are the offices of defense contractors that have perceived relationships with the IDF or the Israeli government. In the UK and Western Europe, Elbit and its subsidiaries and partners have been most frequently targeted in Palestine Action attacks. However, due to the global footprint of Palestine Action's network and the expansion of the Israel-Hamas conflict since October 2023, Palestine Action and similar groups have also attacked entities in other sectors that are perceived to be doing business with the IDF, the Israeli government, or Elbit. Aside from defense contractors and governments, the most frequently targeted industry sectors are insurance, banks and financing, logistics, and shipping.

Direct Action TTPs

Palestine Action almost certainly uses physical attack TTPs that are intended to maximize the degree of economic disruption and damage to targeted facilities, but minimize the risks of harm to individuals and detection by law enforcement. By imposing financial cost on targeted companies during operations, Palestine Action almost certainly seeks to convince the targeted entity to sever its relationships with the IDF or Israeli government. Insikt Group associates the following overarching TTPs with attacks perpetrated by Palestine Action or its global network:

- Palestine Action operations are typically carried out by small cells, mostly consisting of fewer than five activists.
- Palestine Action conducts targeted operations against facilities outside of business hours to maintain operational security and minimize the risks of harm to personnel or the identification/detection of its operatives.
- Palestine Action operations aim to impose substantial financial costs to targeted entities through rudimentary, low-sophistication methods.
- Palestine Action operatives prefer vandalism, obstruction, and sabotage as TTPs; which TTP is selected is very likely contingent on the degree of access to the facility.

[5] Source document held by Insikt Group.

- If operatives cannot gain entry to the facility, they will very likely prefer to vandalize the exterior of the facility or attempt to block external entry.
- If operatives are able to gain internal access to the facility — usually by identifying and exploiting potential access points during pre-attack reconnaissance or by using physical force to enter — they will very likely attempt to sabotage infrastructure inside the facility.

Vandalism

Almost all observed Palestine Action operations involve vandalism of the exterior of targeted facilities, with two types of actions especially prominent. First, DVEs affiliated with Palestine Action have frequently used red spray paint to either indiscriminately color or write messages on the facades of targeted facilities, or, by dispersing paint through a fire extinguisher, blanketing the exterior or interior of a facility with red paint. Second, these DVEs use tools or projectiles, including hammers, crowbars, blunt objects, and bricks, to destroy windows on the exterior of targeted buildings.

These vandalism methods are each attested to in Palestine Action's official instructional guide as effective ways to "destrupt [sic], damage or destroy your target."[6] The manual also recommends that DVEs use the same vandalism TTPs to damage exterior surveillance systems in order to avoid detection during direct actions, or to destroy infrastructure such as air conditioning systems or pipes outside the facility to "sabotage the profits of your target even further."[7]

***Figure 3**: Evidence of vandalism TTPs from a February 2025 Palestine Action attack against an Allianz insurance office in Milton Keynes, UK (Source: Palestine Action)*

[6] Source document held by Insikt Group.
[7] Source document held by Insikt Group.

Obstruction

Palestine Action operations have also used physical obstruction as a TTP to prevent access to targeted facilities. Unlike other attack TTPs associated with Palestine Action, the group has often used methods of obstructing facilities that are very unlikely intended to maintain the covert nature of the operation. Specifically, in some operations, Palestine Action cells have physically obstructed access to targeted facilities by forming a human blockade: sitting down, interlocking arms, blocking access to a main doorway, and on occasion chaining themselves together or to an immovable object (such as a vehicle or post). In a break from the patterns of other observed Palestine Action TTPs, activists have attempted blockades during normal business hours, mainly to prevent facility employees from entering the premises.

Figure 4: *Palestine Action activists blockade a Lockheed Martin facility in Bedfordshire, UK, in a November 2023 protest (Source: BBC)*

Palestine Action network groups — particularly in the United States (US) — have also experimented with more novel methods of facility obstruction that can be covertly conducted. Cells with a nexus to the US-based Palestine Action offshoot Unity of Fields (UoF), for instance, launched a campaign in the summer and fall of 2024 to target Citibank automated teller machine (ATM) locations in the New York and Los Angeles metropolitan areas due to the bank's perceived support of Israeli interests. In addition to vandalizing the facilities, the cells inserted epoxy and affixed cement-glue stickers to exterior

card-reader devices that were necessary to enter the facilities.[8] Palestine Action's instructional guide also calls for activists to use concrete to plug water or sewage pipes leading to targeted facilities, although Insikt Group has not observed Palestine Action operatives using this TTP.

