June 18, 2025

Hybrid Warfare Unfolded: Cyberattacks, Hacktivism and Disinformation in the 2025 Israel-Iran War

Key Insights Since the Start of the Conflict:

- Israel launched high-impact cyber strikes on Iranian financial infrastructure
- Iran responded with disinformation and psychological warfare
- Hacktivist activity surged, heavily skewed toward Iran's side
- Disinformation and AI-generated media continue to flood the online narrative
- Cyber conflict threatens regional and global spillover

The outbreak of the open conflict between Israel and Iran on June 13, 2025, marked by Israeli airstrikes on Iranian nuclear and military sites and Iranian missile salvos in return, has rapidly expanded into cyberspace. Both nations are renowned cyber powers with a long history of digital attacks against each other. In the days since the fighting began, government-backed hackers, patriotic hacktivists, online propagandists and opportunistic cybercriminals have all been active. This report provides an overview of the most significant cyber activities related to the conflict, including state-sponsored operations, hacktivist attacks and disinformation campaigns.

State-Sponsored Cyberattacks

Israeli Operations

Israel has a formidable offensive cyber capability, famously exemplified by the Stuxnet virus that sabotaged Iran's uranium centrifuges in 2010. In this conflict, Israel-linked actors have already conducted major cyber strikes on Iranian critical infrastructure. On June 17, the Israeli hacking group Gonjeshke Darande (Persian for Predatory Sparrow) claimed it had infiltrated Iran's state-owned Bank Sepah and destroyed the bank's data. The attack caused widespread service outages. Iranian media reported that customers are unable to access accounts, withdraw cash or use bank cards. Predatory Sparrow, widely seen as a front for Israeli cyber units, has a track record of causing physical disruptions in Iran. It previously sabotaged steel plants, railways and gas stations.

Figure 1: Predatory Sparrow announcing the destruction of data from Bank Sepah (source: X)

Just a day after the bank hack, the same group announced it had breached Nobitex, a major Iran-based cryptocurrency exchange, calling it "a tool for financing terrorism and violating sanctions." The hackers threatened to publish Nobitex's source code and internal data within 24 hours, warning users to remove any remaining funds. Blockchain investigators later confirmed that approximately $81.7 million in digital assets were stolen from Nobitex's wallets during the breach.

Figure 2: Predatory Sparrow announcing the breach of Nobitex (source: X)

Iranian Operations

For its part, Iran has a considerable number of state-sponsored threat groups that have engaged in espionage and disruptive attacks. In the past, groups like APT34 (OilRig), APT35 (Charming Kitten), APT39 (Remix Kitten), and others under the IRGC (Islamic Revolutionary Guard Corps) have targeted Israeli infrastructure, including water systems, transportation control, and even

surveillance networks. Since the conflict began, Iran's cyber response has been aggressive but so far lower in profile and mostly psychological in effect. Israeli cybersecurity officials report that Iranian-linked actors have launched waves of phishing emails, DDoS attacks, and fake alert messages aimed at Israeli civilian systems in the days following the initial strikes. For example, shortly after hostilities broke out, many Israelis received alarming but false text messages. One claimed fuel supplies would run out at gas stations within 24 hours. Another warned of an imminent terrorist bombing at a shelter. All were spoofed to appear as if sent by Israel's Home Front Command. These were disinformation attacks intended to sow panic on the home front.

Analysts suggest Iran's top-tier hackers may be holding back more devastating cyber weapons unless the conflict escalates further. However, given Iran's diminished ability to respond militarily after Israeli strikes killed several senior commanders and damaged bases, it would be safe to assume that Tehran is more likely than ever to retaliate through cyberattacks as an asymmetric alternative. Scenarios of concern include Iranian state hackers deploying ransomware or wiper malware to sabotage Israeli critical services or attempting to steal sensitive military data via stealthier espionage intrusions.

Both Israel and Iran are fully aware that cyberspace is a key battleground in this war, and each side is poised to unleash more potent digital operations if strategically necessary.

Surge of Hacktivism

Beyond official state operations, a swarm of hacktivist groups around the world has mobilized in response to the Israel-Iran war. Many are ideologically aligned with one side or the other, and they have been defacing websites, knocking services offline and leaking stolen data in a bid to score propaganda points. In fact, by the first weekend of fighting, nearly 100 different hacktivist groups had declared themselves part of the cyber conflict (source: CyberKnow). The vast majority, at least 60+ groups, are pro-Iran and hail from across the Middle East and Asia, where Iran has sympathizers. A smaller contingent of pro-Israel hacktivists has also emerged, around a dozen groups, but the scene is dominated by actors supporting Iran's cause.

Since the conflict began, Radware observed roughly 30 DDoS attack claims targeting Israel per day, with activity peaking on Saturday, June 14, when 40 DDoS attacks were claimed.

