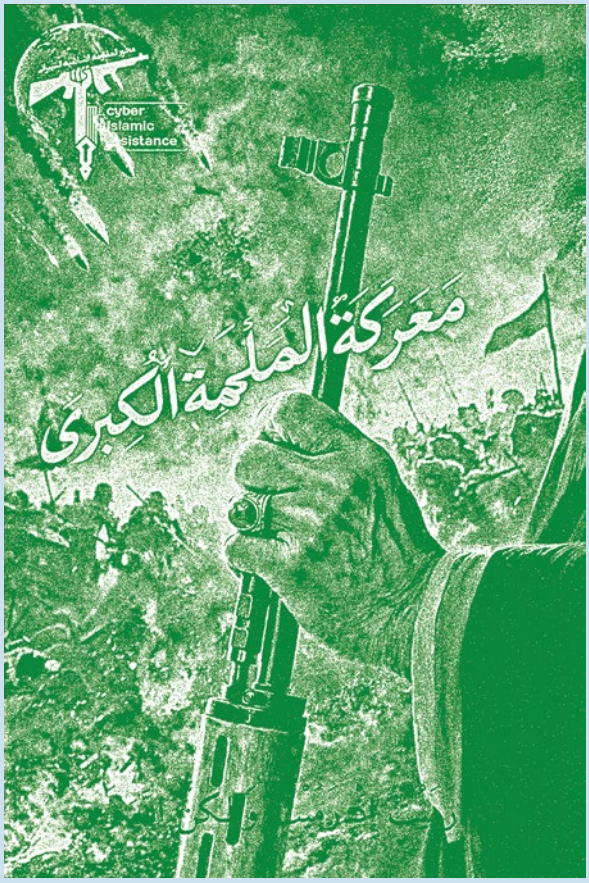
Antisemitische Cyberbedrohungen im Schatten des Iran-Israel-Konflikts



Ein Lagebild für Politik, Behörden und jüdische Institutionen in Deutschland

März 2026

democ.

Antisemitische Cyberbedrohungen im Schatten des Iran-Israel-Konflikts

Ein Lagebild für Politik, Behörden und jüdische Institutionen in Deutschland

März 2026

democ e.V.

Der Verein democ analysiert extremistische Bewegungen und entwickelt Gegenstrategien. Mit dem Projekt Projekt »Teilhabe verteidigen« stärkt democ die digitale Resilienz jüdischer und antisemitismuskritischer Organisationen und unterstützt ihre sichere Teilhabe am öffentlichen Diskurs. Durch Monitoring, Schulungen und die Entwicklung von Sicherheitskonzepten hilft das Projekt, digitale Bedrohungen frühzeitig zu erkennen und wirksam darauf zu reagieren.

IMPRESSUM

HERAUSGEBER
democ e.V.
Postfach 440648
12006 Berlin
Mail: kontakt@democ.de
Telefon: 030.57 71 22 21

ERSCHEINUNGSJAHR
2026

VERANTWORTLICHER IM SINNE DES PRESSERECHTS
Linus Kebba Pook

REDAKTION
democ e.V.

»Teilhabe verteidigen – Prävention antisemitischer Online-Gefährdungen« ist ein Projekt von democ. Für inhaltliche Aussagen tragen allein die AutorInnen die Verantwortung.

Gefördert durch:

Bundesministerium des Innern

aufgrund eines Beschlusses des Deutschen Bundestages

Titelbild: Propagandabild der Allianz »Cyber Islamic Resistance« (Quelle: Telegram)

Zusammenfassung

- **Die militärische Eskalation zwischen Israel, den USA und Iran** im Kontext der Operationen *Epic Fury* und *Roaring Lion* wird von einer deutlichen **Zunahme cyberbezogener Aktivitäten** begleitet. Internationale Analysen dokumentieren eine Welle von Distributed Denial of Service (DDoS)-Angriffen, Leak-Kampagnen, Desinformation und Social Engineering gegen israelische und westliche Ziele; ausgeführt von staatlichen iranischen Cyberakteuren und ideologisch motivierten Hacktivisten, die sich in pro-iranischen Netzwerken organisieren (Radware 2026; Sophos 2026; Anomali 2026).

- Frühere Konflikte zeigen, dass solche **Cyberkampagnen** häufig von antisemitischer Rhetorik begleitet werden und **auch jüdische Einrichtungen und Personen außerhalb Israels** betreffen.

