RGe
ISSN: 2177-3246

ATAQUES CIBERNÉTICOS CONTRA O IRÃ: REVISÃO DOS PRINCIPAIS INCIDENTES E SEUS IMPACTOS ESTRATÉGICOS (2010–2026)

CYBERATTACKS AGAINST IRAN: A REVIEW OF KEY INCIDENTS AND THEIR STRATEGIC IMPACTS (2010–2026)

CIBERATAQUES CONTRA IRÁN: UN ANÁLISIS DE LOS INCIDENTES CLAVE Y SUS REPERCUSIONES ESTRATÉGICAS (2010-2026)

10.56238/revgeov17n6-037

Jovair Pazzini de Melo Souza
Mestrando em Ciências Militares
Instituição: Escola de Aperfeiçoamento de Oficiais (EsAO)
E-mail: pazzini.jovair@eb.mil.br

Carlos Henrique do Nascimento Barros
Doutor em Ciências Militares
Instituição: Escola de Comando e Estado-Maior do Exército (ECEME)
E-mail: carloshnbarros@gmail.com

João Marcos Barbosa Oliveira
Mestre em Ciências Militares
Instituição: Escola de Aperfeiçoamento de Oficiais (EsAO)
E-mail: barbosaoliveira.joao@eb.mil.br

Ismael Deus Marques
Mestre em Políticas Públicas e Governo
Instituição: Fundação Getulio Vargas (FGV)
E-mail: ismaeldmarques@gmail.com

Eduardo Stefani
Doutor em Informática e Gestão do Conhecimento
Instituição: Universidade Nove de Julho (UNINOVE)
E-mail: eduardo_stefani@outlook.com

RESUMO
Este artigo analisa a trajetória dos principais ataques cibernéticos sofridos pelo Irã entre os anos de 2010 e 2026. Por meio de uma revisão da literatura e de relatórios técnicos, o estudo mapeia incidentes, desde o surgimento do Stuxnet até operações militares integradas recentes. A pesquisa identifica que as ofensivas deixaram de focar exclusivamente no programa nuclear para atingir sistematicamente infraestruturas civis críticas, como os setores de energia, transportes e indústria pesada. Os resultados indicam que o ciberespaço consolidou-se como um domínio de guerra híbrida, funcionando tanto para a sabotagem técnica quanto como ferramenta de pressão psicológica e política sobre o Estado iraniano. A análise conclui que a vulnerabilidade a esses ataques atuou como um catalisador para o

desenvolvimento das capacidades defensivas e ofensivas do Irã, posicionando-o como uma potência cibernética emergente no cenário global.

Palavras-chave: Ciberguerra. Irã. Infraestrutura Crítica. Cibersegurança. Conflito Híbrido.

ABSTRACT
This article analyzes the trajectory of the main cyberattacks suffered by Iran between 2010 and 2026. Through a literature review and technical reports, the study maps emblematic incidents, ranging from the emergence of Stuxnet to recent integrated military operations. The research identifies that these offensives shifted from focusing exclusively on the nuclear program to systematically targeting critical civilian infrastructures, such as the energy, transport, and heavy industry sectors. The results indicate that cyberspace has established itself as a domain of hybrid warfare, serving both for technical sabotage and as a tool for psychological and political pressure on the Iranian state. The analysis concludes that the vulnerability to these attacks acted as a catalyst for the development of Iran's defensive and offensive capabilities, positioning the country as an emerging cyber power on the global stage.

Keywords: Cyber Warfare. Iran. Critical Infrastructure. Cybersecurity. Cyber Power. Hybrid Conflict.

RESUMEN
Este artículo analiza la trayectoria de los principales ciberataques sufridos por Irán entre 2010 y 2026. Mediante una revisión de la literatura y los informes técnicos, el estudio traza un mapa de los incidentes desde el surgimiento de Stuxnet hasta las recientes operaciones militares integradas. La investigación identifica que las ofensivas han cambiado su enfoque, pasando de atacar exclusivamente el programa nuclear a atacar sistemáticamente infraestructuras civiles críticas, como los sectores de energía, transporte e industria pesada. Los resultados indican que el ciberespacio se ha consolidado como un dominio de guerra híbrida, funcionando tanto para el sabotaje técnico como para ejercer presión psicológica y política sobre el Estado iraní. El análisis concluye que la vulnerabilidad a estos ataques actuó como catalizador para el desarrollo de las capacidades defensivas y ofensivas de Irán, posicionándolo como una potencia cibernética emergente en el escenario global.