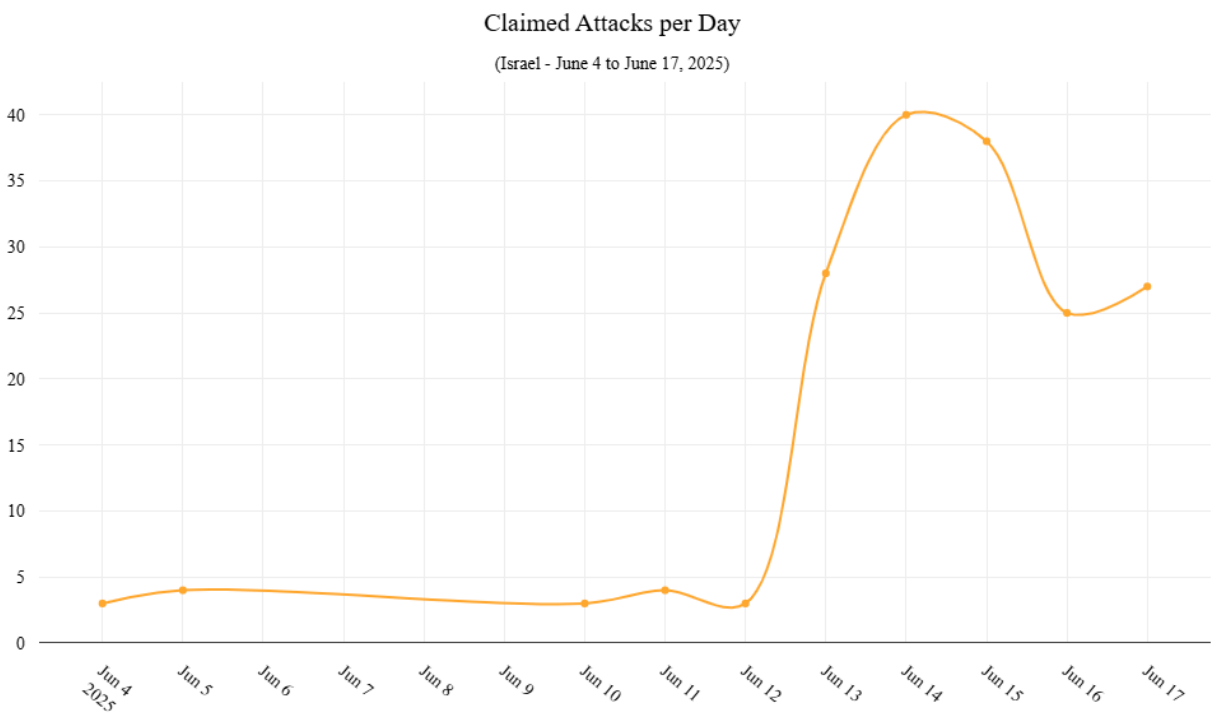

Figure 3: Hacktivist claimed DDoS attacks targeting Israel from June 4 untill June 17, 2025 (source: Radware)

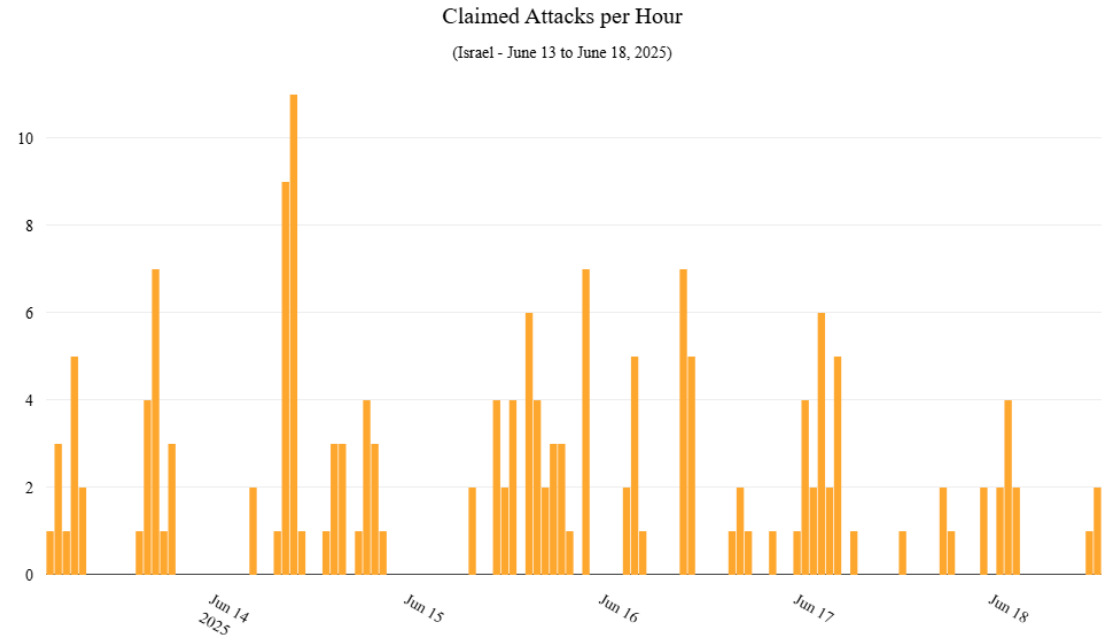

Figure 4: Claimed DDoS attacks per hour targeting Israel between June 13 and June 18, 2025 (source: Radware)

Since the onset of the conflict, nearly 40% of all hacktivist DDoS activity tracked by Radware has been directed at Israel.