- Für **Deutschland** weisen **mehrere Indikatoren auf eine hohe Bedrohungslage hin**: ideologisch motivierter Hacktivismus, ein stark antisemitisches Onlineklima sowie Warnungen deutscher Sicherheitsbehörden zu iranbezogenen Cyberaktivitäten (BKA 2025; RIAS 2025; Tagesspiegel 2025). Gleichzeitig fehlt bislang eine systematische Erfassung und Analyse antisemitisch motivierter Cyberangriffe, wodurch ein potenziell erhebliches Bedrohungsrisiko unterbelichtet bleibt.

- Das vorliegende **Lagebild** analysiert Cyberaktivitäten im Kontext des Iran-Israel-Konflikts, dokumentiert Angriffe und Vorfälle mit Deutschlandbezug und leitet daraus **Bedrohungsszenarien für Behörden, Unternehmen sowie jüdische Organisationen und Einzelpersonen in Deutschland ab**:
  - **Kurzfristig**: Leak-Behauptungen, DDoS-Angriffe und Website-Defacements.
  - **Mittelfristig**: Phishing-Kampagnen, gezielte Datensammlungen und koordinierte Desinformation.
  - **Langfristig**: Infiltration von IT-Systemen sowie Spionageoperationen.

- Zu beachten ist, dass iranische Cyberoperationen häufig zeitverzögert aktiviert werden. Vorpositionierte Zugänge in kritischer Infrastruktur – im Februar 2026 für US-amerikanische Netzwerken bestätigt – deuten darauf hin, dass bedeutende Operationen noch bevorstehen könnten (Symantec 2026).

Handlungsempfehlungen

Für öffentliche Einrichtungen, Unternehmen und jüdische Organisationen: Sensibilisierung für Phishing, Social Engineering und Doxxing sowie die konsequente Umsetzung grundlegender IT-Sicherheitsmaßnahmen: Multifaktor-Authentifizierung, regelmäßige Sicherheitsupdates, Backup-Strategien und DDoS-Schutz, z. B. über das Programm Cloudflare Project Galileo für zivilgesellschaftliche Organisationen.

Für Behörden: Systematische Beobachtung antisemitisch motivierter Hacktivisten-Netzwerke, enger Austausch mit potenziell betroffenen Einrichtungen sowie stärkere Sensibilisierung von Behördenmitarbeitenden für die Verbindung von Cyberangriffen, Desinformation und Antisemitismus. Erfassung und Auswertung antisemitisch motivierter Cybervorfälle als eigenständige Kategorie in Lagebildern und Berichten.

Für Politik und Zivilgesellschaft: Ausbau von Programmen zur digitalen Sicherheit zivilgesellschaftlicher Organisationen sowie Etablierung von Melde- und Monitoringstrukturen für antisemitisch motivierte Cyberangriffe und Desinformationskampagnen.

Bedrohungslage in Deutschland: Dokumentierte Fälle antisemitischer Cyberangriffe

Zahlreiche jüdische Einrichtungen in Deutschland verfügen über digitale Infrastruktur, die Ziel von Cyberangriffen werden kann. Bereits in der Vergangenheit **warnten Sicherheitsbehörden vor Social-Engineering-Operationen iranischer Cybergruppen gegen Personen mit Bezug zu jüdischen oder pro-israelischen Organisationen**. Ein prominenter Fall ist der Cyberangriff auf die Berliner Justizsenatorin Felor Badenberg im Jahr 2025, bei dem Angreifer sich als Vertreter des Zentralrats der Juden ausgaben und über eine Phishing-E-Mail erfolgreich Schadsoftware einschleusten (Tagesspiegel 2025; Handelsblatt 2025).