Palabras clave: Guerra Cibernética. Irán. Infraestructura Crítica. Ciberseguridad. Conflicto Híbrido.

1 INTRODUÇÃO

A crescente centralidade do ciberespaço como domínio de disputa tem alterado a forma como os Estados empregam recursos de coerção, inteligência e defesa; nesse contexto, o Irã destaca-se como caso especialmente relevante, por ter sido alvo de operações cibernéticas altamente sofisticadas e por, em resposta, ampliar e consolidar suas capacidades ofensivas e defensivas (Freilich, 2024)

O ataque *Stuxnet*, revelado em 2010, é descrito como um dos primeiros casos de *malware* projetado para sabotar sistemas de controle industrial em instalações nucleares, provocando dano físico e sendo atribuído aos Estados Unidos e Israel. Operações deste tipo são frequentemente tratadas como marco da ciberguerra moderna, tornando o Irã um país frequentemente citado como exemplo de laboratório de táticas cibernéticas de alto impacto contra infraestruturas críticas (Tidy, 2026).

Na sequência, o Irã foi alvo de campanhas de espionagem em larga escala, entre as quais se destaca o uso do *malware Flame*, identificado em 2012 e descrito como uma ferramenta modular voltada à coleta de informações em amplo espectro de alvos, incluindo organizações governamentais, instituições acadêmicas e indivíduos em países do Oriente Médio (Gostev, 2012). Gostev relata ainda que o código foi empregado para registrar teclas, capturar telas, acionar microfones e exfiltrar grandes volumes de dados, compondo um quadro de vigilância prolongada sobre alvos em território iraniano e em países da região.

A literatura especializada destaca que a posição geopolítica do Irã, marcada por tensões persistentes com Estados Unidos, Israel e aliados regionais, contribui para que o país se torne alvo prioritário de operações cibernéticas, ao mesmo tempo em que impulsiona o desenvolvimento de suas próprias capacidades ofensivas (Freilich, 2024). Após 2010, Teerã acelerou a formulação de estratégias nacionais de cibersegurança, criou estruturas institucionais voltadas ao domínio cibernético e passou a integrar sistematicamente ferramentas digitais às suas respostas assimétricas frente a adversários militarmente superiores. Nesse contexto, compreender os últimos ataques cibernéticos sofridos pelo Irã é fundamental para analisar a dinâmica da ciberguerra e os impactos sobre a segurança regional no Oriente Médio.

Diante disso, este artigo tem como objetivo revisar, de forma narrativa, os principais ataques cibernéticos sofridos pelo Irã entre 2010 e 2026, com base em literatura acadêmica e fontes abertas. Busca-se, especificamente, atingir os seguintes objetivos: mapear os incidentes mais relevantes registrados no período, descrever seus alvos e efeitos conhecidos, com ênfase em infraestruturas críticas, e analisar, em perspectiva estratégica, de que modo esses ataques contribuíram para redefinir a postura iraniana em cibersegurança e defesa. Ao final, será apresentada uma representação estatística simples sobre a distribuição dos alvos atingidos, de modo a identificar quais setores iranianos foram mais frequentemente impactados por operações cibernéticas no recorte temporal considerado.

2 CIBERGUERRA E PODER CIBERNÉTICO NO CONTEXTO DO IRÃ

A consolidação do ciberespaço como contexto para a projeção de poder é frequentemente associada às suas características de baixo custo de entrada, assimetria de vulnerabilidades e ampliação do espaço de atuação para atores estatais e não estatais (Nye, 2010). Nesse ambiente, Nye (2010) destaca ainda que pequenas e médias potências, bem como grupos hacktivistas e organizações criminosas, podem influenciar, coagir ou desestabilizar adversários com investimentos significativamente menores do que aqueles exigidos em domínios tradicionais, como o marítimo ou o aéreo.

Parte da literatura argumenta que o grande número de operações frequentemente rotuladas como “ciberguerra” corresponde, na prática, a extensões digitais de práticas clássicas de sabotagem, espionagem e subversão, as quais não satisfazem os critérios tradicionais de guerra no que diz respeito à violência física direta (Rid, 2012). Ainda assim, o autor reconhece que tais mecanismos geram efeitos estratégicos significativos, especialmente se dirigidos a infraestruturas críticas ou integrados a campanhas militares amplas. Por esse motivo, propõe-se uma terminologia mais refinada como “operações cibernéticas”, englobando ações de espionagem, disrupção e influência, em substituição ao rótulo contestado de “guerra cibernética”.