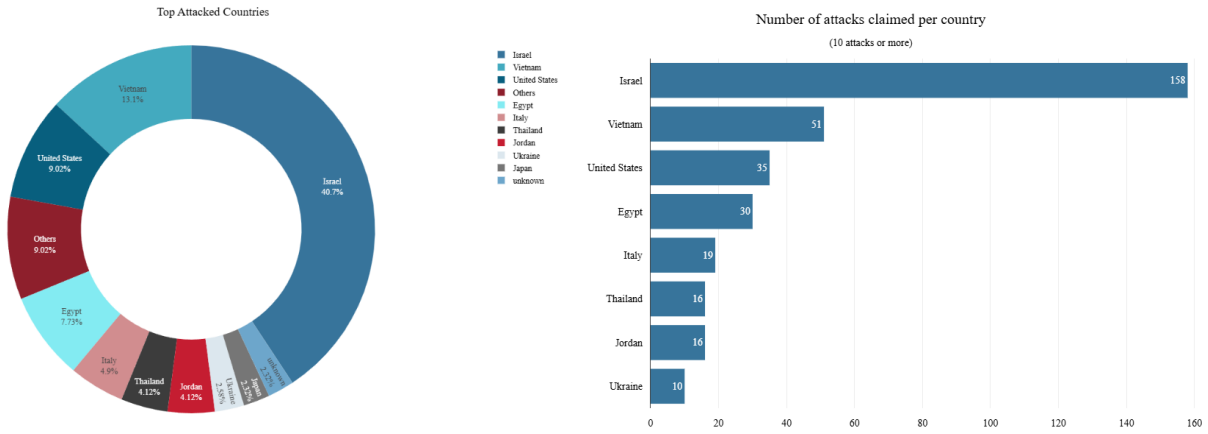

Figure 5: Global hacktivist activity between June 13 and June 17, 2025 (source: Radware)

The campaign targeting Israel is primarily led by two groups, Mr Hamza and Arabian Ghosts. Below is the full list of hacktivist groups observed targeting Israeli resources with DDoS attacks since the beginning of the conflict:

1. Mr Hamza
2. Arabian Ghosts
3. Server Killers
4. Lulzsec Black
5. Unknowns Cyber Team
6. Elite Squad
7. TwoNet
8. Moroccan Black Cyber Army
9. DieNet
10. Nation of Saviors
11. RipperSec
12. Sylhet Gang
13. Anonymous Guys
14. Keymous+
15. Mysterious Team Bangladesh
16. Red wolf cyber
17. Cyber Fattah team
18. Team Fearless
19. Coup Team
20. Ghost Clan
21. Garuda Error System
22. MadCap
23. Desinformador ruso
24. Tunisian Maskers Cyber Force

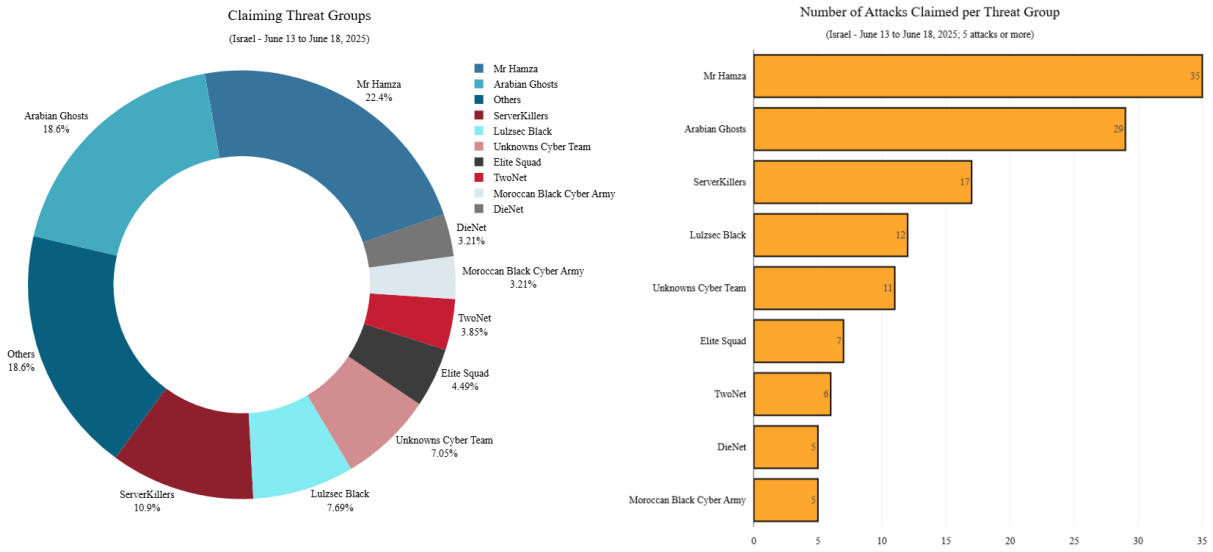

Figure 6: Groups claiming DDoS attacks targeting Israel between June 13 and June 18, 2025 (source: Radware)