Figure 5: *Activists insert epoxy into a Citibank card reader in New York City on October 7, 2024 (Source: Unity of Fields[9])*

Sabotage

Sabotage operations remain the most likely of the TTPs historically employed by Palestine Action to impose serious financial costs on the victims of its operations. While almost certainly relying on low-tech and low-sophistication methods, Palestine Action has caused millions of dollars in damages through sabotage operations, mainly to technology and other assets inside targeted facilities. In previous incidents, cells linked to Palestine Action have relied on the same toolkit used for vandalism and obstruction — large, blunt objects like crowbars and wrenches and fire extinguishers filled with paint — to sabotage their target. Activists almost certainly prefer these tools due to their low cost, ease of use, minimal profile, and the inability to trace their purchase; their use across the spectrum of Palestine Action's TTPs likely suggests that activists are opportunistic, employing the toolkit in sabotage operations as opposed to vandalism or obstruction when they can exploit vulnerabilities in facility security.

[8] Source document held by Insikt Group.
[9] Source document held by Insikt Group.

The most notable and recent sabotage incident connected to Palestine Action was the aforementioned breach of RAF Brize Norton, the largest RAF base in the UK, on June 20, 2025. A video of this attack posted by the group shows activists approaching Airbus A330s on the base using electric scooters. They damaged the aircraft by spraying red paint through a fire extinguisher directly into the plane's engines and striking the plane with crowbars. The attack caused approximately £7 million ($9.4 million) in damages to the aircraft, almost certainly due to the impact of the attack on sensitive parts and equipment inside the planes' engines. The attack on RAF Brize Norton led to the arrest and indictment of five Palestine Action-linked activists and almost certainly prompted the UK terrorism designation of the group, as well as improvements to facility and perimeter security at the RAF base.

Figure 6: *Palestine Action activists approach aircraft at RAF Brize Norton on electric scooters (Source: Palestine Action)*

Palestine Action activists also deployed sabotage TTPs on several additional operations targeting defense contractors in the UK. In August 2024, a Palestine Action cell in Bristol breached an Elbit warehouse by piloting a van through perimeter fencing, entered the facility, and began sabotaging internal equipment within the facility with sledgehammers, axes, and other blunt instruments. In total, the operation caused over £1 million ($1.3 million) in damages; protesters also allegedly assaulted a security guard and law enforcement officers responding to the incident, prompting JTAC to label the attack as an "act of terrorism." During a June 1, 2022, incident at a Thales Group facility in Glasgow, Palestine Action activists accessed the roof and entered the facility, destroying parts used for submarines with blunt instruments. In conjunction with the sabotage operation, two protesters glued themselves to the roof, likely attempting to obstruct access to the facility.

Targets

Palestine Action's primary target in the UK has almost certainly been Elbit: the global defense contractor has been the most frequent victim of its attacks, the group's propaganda and instructional material list Elbit as the group's preferred target, and Palestine Action has launched branded campaigns designed specifically to encourage activists to attack Elbit facilities. As secondary targets, the group has conducted notable attacks against other public and private sector defense entities perceived to have some association with the Israeli military, namely the UK's Ministry of Defence (MoD), Teledyne Technologies, Thales Group, Leonardo, and Rafael Advanced Defense Systems. According to its 2023 announcement and its post-October 7, 2023, activity, the group and its international network consider a range of entities in sectors that reportedly supply goods or services to Elbit or the Israeli military — including banks, financial institutions, insurance agencies, real estate brokers, accounting firms, human resources contractors, and international shipping and logistics companies — as legitimate targets for militant direct action. Direct actions have also targeted other UK government entities, including the UK Foreign and Commonwealth Office, the BBC, and the London Stock Exchange. Palestine Action almost certainly targets these companies with the goal of inflicting maximum financial and reputational damage through its operations, in order to convince companies to cease their business with Elbit or Israeli entities.