Os trabalhos sobre segurança internacional destacam que a crescente dependência das sociedades modernas em relação às redes digitais e aos sistemas de informação expandiu a vulnerabilidade estatal a infraestruturas estratégicas (Nye, 2010). Setores vitais como energia, transporte, finanças e serviços essenciais operam hoje por meio de tecnologias de controle industrial fortemente conectadas; essa ampliação da superfície de ataque abre espaço para que operações cibernéticas provoquem não apenas a perda de dados, mas também impactos físicos diretos, interrupções prolongadas e efeitos em cascata sobre a economia e a ordem social (Freilich, 2024).

Em Estados submetidos a sanções e fortes pressões externas, a dimensão cibernética assume um caráter estratégico ainda mais sensível. Analisando o cenário do Oriente Médio, Freilich (2024) aponta que operações direcionadas a sistemas industriais, redes de transporte e cadeias de distribuição são empregadas como ferramentas de coerção e sinalização política, explorando o impacto direto que a interrupção de serviços básicos causa na população. Diante dessa vulnerabilidade, há uma clara convergência doutrinária que posiciona a proteção de infraestruturas críticas e a construção de resiliência cibernética como pilares centrais das estratégias de segurança nacional e defesa, especialmente em países inseridos em contextos de isolamento geopolítico, como o Irã (Freilich, 2024).

Relatórios de instituições de estudos estratégicos indicam que o Irã evoluiu, ao longo da última década e meia, de ator periférico para potência cibernética emergente. Embora permaneça abaixo do "primeiro escalão" ocupado por Estados Unidos, China e Rússia, o país posiciona-se à frente de muitos Estados em termos de organização e estratégia no domínio digital (Shafa, 2014). A literatura sugere

que, até o início da década de 2010, as capacidades iranianas eram frequentemente classificadas como de "terceiro nível", quadro que se alterou de forma acelerada após o impacto catalisador de operações como o Stuxnet.

Pesquisas sobre o desenvolvimento das capacidades cibernéticas iranianas apontam que a experiência do país como alvo de ataques sofisticados atuou como catalisador para um processo acelerado de construção de capacidades ofensivas e defensivas, incluindo a criação de estruturas dedicadas no Corpo de Guardas da Revolução Islâmica, na milícia Basij e na Organização de Defesa Passiva (Freilich, 2024). Nessa perspectiva, relatórios estratégicos caracterizam o Irã como detentor de um "programa cibernético ofensivo em amadurecimento", o qual adota a doutrina da "Resistência Cibernética Islâmica" para recorrer ao ciberespaço como um instrumento assimétrico fundamental, compensando a falta de opções de resposta militares convencionais face a adversários externos (CSIS, 2019).

Ao mesmo tempo, a condição do país como alvo recorrente de operações cibernéticas, em geral atribuídas a Estados Unidos, Israel e aliados, é apontada como fator que molda sua doutrina e seu padrão de atuação (Freilich, 2024). Nessa leitura, o Irã aparece simultaneamente como vítima de campanhas de sabotagem e espionagem de alta complexidade e como promotor de operações ofensivas contra adversários regionais e globais, configurando um ciclo de ação e reação que torna o caso iraniano especialmente fértil para o estudo da interação entre vulnerabilidade, aprendizado institucional e construção de poder cibernético (CSIS, 2019).

3 METODOLOGIA

O estudo adota o delineamento de revisão narrativa da literatura, adequado para o objetivo de integrar, de forma crítica, diferentes tipos de fontes sem seguir protocolos tão rígidos quanto os de revisões sistemáticas (Rother, 2007). O recorte temporal compreende o período de 2010 a 2026, por abranger desde a divulgação do ataque Stuxnet até o ciclo recente de operações contra infraestruturas civis iranianas, como combustíveis, transporte e indústria. Foram considerados apenas incidentes em que o Irã figura como alvo direto de operações cibernéticas, excluindo-se ações ofensivas atribuídas ao país.