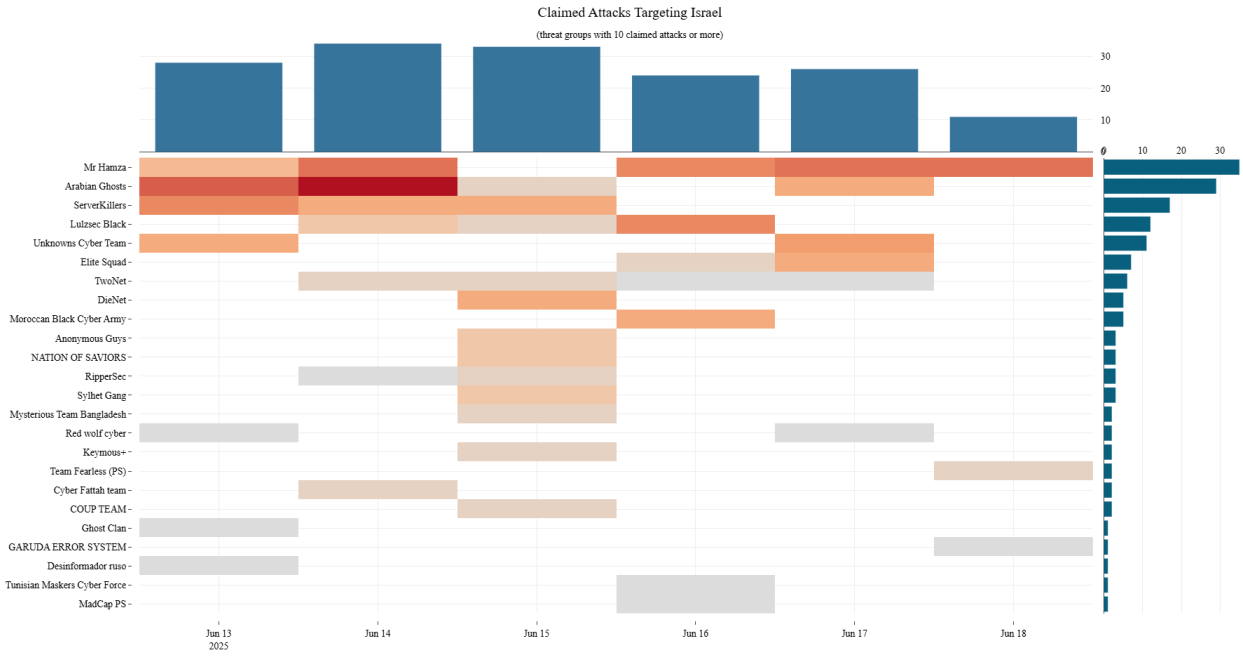

Figure 7: Heatmap of DDoS attacks targeting Israel, claimed per day, per group (source: Radware)

The top five industries in Israel most frequently targeted by hacktivist DDoS attack claims since the start of the conflict are:

1. Government & Public Sector (~27%)
2. Manufacturing (~20%)
3. Telecommunications (~12%)
4. Media & Internet (~9%)
5. Banking and Financial Services (~5.3%)

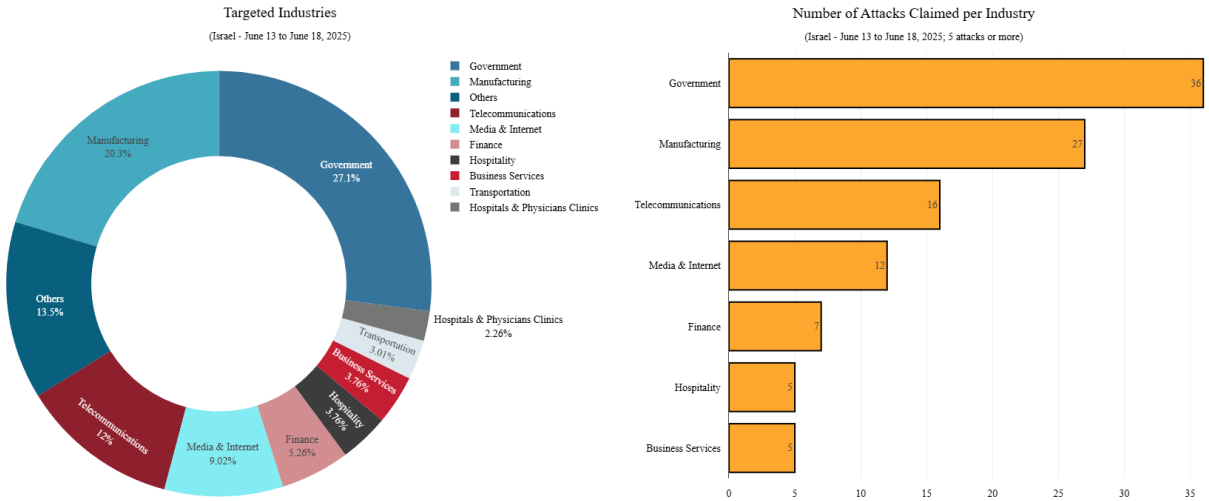

Figure 8: Top targeted Israeli industries between June 13 and June 18, 2025 (source: Radware)