As the next section demonstrates, the international expansion of Palestine Action network groups adopting the UK branch's modus operandi or TTPs has almost certainly broadened the range of secondary and tertiary targets that are likely to be affected by militant direct action campaigns. However, Palestine Action and its global network very likely share a focus on specific sectors — defense contracting, banking, insurance, and international shipping and logistics — that relevant groups and cells are likely to target regardless of their respective area of operations. Moreover, the TTPs Insikt Group associates with Palestine Action's UK branch have almost certainly been adopted by its international counterparts, very likely due to the influence of Palestine Action's militant direct action campaigns in the UK, instructional material, and training sessions for activists.

Palestine Action's Global Network

Palestine Action's global network consists of groups of activists around the world who share Palestine Action UK's commitment to disrupting the normal business operations of entities partnered with the State of Israel through militant direct action. Some of these groups refer or have referred to themselves explicitly as "Palestine Action"; have direct relationships to the UK branch through their members, partners, or benefactors; choose identical targets, such as Elbit; or, like Palestine Action UK, are solely motivated by the anti-Israel cause. Others, despite lacking these relationships, have directly appropriated Palestine Action UK's TTPs, targets, or other aspects of the organization to support their own operations.

We classify groups in Palestine Action's global network based on which elements they share in common with the UK branch. As depicted in **Table 1**, our four-part classification labels Palestine Action network groups as either Palestine Action **franchises**, **affiliates**, **offshoots**, or **partners**, depending on whether they share areas of operation, motivating ideology, TTPs, or targets with the UK branch. These categories are not static and are subject to change over time, particularly as groups founded as Palestine Action franchises outside the UK adapt to the local landscape in their own countries and form their own brand. Table 1 additionally contains examples of each of the four categories of Palestine Action network groups, with the following subsections containing case studies of particularly notable franchise, affiliate, offshoot, and partner groups.

Label	Nexus	Distinction	Examples
Franchise	Ideology, TTPs, targets	Area of operation	Palestina Libera (Italy), Palestine Action Germany, Palestine Action Sweden, Palestine Action Eire (Ireland), Palestine Action Belgium, Palestine Action NL, Palestine Action Norway, Palestine Action Canada, Palestine Action Group Canberra (Australia), Palestine Action Tunisia
Affiliate	Ideology, TTPs	Area of operation, targets	Death to Toll (Australia)
Offshoot	Ideology, targets	Area of operation, TTPs	Unity of Fields (US), Shut Elbit Down (Germany/Austria)
Partner	Area of operation, TTPs	Ideology, targets	Shut the System (UK)

Table 1: *Classification of Palestine Action global network groups (Source: Insikt Group)*

Franchise: Palestine Action Italia/Palestina Libera (Italy)

Figure 7: *Palestine Action Italia logo (Source: Palestine Action Italia)*

Palestine Action Italia, more commonly known as Palestina Libera, is Palestine Action's Italy-based franchise. On its website, the group directly identifies itself as "the Italian branch of the international 'Palestine Action' campaign, which in England directly led to the closure of three arms factories involved in the genocide in Gaza." The group also uses similar branding as the UK branch, employs similar TTPs, and targets the same sectors, focusing largely on defense contractors with facilities in Italy. In particular, Palestina Libera's direct actions have frequently targeted the Italy-based defense contractor Leonardo at its offices throughout the country, due to its joint ventures with Elbit.

The organization very likely emerged from pro-Palestinian activist factions in Italy that increasingly aligned with Palestine Action's global network in the wake of the October 7, 2023, attack. While data in the Recorded Future Platform indicates the group's website was registered on February 4, 2024, a 2008 issue of al-Majdal Magazine — the quarterly publication of the BADIL Resource Center for Palestinian Residency & Refugee Rights — indicates that the same domain was operated by an Italian pro-Palestinian organization, the Comitato di Solidarietà con il Popolo Palestinese, Torino [Committee for Solidarity with the Palestinian People in Turin, Italy]. Screenshots of the domain captured in the Wayback Machine indicate that between October 2010 and the website's registration in February 2024, the site displayed a message indicating the administrator should "upload [their] website into the public_html directory." This message almost certainly indicates that an administrator account was active during the interim, but that it had not uploaded any information onto the domain. The group's active social media accounts were created in November and December 2023, respectively.