A busca incluiu literatura científica em bases como *Scopus*, *Web of Science*, *IEEE Xplore* e *SciELO*, bem como relatórios técnicos de instituições especializadas em segurança e defesa, entre elas INSS, *Strategic Studies Institute* e CSIS, e documentos de empresas de segurança da informação (por exemplo, *Kaspersky*, *Microsoft*, *Radware*). Complementarmente, foram utilizadas reportagens de veículos jornalísticos reconhecidos para descrever incidentes específicos e refinar a linha do tempo dos eventos.

Os incidentes identificados foram organizados em um banco de dados próprio, com codificação de variáveis como ano, incidente, setor afetado, tipo de operação e suposta ou confirmada autoria, a partir de categorias amplas de infraestrutura crítica (nuclear; energia e combustíveis; transporte; indústria e manufatura; setor governamental; serviços digitais e comunicação).

4 PRINCIPAIS ATAQUES CIBERNÉTICOS SOFRIDOS PELO IRÃ (2010–2026)

O primeiro grande marco do período analisado é o ataque Stuxnet, revelado em 2010, frequentemente descrito como uma das primeiras operações cibernéticas conhecidas capazes de causar dano físico significativo em instalações industriais (Zetter, 2014). O alvo principal foi a usina de enriquecimento de urânio em Natanz, onde o malware teria manipulado a rotação de centrífugas utilizadas no processo de enriquecimento, levando à destruição de equipamentos e à redução temporária da capacidade nuclear iraniana (Shafa, 2014). Embora nenhum Estado tenha assumido publicamente a autoria, investigações técnico-forenses e análises de segurança internacional apontam, com elevado grau de consenso, para uma operação conjunta de Estados Unidos e Israel (Sanger, 2012).

Na sequência, o Irã foi alvo de campanhas de ciberespionagem em larga escala, entre as quais se destaca o uso do malware Flame, identificado em 2012 e descrito como uma plataforma modular de ataque voltada à coleta de informações em sistemas governamentais e infraestruturas estratégicas (Gostev, 2012). Relatos indicam que o código foi empregado para registrar teclas, capturar telas, acionar microfones e exfiltrar grandes volumes de dados, compondo um quadro de vigilância prolongada sobre alvos próximos ao programa nuclear e a outras áreas sensíveis (Wired, 2012). Essas operações reforçaram a percepção, em relatórios técnicos e estudos de segurança, de que o Irã funcionava como laboratório para o teste de capacidades cibernéticas avançadas associadas a Estados com elevada sofisticação tecnológica (Freilich, 2024).

Segundo Clayton (2012), servidores do Ministério do Petróleo e da Companhia Nacional de Petróleo do Irã foram atingidos por um vírus referido como “Viper”, que apagou dados em sistemas oficiais e derrubou os sites desses órgãos. No mesmo episódio, sistemas ligados às exportações, incluindo infraestruturas associadas à Ilha de Kharg, principal terminal de embarque do país, foram temporariamente desconectados da rede, e autoridades afirmaram que os dados principais permaneceram preservados e que as exportações de petróleo não foram interrompidas.

Nos anos seguintes, multiplicaram-se relatos de ataques a portos e órgãos governamentais. Em 2020, a infraestrutura do porto de Shahid Rajaee, em Bandar Abbas, foi alvo de intrusões atribuídas a Israel em resposta a tentativas iranianas de comprometer sistemas de água israelenses, gerando atrasos e desorganização nas operações logísticas, segundo fontes ocidentais (Nakashima, 2020). Autoridades iranianas minimizaram o impacto e falaram em tentativa "fracassada" de ataque, mas o incidente

reforçou a percepção de que hubs logísticos e portuários haviam se tornado alvos prioritários em um ciclo de ação e reação cibernética associado à disputa regional (USIP, 2022).

A partir de 2021, a atenção volta-se para infraestruturas civis de alto impacto social. Em julho daquele ano, um ataque à rede ferroviária iraniana provocou atrasos e paralisações em diversos trechos, em um incidente inicialmente descrito apenas como uma falha generalizada nos sistemas de controle (Naraine, 2021). Análises posteriores de amostras de malware associadas ao caso identificaram o uso de um wiper inédito, batizado de “Meteor” ou “MeteorExpress”, capaz de apagar arquivos, remover cópias de sombra, alterar credenciais e bloquear o acesso dos usuários, em uma cadeia de ataque que combinava múltiplos componentes e foi considerada tecnicamente sofisticada (Security Affairs, 2021; Naraine, 2021). O episódio reforçou a percepção de que sistemas de transporte terrestre podem ser alvo de operações destrutivas projetadas para causar disrupção ampla, mesmo sem dano físico direto à infraestrutura.