Global Fallout: Countries Targeted by Hacktivists Over the Conflict

On Friday, June 13, Mr Hamza, in coordination with Anonymous Guys, Team 1722, and Desinformador Ruso, announced a coordinated campaign of cyberattacks targeting the United States, the United Kingdom, and Israel.

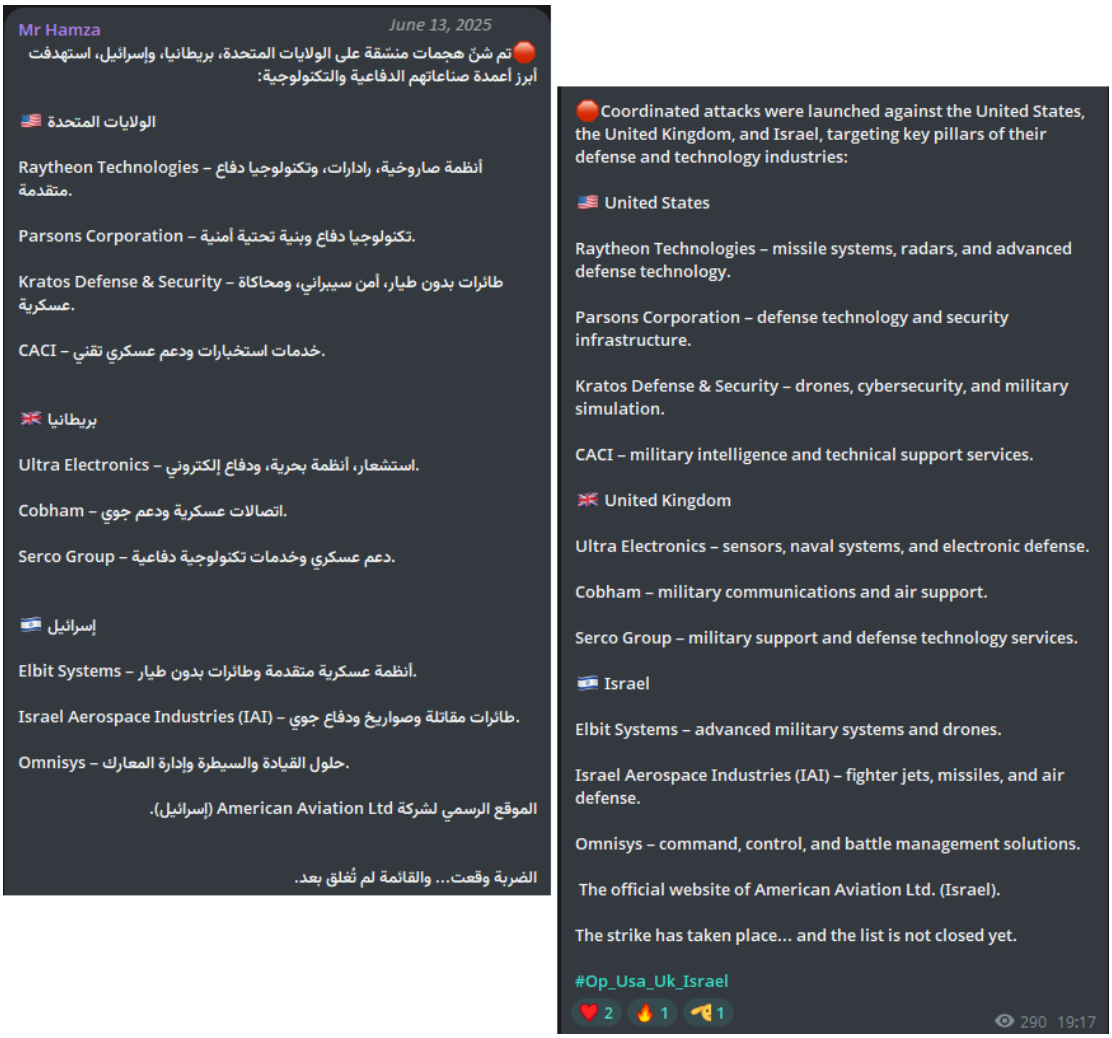

Figure 9: Mr Hamza announcing #Op_Usa_Uk_Israel campaign targeting US, UK and Israel (source: Telegram)