Following Palestine Action's July 5, 2025, designation as a terrorist organization in the UK, Palestine Action Italia has likely become one of the organization's most prioritized franchises. Palestine Action's main website currently includes a link to donate to Palestina Libera, hosted on Palestina Libera's website. This donation section uses the service provider Donorbox to facilitate transactions, with options for donors including sending €15 for "a little bit of paint," €50 for "smoke bombs in action," €100 for the "legal expenses fund," or another amount determined by the donor. Palestina Libera has also very likely increased its operational tempo in the wake of the proscription, citing Palestine Action UK's designation and the arrests of protesters at rallies in the UK as motivation for new direct actions. For instance:

- On October 3, 2025, Palestina Libera took part in pro-Palestine direct actions across Italy, protesting the Israeli government's interception of the Global Sumud Flotilla. Activists very likely affiliated with Palestina Libera participated in occupations and blockades of major transportation

and logistics infrastructure, including obstructing a runway at Pisa International Airport, occupying several highways in the Tuscany region, and blockading an Amazon Logistics facility in Brandizzo.
- On September 29, 2025, the group claimed to have blockaded a Leonardo facility in the town of Nerviano. In a social media post, it alleged that at least one Leonardo employee working at the facility joined its protest.
- On September 25, 2025, several of the group's activists chained themselves together outside a Rheinmetall facility in Rome, which they claimed "hindered production" and "made the gate inaccessible for an entire work shift."

Affiliate: Death to Toll (Australia)

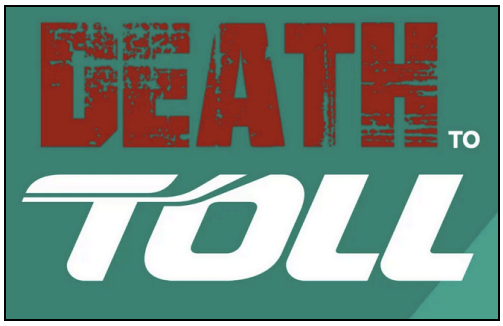

Figure 8: *Death to Toll logo (Source: Instagram)*

"Death to Toll" is a campaign by anarchist violent extremists (AVEs) in Australia to conduct vandalism, obstruction, and sabotage against the Australian international logistics and shipping company Toll Group (Toll), its parent organization Japan Post Holdings, and defense contractors working with the Australian Defense Force (ADF), due to accusations that Toll and the ADF are partnering with the Israeli military. The group responsible for this campaign is classified as a Palestine Action affiliate, as it almost certainly shares Palestine Action UK's ideology and uses TTPs promoted by the group, but operates solely in the Melbourne, Australia area and has chosen its own companies to target.

The first attack claimed by this group was a sabotage of a Heat Treatment Australia (HTA) facility on October 14, 2024; the campaign against Toll began with an obstruction of one of the company's facilities in Melbourne on November 22, 2024. In an August 7, 2025, interview, Death to Toll's organizers cited Palestine Action's targeting of UK shipping organizations that partnered with Elbit as an inspiration for their attacks. They also have shared a copy of Palestine Action's 2023 instructional guide on their website.[10]

In recent months, the Death to Toll group has claimed responsibility for several acts of vandalism, obstruction, and sabotage targeting Toll:

- On October 7, 2025, AVEs claimed responsibility for intercepting a Toll fuel truck in Melbourne by obstructing a road with flaming objects. They subsequently spraypainted the truck with red

[10] Source document held by Insikt Group.

graffiti.

- On August 31, 2025, AVEs claimed to have attacked a Toll facility in Dandenong South. A video posted to the group's Instagram account shows activists smashing exterior glass doors of the facility with a blunt object and dousing them with a flammable liquid in a bottle, very likely gasoline.
- On August 11, 2025, AVEs claimed to have vandalized a Toll facility in Truganina, writing graffiti, spraying red paint, and damaging keycard access devices on the exterior of the facility. Toll confirmed the attack in a statement to the press, and Victoria Police indicated they were investigating the incident.

Beyond its website, the Death to Toll campaign operates a social media account and accepts submissions from independent AVEs for claims of responsibility and tips on potentially vulnerable facilities on a Mega file-sharing site and through a Proton Mail email address. The social media pages attributed to the group have frequently used the hashtags #socalledaustralia, #DeathToll, and #TheDeathTollisRising. On the front page of their website, the administrators have posted a call to action against industries in Australia that they perceive to be providing support for the IDF. Specifically, they claim that "all sites and equipment used or owned by Toll Holdings and its parent company, Japan Post, are legitimate targets for anti-genocide action. This includes sabotage, vandalism, blockades, strikes, occupations, and all forms of resistance and disruption. Everything is on the table."

