The Role of Cyber Operations in Middle East Conflict

Teneo Insights | October 2024

As the Israel-Hamas conflict enters its second year, the military escalation between Israel and Iran-backed Hezbollah in Lebanon, along with increasing tensions between Iran and Israel, is likely to drive an increase in cyber operations from Iran, its proxies and other hacktivist groups.

As highlighted in our September cybersecurity insights article on the evolution and surge of "cyberpolitical risk," this recent activity underscores the need for heightened vigilance surrounding company cybersecurity, as organizations may become unexpected targets of politically motivated cyberattacks.

Widespread Cyber Campaign Targets Israeli Interests

Hacktivist groups from Iran, Iraq, Lebanon and Sudan are working together under the campaign name "OpIsrael" to pool their resources and expertise to launch more sophisticated and destructive attacks. These attacks aim to disrupt infrastructure, gather intelligence or spread propaganda to undermine Israel's war efforts. Israeli-based cybersecurity firm Check Point Software tracked over 40 cybergroups conducting attacks on government and media sites during Hamas' initial attack. As of July 2024, Israel

reported that Iran and Iran-backed groups have been responsible for roughly three billion cyberattacks, with Israel's cyber defenses successfully preventing almost every attack. However, some attacks were reportedly able to circumvent Israel's cyber defenses.

The pro-Russia hacktivist group Anonymous Sudan is collaborating with pro-Palestine hacktivist groups to conduct large-scale Distributed Denial-of-Service (DDoS) attacks on critical Israeli websites. In November 2023, the pro-Palestine, Iranian-linked hacking group Cyber Toufan claimed responsibility for targeting multiple Israeli government sites, including the Israel State Archives, stealing the personally identifiable information of thousands of the archives' users. This attack reportedly took the State Archives offline for several months, highlighting the effectiveness of the coordinated cyber campaign.

Cyber Toufan has also claimed responsibility for cyber breaches targeting Israel-based subsidiaries or Israeli branches of international companies, underscoring the spillover effect of global conflicts on the private sector in cyberspace. On November 16, 2023, Cyber Toufan hacked Signature-IT, an Israeli company that hosts websites for businesses operating in Israel. Through this attack, Cyber Toufan gained access to and leaked data from several multinational companies, including Toyota, ACE Hardware, Toys 'R' Us, Ikea and organizations conducting business with Israeli firms, such as SpaceX and a subsidiary of Berkshire Hathaway. In addition to disrupting website functionality and leaking sensitive data, Cyber Toufan leveraged access to company emails to send propaganda. While these attacks primarily targeted Israeli branches of international organizations, the increasing sophistication of cyber operations puts global companies at risk.

Many hacktivist groups hijack websites to display anti-Israel propaganda or claim successful hacks via messaging platforms like Telegram, often aligning their actions with military operations as part of a coordinated psychological warfare effort. For example, on April 13, 2024, the day that Iran launched missiles and drones at Israel, Handala Hack, a pro-Palestine cyber group with ties to Anonymous, claimed to have breached Israel's missile-tracking, allowing Israel to intercept them before reaching their targets. Despite these claims, Israel and U.S. defenses intercepted almost every missile, casting doubt on the validity of Handala's claims and those of other hacktivist groups. Most recently, Handala claimed to have successfully attacked Israel's Soreq Nuclear Research Center, stealing 197 gigabytes of data. These groups often republish previously stolen data, falsely suggesting new breaches to incite fear. While the success of the Soreq attack remains unconfirmed, the speculation surrounding it creates public anxiety, which groups hope will translate to political pressure, ultimately pushing forward these hacktivist groups' agendas.

Iran continues to fund its proxies, which have launched successful cyberattacks targeting Israel, organizations and platforms that can impact companies beyond the region. The Iranian-backed hacking group Moses Staff specializes in hacking and leaking sensitive information to undermine trust in Israeli cybersecurity and expose military plans to weaken Israel's strategic position. The group also targets government agencies, financial institutions, energy companies and the manufacturing and utilities sectors. Similarly, Iran-sponsored groups APT33 and APT34 have targeted critical infrastructure, including hospitals, through phishing attacks and exploiting vulnerabilities on Microsoft Exchange servers.

In addition to disrupting website functionality and leaking sensitive data, Cyber Toufan leveraged access to company emails to send propaganda. While these attacks primarily targeted Israeli branches of international organizations, the increasing sophistication of cyber operations puts global companies at risk.

Limited, but Effective Israeli Cyber Operations

While Israel has conducted fewer, or less reported cyberattacks, it is likely to take a more aggressive stance as the conflict escalates. Israel has previously demonstrated its cyber capabilities, such as in December 2023 when the Israeli-linked group Predatory Sparrow claimed responsibility for a cyberattack that disrupted 70% of Iran's gas stations, creating chaos at gas stations nationwide.

Governments at Risk as Conflict Persists

Governments and public sector organizations in the Middle East, particularly Israel's Abraham Accords partners, are likely to face heightened risk of cyberattacks as regional tensions persist. These attacks are unlikely to originate from state-affiliated entities due to the potential diplomatic consequences of direct involvement. However, Iran-linked cyber proxy groups are likely to be more motivated to carry out cyberattacks, as these actions offer Iran plausible deniability while expressing discontent over certain Middle East states' perceived support of Israel. In November 2023, Bahrain reported a cyberattack on the websites of the country's Foreign Ministry and Information Affairs Ministry, which was later claimed by Cyber Toufan. The group posted scans of passports, including those of American citizens and a top Russian diplomat in Bahrain, allegedly obtained during the hack. As tensions persist, the Abraham Accords countries will need to remain vigilant against attacks stemming from the conflict.

Considerations for Executives

As tensions spread throughout the Middle East, Iran and its proxies will likely continue to attempt destructive cyberattacks, offering them low-risk and low-cost methods to target their adversaries. The escalation of cyberwarfare underscores the critical role of cybersecurity during times of conflict, requiring organizations and employees to remain vigilant in preventing increasingly common attacks.

In the face of geopolitical cyber conflicts, companies must adopt robust cybersecurity strategies that include real-time threat detection, multi-layered defenses and automated incident response. Essential measures include implementing zero trust architecture, DDoS protection and end-to-end encryption to safeguard systems and data. Additionally, companies must focus on employee training to counter social engineering threats, ensure vendor risk management and maintain business continuity through cyber resilience. Leveraging cloud security and threat intelligence sharing further strengthens a company's defense against the threat of state-sponsored attacks and hacktivist campaigns. As cyberattacks become an integral piece of modern warfare, it is essential that companies prioritize robust cybersecurity capabilities.

Author

Lauren Menzie
Associate

For more information, email: Resilience&Intelligence@teneo.com

Teneo
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,600 employees located in 40+ offices around the world.

teneo.com