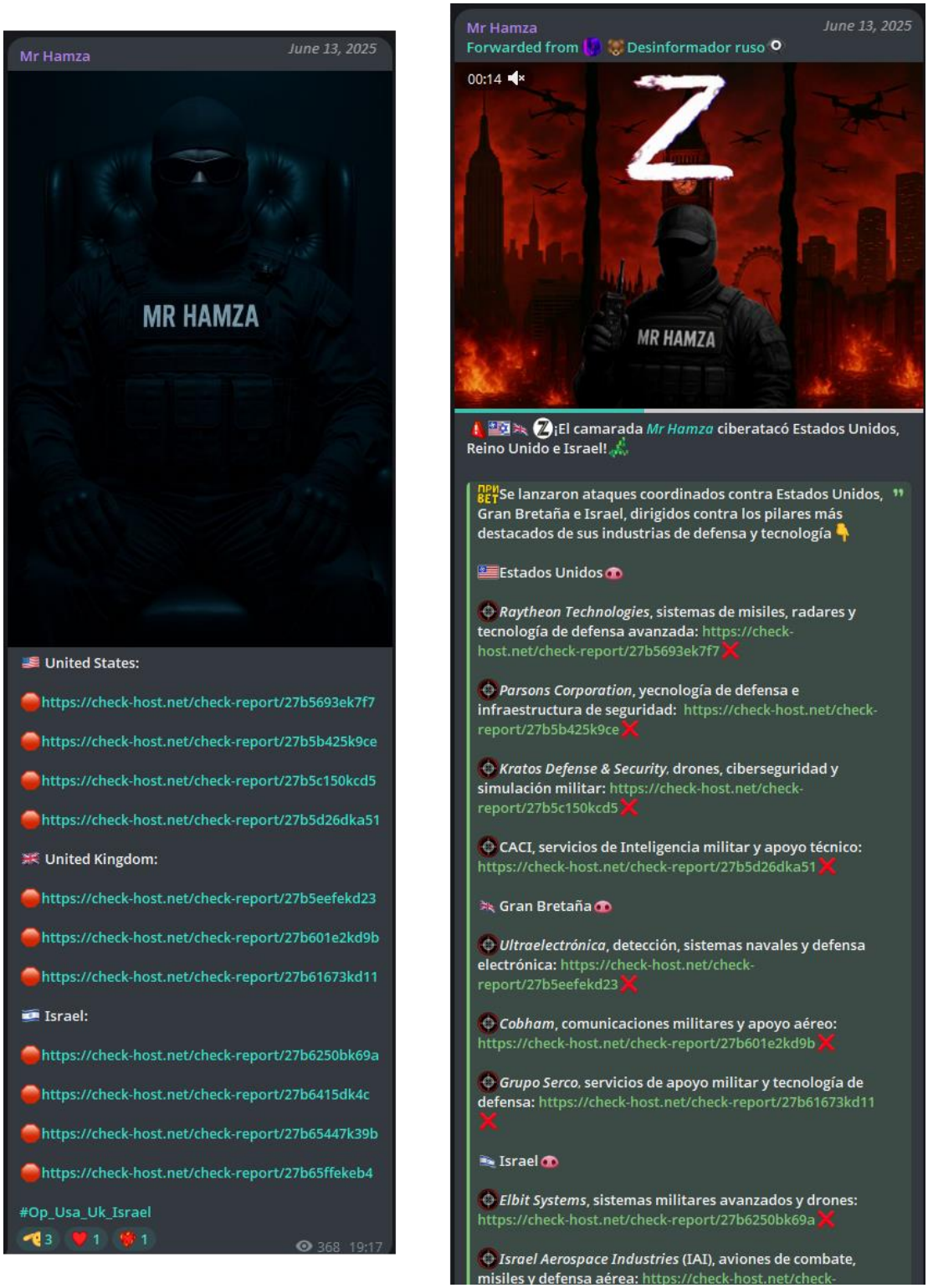

Figure 10: Attacks claimed by Mr Hamza and Desinformador Ruso after announcing #Op_Usa_Uk_Israel (source: Telegram)

On the evening of Tuesday, June 17, the hacktivist group DieNet issued a warning that they would launch cyberattacks against the United States if it "joins the war against Iran." The announcement was rapidly amplified by affiliated or sympathetic groups, including Arabian Ghosts, Sylhet Gang, and Team Fearless, signaling potential coordination and escalation in response to the developments.

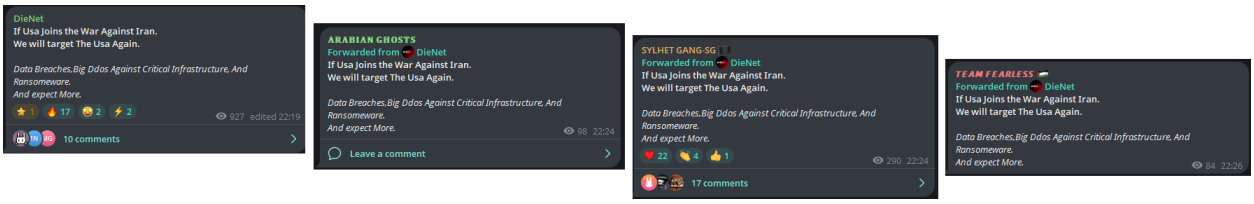

Figure 11: DieNet issuing a warning to the United States, forwarded by Arabian Ghosts, Sylhet Gang and Team Fearless (source: Telegram)

It comes as no surprise that DieNet would take the lead in a campaign targeting the United States, given their established track record of launching cyberattacks against U.S. entities and infrastructure. Their history reflects a consistent focus on American targets, making their latest threat a continuation of prior hostilities rather than a deviation.