Offshoot: Unity of Fields (United States)

Figure 9: *Unity of Fields logo (Source: Social Media)*

Unity of Fields (UoF) describes itself as an "anti-imperialist propaganda front" that reports on the activities of militant pro-Palestinian activists in the US. In this regard, it functions in a similar fashion to AVE "counter-info" outlets, which provide AVEs in a specified geographic area with information pertaining to upcoming protests and demonstrations, claims of responsibility for AVE attacks, guides and instructional material for carrying out attacks, and communiqués from local AVE groups.

UoF was almost certainly founded as a Palestine Action franchise in the US: during its initial years of operation, it used the name "Palestine Action US," was managed by a cell of activists who almost certainly founded the group with insight from Palestine Action UK members, and devoted itself to attacking Elbit facilities in the US using Palestine Action's standard TTPs.

From October 7, 2023, to August 2024, Palestine Action US predominantly conducted vandalism, obstruction, and sabotage against Elbit facilities, particularly in Cambridge, Massachusetts, and Merrimack, New Hampshire. Calla Walsh — almost certainly one of Palestine Action US and UoF's de facto leaders between October 2023 and July 2025 — was arrested and convicted for her role in a November 20, 2023, Palestine Action US attack on an Elbit facility in Merrimack.

In August 2024, following Walsh's release from prison, Palestine Action US announced its rebranding as "Unity of Fields", appropriating a concept from the Yemeni Houthi movement. The group subsequently renamed its social media and online messenger accounts, launched a new website dedicated to the group's communiqués and instructional materials, and claimed the group's new mission was to establish "a militant propaganda front against the US-NATO-zionist axis of imperialism." In addition to claims of responsibility for attacks, the website also hosts a repository of instructional and ideological material, as well as publications produced by other AVE groups.

Autonomous pro-Palestinian activists across the US have sent several dozen claims of responsibility to UoF for publication claiming responsibility for operations against an array of targets, including defense contractors (including Magellan Aerospace, Rolls-Royce and MTU America, Lockheed Martin, Ghost Robotics Corporation, Leidos, and Israel Chemicals), banks (including Bank of America, Citibank, Wells Fargo, Chase Bank, and BNY Mellon), shipping and logistics companies (including Maersk and Amazon), US military recruitment centers, law enforcement infrastructure (particularly vehicles), university buildings and officials, public transportation, and construction buildings and equipment.[11] Occasionally, DVEs from outside of the US — including other Palestine Action global network groups — send communiqués to UoF for publication. At the time of writing, the most recent claims of responsibility include:

- An August 7, 2025, communiqué claiming responsibility for an arson of several vehicles at a Lovitt Technologies plant in Melbourne, Australia[12]
- A May 29, 2025, communiqué claiming responsibility for spraypainting several pro-Palestinian messages on a Maersk shipping container in Oakland, California[13]
- A May 9, 2025, communiqué from protesters at the University of Washington that details the occupation of a university building[14]

UoF has significantly decreased its output of new claims of responsibility since late July 2025, very likely because of internal disputes and a leadership transition within the group. On July 29, 2025, Calla Walsh reported on social media that she was "no longer part of" UoF after a dispute over the "direction in which the project is going," following which Walsh reported "the organization purged me" and that she had "complied with the decision and transferred them ownership of the accounts." While Insikt

[11] This assessment is predicated on Insikt Group's review of claims of responsibility posted to UoF's websites between August 2024 and the present.
[12] Source document held by Insikt Group.
[13] Source document held by Insikt Group.
[14] Source document held by Insikt Group.