Em outubro de 2021, um novo ataque de grande escala atingiu o sistema de distribuição de combustíveis subsidiados, bloqueando o uso de cartões inteligentes em milhares de postos e exibindo mensagens de "cyberattack 64411" em bombas e painéis digitais (Reuters, 2021). Estimativas indicam que grande parte das estações de serviço do país ficou temporariamente impossibilitada de operar dentro do sistema de subsídios, gerando filas, desabastecimento localizado e forte repercussão interna (Reuters, 2021). A operação foi associada a um grupo hacktivista que posteriormente passaria a se identificar como *Predatory Sparrow*, frequentemente mencionado na literatura como exemplo de ator híbrido, com possíveis vínculos com serviços de inteligência estrangeiros (USIP, 2022).

O ano de 2022 marcou a transição para operações abertamente destrutivas contra a indústria pesada. Em junho, uma ofensiva cibernética contra siderúrgicas iranianas provocou, ao menos em um dos alvos, o derramamento de aço derretido e um incêndio em instalações industriais, com imagens de circuito interno mostrando trabalhadores deixando a área instantes antes da desestabilização súbita do processo (BBC, 2022). Relatos técnicos e análises posteriores indicam que o ataque comprometeu sistemas de controle industrial e desencadeou ações em momento inadequado, resultando em danos físicos significativos à planta (Greenberg, 2024). O grupo Predatory Sparrow reivindicou a ação e declarou ter planejado a operação de forma a evitar vítimas, declaração que levou parte da literatura a descrever o episódio como um exemplo de sabotagem “cirúrgica” contra infraestrutura crítica iraniana (BBC, 2022; Greenberg, 2024).

Além das infraestruturas estritamente econômicas, houve também ataques com forte impacto simbólico e político. Em 2021, um grupo que se autodenomina Adalat Ali divulgou vídeos obtidos por meio da invasão do sistema de vigilância da prisão de Evin, em Teerã, exibindo cenas de maus-tratos a presos e mensagens anunciando um “ciberataque” e conclamando a protestos (Zetter, 2021). O incidente expôs fragilidades na segurança de sistemas de câmeras e controle de instalações sensíveis e

foi amplamente interpretado como parte de um esforço para constranger o regime iraniano no plano interno e internacional (Zetter, 2021).

A partir de 2023, observa-se intensificação das operações contra infraestruturas civis, com destaque para a continuidade dos ataques ao sistema de combustíveis. Em dezembro de 2023, um ciberataque interrompeu o funcionamento de uma parcela substancial dos postos de gasolina do país, com o governo reconhecendo falhas generalizadas na rede de abastecimento e a paralisação de cerca de 70% das bombas, enquanto o grupo de hackers Gonjeshke Darande ("Predatory Sparrow"), associado por analistas a Israel, reivindicava a autoria da operação (Fritzhand, 2023).

Relatórios de empresas de segurança associam o episódio à mesma campanha que, em 2021, havia paralisado o sistema de subsídios de combustíveis, sugerindo um padrão de ataques recorrentes voltados a expor a vulnerabilidade do regime por meio da interrupção de serviços essenciais, sem necessariamente buscar a destruição permanente da infraestrutura física (Greenberg, 2024). Em análises estratégicas, esse tipo de operação é descrito como instrumento de pressão política e psicológica, destinada a evidenciar a incapacidade do Estado em garantir o funcionamento de serviços básicos (Freilich, 2024).

No limite superior do recorte, o período iniciado em fevereiro de 2026 representa um ponto de inflexão, marcado pela integração crescente entre operações cibernéticas e ofensivas militares convencionais. Em 28 de fevereiro de 2026, Estados Unidos e Israel lançaram uma campanha conjunta contra alvos militares, de inteligência e nucleares iranianos, designada como Operation Epic Fury na terminologia norte-americana e Roaring Lion na israelense (ICT, 2026).