The most frequently targeted countries in relation to the Israel/Iran conflict include:

- **United States:** Targeted by Mr Hamza, Arabian Ghosts, Unknowns Cyber Team, DieNet, Elite Squad, Morrocan Black Cyber Army and Mysterious Team Bangladesh, who also targeted Israel in the same period
- **Jordan:** Targeted by Arabian Ghosts, LulzSec Black, Morrocan Black Cyber Army and Mysterious Team Bangladesh, who also targeted Israel in the same period
- **United Kingdom:** Mr Hamza, Unknowns Cyber Team and TwoNet, who also targeted Israel in the same period

Keymous+ and Mysterious Team Bangladesh primarily focused their cyber operations on Egypt, but both groups also claimed responsibility for attacks against Israeli organizations.

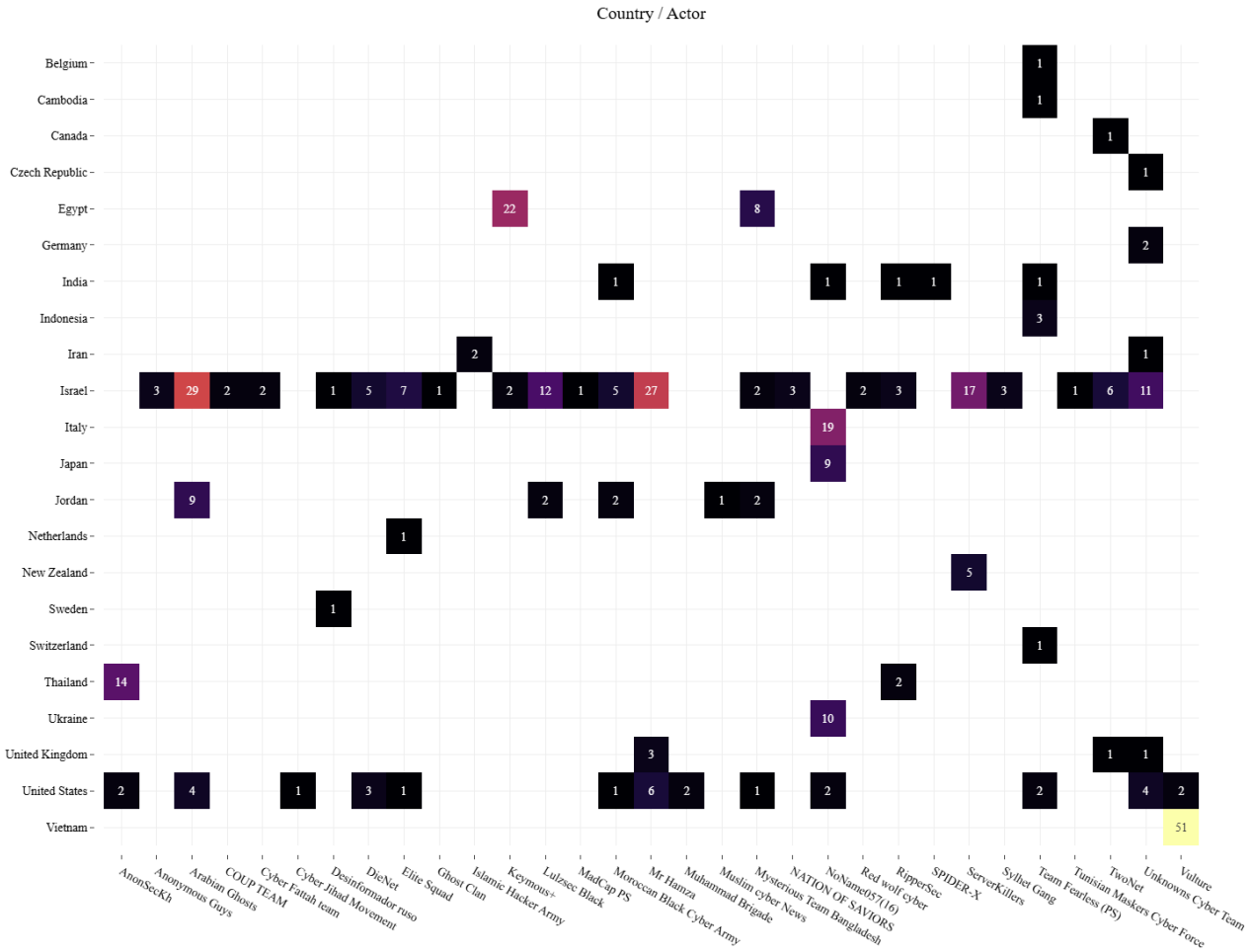

Figure 12: Heatmap of countries targeted by hacktivist groups between June 13 and June 17, 2025 (source: Radware)