Abb 1–3 Statements der Hackergruppe BD Anonymous zu den Kampagnen #OpGermany und #OperationElectronicHolocaust, März 2026 (Quelle: Telegram)

Aktuell zeigt sich eine sehr konkrete Bedrohungslage für Deutschland: Zwischen dem 2. und 8. März 2026 führte die pro-russische Hackergruppe **NoName057(16)** 65,6 % ihrer gesamten Wochenkampagne gegen deutsche Ziele durch und griff dabei 17 öffentliche Vergabeportale sowie Kommunal- und Bundesbehörden an (SOCRadar 2026). Die Gruppe **BD Anonymous** griff im Rahmen der Kampagne **#OpGermany** zwischen dem 5. und 8. März 2026 mehrere deutsche Kommunalverwaltungen an, begründete dies mit angeblich fehlender deutscher Solidarität mit Palästina und verbreitete explizit antisemitisches Material unter dem Titel »**Operation Electronic Holocaust**« (Abb. 1–3)

Ähnliche Kampagnen finden auch im internationalen Kontext statt. Gemeinsam ist ihnen eine explizit antisemitische Rahmung, wie die Gleichsetzung Israels mit dem Nationalsozialismus und die Instrumentalisierung des Holocaustbegriffs als Kampfbezeichnung gegen jüdische Ziele – eine antisemitische Verhöhnung, die auf Wirkung über den digitalen Raum hinaus abzielt.

Im Berichtszeitraum dokumentierte Democ auf Telegram und in Hackerforen zudem **zahlreiche Datenleaks mit Israelbezug, die mit explizit antisemitischer Bildsprache und Texten verbreitet wurden**; darunter Militär- und Geheimdienstdatenbanken, Nationalausweisdaten, Facebook-Profile sowie Datensätze aus Telekom- und Hotelunternehmen – teils kostenlos, teils zum Kauf angeboten.

In diesem Zusammenhang konnte Democ einen **Datensatz verifizieren, der aus einem früheren großangelegten Facebook-Datenleak** stammt und nun erneut veröffentlicht wurde (Abb. 4). Er enthält u. a. **personenbezogene Daten israelischer Staatsbürger mit deutscher Staatsbürgerschaft, die in Deutschland leben**. Die gezielte Auswahl und Wiederverbreitung dieses Datensatzes im

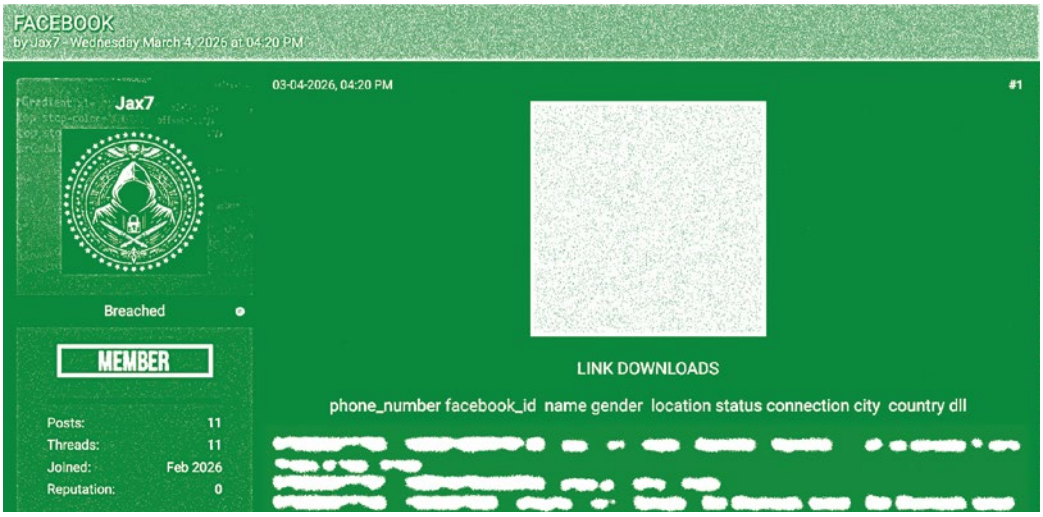


Abb. 4 Auszug eines Facebook-Datenleaks mit personenbezogenen Daten israelischer Staatsbürger. Die aktuelle Weiterverbreitung und Aufrufe, diese Informationen gegen »Zionisten« zu nutzen, macht Betroffene zum Ziel von Phishing, Einschüchterung und Doxxing.

Kontext von Aufrufen zur Nutzung »gegen Zionisten« macht die Betroffenen zu konkreten Zielen für Phishing, Einschüchterung und Doxxing.

Weitere dokumentierte Fälle, die auch deutsch-israelische Staatsbürger betreffen, sind **Malwarekampagnen über gefälschte Sicherheits-Apps** (Acronis Threat Research Unit 2026) sowie in der Vergangenheit verbreitete **verdächtige Websites zur Datensammlung über jüdische oder israelische Personen** (DOJLife 2025).