Group is unaware of the exact nature of this dispute, Walsh's departure from UoF directly followed a July 2025 trip she made to Iran, where she participated in an event hosted by the World Service of the Islamic Republic of Iran Broadcasting (IRIB), Iran's government-operated media agency. In an October 5, 2025, article on her Substack page, Walsh reported that she had been detained by US Customs and Border Protection (CBP) officers at New York's John F. Kennedy International Airport following her return from Tehran.[15]

Partner: Shut the System (United Kingdom)

Figure 10: *Shut the System logo (Source: Social Media)*

Unlike other groups included in this report, which are predominantly motivated by the Palestinian cause, Shut the System is a UK-based environmental violent extremist (EVE) group that likely emerged as an offshoot of the UK climate activist group Extinction Rebellion (XR). However, the group has also almost certainly conducted pro-Palestinian direct actions. In addition, Shut the System has also directly collaborated with Palestine Action in the UK, almost certainly due to substantial overlaps between Palestine Action's and Shut the System's TTPs, preferred targets, and areas of operation. For instance, Shut the System frequently targets insurers and banks that it claims provide services to major global fossil fuel extraction projects; Palestine Action has also targeted many of the same companies on the grounds that they provide services to the IDF or Israeli government. Both groups also frequently use vandalism with red paint, projectiles, or blunt objects to deface the facade of target properties, as well as sabotage, although Shut the System has very likely deployed more sophisticated methods of infrastructure sabotage than Palestine Action. Overall, Shut the System fits the profile of a Palestine Action partner organization.

The first reported Shut the System operation took place in late February 2024. During 2024, the group predominantly conducted vandalism targeting the London offices of insurance companies, such as AIG, Probitas 1492, Chubb, Liberty General, Lloyd's of London, Markel UK, QBE, Tokio Marine, as well as Barclays, using red paint, graffiti, and projectiles.[16] In a January 2025 communiqué, Shut the System claims to have selected these companies as targets because they were identified in a November 2023 article from Insurance Business Magazine as among the top ten insurers of fossil fuel extraction projects in the world. On June 10, 2024, Shut the System and Palestine Action conducted a joint,

[15] Source document held by Insikt Group.
[16] This assessment is predicated on Insikt Group's review of claims of responsibility posted to Shut the System's social media accounts and websites.

UK-wide operation targeting Barclays bank branches in Birmingham, Bristol, Brighton, Edinburgh, Exeter, Glasgow, Lancashire, London, Manchester, Northampton, Sheffield, and Solihull. Activists from both groups sprayed red paint on the exterior of the branch facilities and smashed their windows with projectiles.

Subsequently, the group has very likely expanded its targeting aperture to include conservative think tanks, additional financial services providers, and events for defense contractors, posting claims of responsibility for attacks on its websites and social media profiles. Shut the System's website also contains instructions on how to conduct vandalism, obstruction, and sabotage on behalf of the group, and provides a list of 38 banks and insurance companies that it identifies as priority targets due to their alleged financing of the fossil fuel industry.[17] The group continues to conduct joint operations with a number of UK-based AVE and EVE cells, including cells affiliated with almost certain Palestine Action offshoot groups. For instance, during the past several months, Shut the System claims to have collaborated with pro-Palestinian militant direct action groups during the following operations:

- On October 8, 2025, Shut the System's "Palestine solidarity faction" and activists from the UK group Palestine Pulse claimed to have used projectiles and blunt instruments to destroy "entrances, glass panels, security cameras and ID card readers" at a Palantir Technologies facility in London. They additionally claimed to have sprayed red paint on the building's facade.[18]
- On September 29, 2025, Shut the System claimed to have conducted a joint operation with Shut Elbit Down and French and German XR affiliate groups to target Barclays and BlackRock assets throughout the UK and Europe. Activists sprayed red paint outside of Barclays offices in Paris, France, and Hamburg, Germany, and a BlackRock office in Vienna, Austria, and "superglued locks of [Barclays] branches across the UK." Additionally, Shut the System stated it targeted two Barclays senior executives in the UK by spraying red paint outside of their personal residences, and sending letters to the executives' neighbors "inviting them to a cocktail party hosted by the [executive] where they can explain why they have no conscience."[19]
- On September 8, 2025, Shut the System claimed to have severed fiber-optic cables leading to the London offices of Clarion Events, the company responsible for hosting the Defence and Security Equipment International (DSEI) defense trade exhibition. It conducted the action as part of a campaign, "Shut DSEI Down," that aimed to protest the trade exhibition due to the participation of several defense contractors that pro-Palestinian activists argue provide armaments to the IDF.[20]

From January 2025 onward, Shut the System frequently used a physical attack TTP that we have not observed in the operations of other Palestine Action global network groups, namely, sabotaging communications infrastructure by cutting fiber optics lines. Instructions on Shut the System's website demonstrate how to identify fiber optic cable boxes outside of target facilities, locate the correct wires, and sever them to disrupt internet and other communications services to the building.[21] Between August

[17] Source document held by Insikt Group.
[18] Source document held by Insikt Group.
[19] Source document held by Insikt Group.
[20] Source document held by Insikt Group.
[21] Source document held by Insikt Group.