Disinformation and Influence Campaigns

A parallel information war is raging on social media and messaging platforms, as both sides seek to control the narrative and influence public opinion. Almost immediately after the air war began, Iran and its allies launched extensive propaganda and deception efforts online. Israeli officials describe the primary objective of Iranian cyber efforts right now as “intimidation, fake news, and disinformation” aimed at Israeli society. Specific tactics observed include:

- **Fake Emergency Alerts**: As noted earlier, Iranian operatives sent large amounts of fraudulent text messages to Israelis, aiming to spread panic with fake emergency announcements (e.g. false reports of fuel shortages or imminent terror attacks). These messages were crafted to look official by spoofing the sender as Israel’s Home Front Command.
- **Social Media Botnets**: Radware expects Iran to leverage its well-developed network of fake social media personas and bots to shape perceptions of the conflict. Tehran’s “cyber

armies" (often run by the IRGC's psychological operations units) have in the past created legions of fictitious online characters—complete with AI-generated profile photos—to push coordinated narratives. During this crisis, observers have seen pro-Iran bot accounts amplifying hashtags about alleged Israeli atrocities and portraying Iran's actions as defensive. These inauthentic accounts frequently pose as ordinary citizens (or even as Israelis critical of their own government) to make the messaging more persuasive. Iranian influence campaigns also enlist sympathetic bloggers and media outlets across the region to echo Tehran's line.

- **Fake Images and AI-Generated Media:** A worrying trend is the circulation of doctored images and deepfake videos related to the war. Analysts noted that official channels from both Iran and Israel have shared misleading or fake visuals of battlefield events. For instance, Iranian state media broadcast footage of purported Palestinian civilian casualties that was later identified as a montage of unrelated scenes. Conversely, an Israeli social media account posted an image of a downed Iranian drone that turned out to be from an older incident. Iran's influence apparatus has demonstrated advanced capabilities with AI deepfakes. Notably, Iranian hackers hijacked UAE streaming TV services in late 2023 and aired a deepfake newscast with an AI-generated anchor spreading Tehran's propaganda about the Gaza war. That operation, run by an IRGC-linked group dubbed Cotton Sandstorm, showed the potential for Iran to deploy deepfakes at scale. In the current conflict, experts are on high alert for similar use of fabricated audio or video such as a fake video of an Israeli general surrendering, or footage of carnage designed to inflame public outrage. Such synthetic media can go viral faster than fact-checkers can debunk it, making it a powerful weapon in the information war.
- **Iran's Domestic Controls and Narrative:** Inside Iran, the regime has moved to tighten internet controls and shape the narrative of the war. Over the past week, Iran has imposed internet disruptions nationwide, which officials described as "temporary" measures to maintain network stability amid what they claim are ongoing Israeli cyberattacks. Internet connectivity data showed a sharp drop as these curbs were enacted. In addition, Iranian authorities reportedly restricted access to foreign news sites and even blocked many international calls to prevent the spread of information that contradicts state media. The information blackout is intended to impede any Israeli attempts at psychological ops targeting the Iranian public. Notably, Iran's state television and officials have aggressively pushed the narrative that Israel and its Western allies have initiated a "massive cyber war" against Iran's infrastructure. This framing seeks to cast Iran as the victim of cyber aggression and justify any further Iranian "retaliatory" cyber steps. In one instance of disinformation, Iranian state TV urged citizens to uninstall WhatsApp, accusing the popular messaging app of spying for Israel. WhatsApp firmly denied this, calling it a baseless excuse that Iran might use to ban the app and isolate people.

The online disinformation and influence side of this war is highly active. False narratives, doctored

evidence, and strategic censorship are all in play. This digital fog of war makes it challenging for the public to discern truth, and it underscores how modern conflicts are fought not just with missiles, but with memes and messaging apps.

Summary

In summary, the first week of hostilities has demonstrated that the Israel-Iran conflict is being fiercely contested in cyberspace as well as on the ground. State-backed cyberattacks have already hit significant targets, though Iran's most dangerous cyber weapons may still be in reserve. A tidal wave of hacktivist activity, largely rallying to Iran's side, is keeping Israeli networks busy fending off disruptions and leaks.

A parallel disinformation war is attempting to influence hearts and minds worldwide, fueled by fake personas and fabricated media. Going forward, organizations in the region and around the world are on high alert for spillover effects. Cybersecurity firms are urging maximum vigilance, warning that critical infrastructure, supply chains and even global businesses could become collateral targets if the cyber crossfire intensifies. The Israel-Iran conflict of 2025 is a stark illustration of modern hybrid warfare, where bytes and narratives are as much a part of the fight as bombs and missiles.

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premises and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection – Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation – Promptly protect against unknown threats and zero-day attacks

Web DDOS Tsunami Protection – Automated immediate detection and mitigation of Web DDOS encrypted high RPS and morphing attacks

A Cybersecurity Emergency Response Plan – Turn to a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options including on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.