Insgesamt verdeutlichen diese Beispiele ein **wachsendes Bedrohungspotenzial für Institutionen und Einzelpersonen mit Israel- oder jüdischem Bezug – auch im deutschen Kontext**.

Hintergrund

Cyberoperationen sind zu einem zentralen Instrument geopolitischer Konflikte geworden und prägen seit Jahren die Auseinandersetzung zwischen Israel und Iran (Microsoft Threat Intelligence 2023; Mandiant / Google Cloud 2024 / Google Threat Analysis Group 2024).

Iran verfügt über ein wachsendes Cyberarsenal und nutzt sowohl staatliche Cybereinheiten als auch staatlich unterstützte Hackergruppen, die häufig in hybriden Strukturen mit Proxy-Akteuren und Hacktivisten operieren (CrowdStrike 2023). Parallel existiert ein transnationales Hacktivisten-Ökosystem, das über Plattformen wie Telegram und X mobilisiert wird (FalconFeeds 2026a). Die militärische Eskalation im Frühjahr 2026 hat diese Aktivitäten deutlich verstärkt.

Auch die aktuelle militärische Eskalation zwischen Israel, den USA und Iran wird von intensiven Cyberaktivitäten begleitet. Bis zum 12. März wurden insgesamt über 1.100 Cybervorfälle durch mehr als 70 Gruppen registriert – eine der größten bislang dokumentierten koordinierten Hacktivistenreaktionen (FalconFeeds 2026a, 2026b).

Parallel beobachteten Analysten eine verstärkte **Mobilisierung hacktivistischer Netzwerke** und die **intensive Nutzung sozialer Medien** zur Koordination sowie zur Verbreitung von Propaganda und Desinformation (Radware 2026; Sophos 2026).

Zu den **häufigsten Angriffsmethoden** zählen DDoS-Angriffe zur Störung digitaler Dienste sowie Website-Defacements (Verunstaltungen), mit politischen Botschaften (Recorded Future 2026; Radware 2026). Beide Methoden sind technisch leicht umzusetzen und erzeugen hohe mediale Aufmerksamkeit.

Die Gruppe **Handala**, die dem iranischen Geheimdienst MOIS zugerechnet wird, betreibt seit Oktober 2025 eine **Doxxing-Website** mit persönlichen Daten israelischer Sicherheitskräfte, verbunden mit **Kopfgeldern** von bis zu 50.000 USD für Hinweise auf deren Aufenthaltsort. Sicherheitsforscher sehen ein übertragbares Risiko für israelische Staatsbürger und jüdische Organisationen im Ausland (FalconFeeds 2026).

Neben öffentlich sichtbaren Angriffen spielen **verdeckte Operationen** wie Phishing und Social Engineering eine wichtige Rolle. Dazu gehören Spear-Phishing-E-Mails, gefälschte Websites oder manipulierte Apps, über die Schadsoftware verbreitet wird. Ein Beispiel ist eine Kampagne, bei der Malware über Apps verbreitet wurde, die sich als israelische Raketenwarnsysteme ausgaben (Acronis Threat Research Unit 2026).

Relevante staatlich unterstützte iranische Gruppen sind unter anderem APT42 / Charming Kitten (Social Engineering), MuddyWater (Spionage) und APT34 / OilRig (Angriffe auf staatliche und wirtschaftliche Infrastruktur) (BSI 2025).

Die **pro-russische Hackergruppe** NoName057(16) reklamierte 2024 und 2025 im Rahmen der Kampagne #OpGermany mehrere DDoS-Angriffe auf deutsche Behördenwebsites und beteiligte sich bereits in früheren Jahren gemeinsam mit pro-iranischen Gruppen an der Kampagne #OpIsrael gegen israelische Ziele (BKA 2025, KELA 2025). Am 2. März 2026 trat NoName057(16) formell der pro-iranischen Koalition bei – eine vollzogene Allianz, die den Angriffsradius auf Europa erheblich vergrößerte (Radware 2026; SOCRadar 2026).