18 and September 31, 2025, Shut the System launched a campaign titled "Summer of Sabotage" in which it encourages activists to use these and other sabotage TTPs to target banks and financial industry entities.[22]

Mitigations

The decentralized nature of individual Palestine Action cells entails that activists very likely plan operations in closed or encrypted communications channels that are almost certainly inaccessible to individuals who have not established their bona fides with the group. The groups' official communications announce operations after the fact; they almost certainly will not provide indicators and warnings (I&W) of planned activities.

To diminish risks from physical threat activities conducted by Palestine Action's global network, organizations and their physical security teams should focus on mitigating the effects of attacks by implementing the following approaches. Overall, physical security measures should aim to deny Palestine Action operatives interior access to facilities. The most costly attacks perpetrated by the group — including the June 2025 attack on RAF Brize Norton — took place after activists were able to breach secure perimeters, enter facilities, and sabotage assets stored inside perimeters.

- Recorded Future customers can leverage the Recorded Future Intelligence Operations Platform to monitor communications sources connected to Palestine Action and its global network, in order to determine evolutions in trends in targeting and TTPs and an organization's overall risk level.
- Customers can use the Recorded Future Platform's Intelligence Cards, Advanced Query Builder, and Insikt Group reporting to track ongoing global events — such as the Israel-Hamas conflict or the status of Palestine Action's legal battle against its terrorism designation in the UK — that are likely to affect threat actors' operational tempo and targeting aperture.
- Integrate this report and other Insikt Group assessments of DVE threat actors' TTP and targeting into structured tabletop exercises for physical security teams.
- Review and, where necessary, implement governmental guidelines for physical protection of business facilities, particularly with regard to electronic surveillance, secure lighting, and security personnel.
- Conduct vulnerability assessments to enable effective contingency and resiliency planning in the event of an incident of vandalism, obstruction, or sabotage, with particular focus on a successful incident disrupting communications, transportation, and energy infrastructure.
- Limit voluntary publication of information about the functions, layout, and location of critical infrastructure assets at facilities, or security measures at a facility, beyond the levels necessary to comply with legal or regulatory requirements.

[22] Source document held by Insikt Group.

Outlook

While Palestine Action's branch in the UK continues the ongoing legal appeal of its terrorism designation — very likely until the designation is rescinded or all of its legal options are exhausted — Palestine Action's global network is very likely to escalate the frequency and scope of its militant direct action operations. In the short to medium term, the formation of new Palestine Action global network groups in North America, Western Europe, Australia, and elsewhere around the world is likely, threatening an increased range of organizations in defense contracting, banking, finance, insurance, and shipping and logistics sectors.

Extant groups linked to Palestine Action are also likely to traverse the various categories of groups described in this report, with cells inside the UK attempting to separate themselves from the Palestine Action brand to avoid legal scrutiny and cells outside the UK highlighting their connections to Palestine Action to build credibility with AVEs and the pro-Palestine activist movement. As such, we expect existing franchises and affiliates in the UK to increasingly become offshoots and partners while the ban is in effect; the reverse is likely in geographic areas outside the UK where Palestine Action is not a designated terrorist organization.

Volatile dynamics in the Israel-Hamas conflict and the situation in the Gaza Strip are also very likely to influence Palestine Action's global network in the short to medium term, especially with regard to the frequency of attacks. At the time of writing, a ceasefire between Israel and Hamas, effective October 10, 2025, remains in effect. While the establishment of the ceasefire likely did not stop Palestine Action network groups from conducting operations — several of the groups profiled in this report have carried out attacks in the interim — any potential breakdown in the ceasefire would very likely augur increased Israeli military activity in the Gaza Strip that has historically caused upticks in attacks related to the network.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com