Ideologisch motivierte Hacktivistennetzwerke koordinieren sich über Plattformen wie Telegram und verbreiten dort ihre angeblichen Angriffserfolge (Radware 2026). So kündigte am 1. März der Telegram-Kanal We are MONARCH eine »**Cyber-Operation Holocaust**« gegen israelische Militärserver an und behauptete, Israel betreibe einen »neuen Nazismus unter israelischer Flagge«. Die Kampagne ähnelt in der antisemitischen Rahmung stark der für den deutschen Kontext dokumentierten Kampagne »Operation Electronic Holocaust«.

Insgesamt zeigt das Lagebild, dass internationale Cyberkonflikte zunehmend auch antisemitische Bedrohungen im digitalen Raum erzeugen, die bis in den deutschen Kontext hineinreichen.

Quellen

Anomali (2026): *Israel in Focus: Iran Retaliatory Posture.* https://www.anomali.com/blog/israel-in-focus-iran-retaliatory-posture

Acronis Threat Research Unit (2026): *Mobile spyware campaign impersonates Red Alert rocket warning system.* https://www.acronis.com/en/tru/posts/mobile-spyware-campaign-impersonates-israels-red-alert-rocket-warning-system/

BKA (2025): *Bundeslagebild Cybercrime.* https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2024.html?nn=28110

BSI (2025): *Threat Intelligence – aktive APT-Gruppen.* https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html

DOJLife (2025): *URGENT Security Alert from Israeli Embassy: Do Not Use Suspicious Website.* https://www.dojlife.com/urgent-security-alert-from-israeli-embassy-do-not-use-suspicious-website

FalconFeeds 2026a: *Inside the Middle East's Cyber Shadow War: Mapping 72+ Pro-Iran and Anti-Iran Groups.* https://falconfeeds.io/blogs/inside-middle-east-cyber-shadow-war-pro-iran-anti-iran-threat-actor-mapping

FalconFeeds 2026b: *Mapping the Cyber Battlefield: Threat Actor Activity Across the Middle East.* https://falconfeeds.io/blogs/mapping-the-cyber-battlefield-middle-east-threat-actor-activity

Google Threat Analysis Group (2024): *Iranian backed group steps up phishing campaigns against Israel, U.S.* https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/

Handelsblatt (2025): *Justizsenatorin Badenberg wird Opfer einer Cyber-Attacke.* https://www.handelsblatt.com/politik/deutschland/berlin-justizsenatorin-badenberg-wird-opfer-einer-cyber-attacke/100149216.html

KELA (2025): *KELA Cybercrime Update: July 2025 Snapshot.* https://www.kelacyber.com/blog/kela-cybercrime-update-july-snapshot/

Mandiant / Google Cloud (2024): *Uncharmed: Untangling Iran's APT42 Operations.* https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations

Microsoft Threat Intelligence (2023): *Iran turning to cyber-enabled influence operations.* https://www.microsoft.com/en-us/security/security-insider/threat-landscape/iran-turning-to-cyber-enabled-influence-operations-for-greater-effect

Radware (2026): *Retaliatory Hacktivist DDoS Activity Following Operation Epic Fury/Roaring Lion.* https://www.radware.com/security/threat-advisories-and-attack-reports/ddos-activity-following-operation-epic-fury-roaring-lion/

Recorded Future (2026): *The Iran War: What You Need to Know.* https://www.recordedfuture.com/blog/ongoing-iran-conflict-what-you-need-to-know

RIAS (2025): *Antisemitische Vorfälle in Deutschland 2024.* https://report-antisemitism.de/documents/04-06-25_RIAS_Bund_Jahresbericht_2024.pdf

SOCRadar (2026): *Iran vs. Israel & US Cyber War 2026: Operation Epic Fury Threat Intelligence.* https://socradar.io/blog/cyber-reflections-us-israel-iran-war/

Sophos (2026): *Cyber advisory: increased cyber risk amid U.S.–Israel–Iran escalation.* https://www.sophos.com/en-us/blog/cyber-advisory-increased-cyber-risk-amid-u-s-israel-iran-escalation

Symantec (2026): *Seedworm: Iranian APT on Networks of U.S. Bank, Airport, Software Company.* https://www.security.com/threat-intelligence/iran-cyber-threat-activity-us

Tagesspiegel (2025): *Verfassungsschutz warnt vor Cyberangriffen in Deutschland.* https://www.tagesspiegel.de/politik/verfassungsschutz-warnt-vor-laufenden-cyberangriffen-in-deutschland-stehen-iranische-regimegegner-juden-und-nahost-experten-im-fokus-15073870.html

democ.de