Análises de centros de pesquisa e veículos especializados descrevem que, nas horas iniciais da operação, ofensivas cibernéticas e espaciais foram empregadas como movimentos iniciais, degradando comunicações, sensores e redes de comando iranianas antes do início dos ataques aéreos e de mísseis (Nextgov, 2026). Relatos indicam que, nesse contexto, a conectividade à internet no Irã teria caído a frações do tráfego normal, enquanto canais de televisão e plataformas digitais sofreram interferências e injeção de conteúdo psicológico voltado à confusão e à desmoralização (Tenable, 2026a).

Em resposta, atores cibernéticos associados ao Irã desencadearam, nos dias e semanas subsequentes, uma campanha de retaliação descrita por empresas de segurança como ofensiva híbrida coordenada (Tenable, 2026b). Essa campanha combinou ataques de negação de serviço distribuída, tentativas de intrusão em infraestruturas de energia, exploração massiva de câmeras IP para fins de reconhecimento e avaliação de danos, além de campanhas de ransomware e de wipers direcionadas a alvos em países aliados dos Estados Unidos e de Israel (Tenable, 2026b).

Relatórios recentes destacam que grupos tradicionalmente vinculados a estruturas estatais iranianas passaram a operar com maior frequência sob a aparência de infraestrutura cibercriminosa,

utilizando técnicas e canais próprios de grupos de crime organizado para dificultar a atribuição direta ao Estado (Flashpoint, 2026).

Segundo a Tenable (2026b), essa sequência de eventos reforça a interpretação de que, em 2026, o teatro cibernético relacionado ao Irã deixa de ser apenas um espaço de sabotagens discretas e campanhas de espionagem, consolidando-se como componente estrutural de uma guerra híbrida em grande escala. De um lado, o país continua a ser alvo de operações altamente sofisticadas, capazes de paralisar setores inteiros de sua infraestrutura crítica e degradar, em curto prazo, sua capacidade de comando e controle; de outro, mantém e emprega ativamente um ecossistema de atores cibernéticos estatais e paraestatais responsáveis por uma combinação de operações de espionagem, ataques destrutivos e campanhas de influência destinadas a projetar poder e impor custos a adversários regionais e globais (CSIS, 2019).

5 PADRÕES DE ALVOS, ATRIBUIÇÃO E IMPACTOS ESTRATÉGICOS

Os casos mapeados indicam que os ataques cibernéticos sofridos pelo Irã entre 2010 e 2026 concentram-se em infraestruturas críticas civis e estratégicas, com ênfase em setores de energia e combustíveis, transporte, indústria pesada e instalações governamentais sensíveis (CSIS, 2019). Embora o *Stuxnet* permaneça como exemplo emblemático de sabotagem a instalações nucleares, incidentes posteriores deslocam o foco para alvos cuja interrupção produz efeitos sociais e econômicos imediatos, como postos de gasolina, ferrovias, portos e siderúrgicas (USIP, 2022).

Os ataques contra o sistema de combustíveis, em especial os episódios de 2021 e 2023, ilustram essa lógica de pressão sobre a população e sobre a capacidade do Estado de prover serviços básicos, explorando o caráter sensível do subsídio à gasolina na política doméstica iraniana (Reuters, 2021; Fritzhand, 2023). De modo semelhante, as operações contra a rede ferroviária e o porto de Shahid Rajaee evidenciam a vulnerabilidade de cadeias logísticas e de transporte, com potencial para gerar atrasos, perdas econômicas e efeitos reputacionais, ainda que os danos materiais diretos sejam, em alguns casos, limitados (Naraine, 2021; Nakashima, 2020).

A dimensão simbólica e política também é marcante em incidentes como o vazamento de imagens da prisão de Evin, nos quais o objetivo principal parece ser a exposição de abusos e a erosão da legitimidade interna e externa do regime, mais do que a destruição de ativos físicos (Zetter, 2021). Nessas operações, a intrusão em sistemas de vigilância é combinada à divulgação orquestrada de conteúdo, aproximando-se de estratégias de guerra de informação e de operações psicológicas (Zetter, 2021).

Do ponto de vista da atribuição, os casos analisados sugerem um padrão em que alguns incidentes são amplamente associados, em fontes abertas, a Estados específicos, como no caso de *Stuxnet*, frequentemente atribuído a Estados Unidos e Israel, enquanto outros permanecem

oficialmente ambíguos, operando sob a "máscara" de *grupos* hacktivistas ou coletivos aparentemente autônomos (Sanger, 2012). O grupo *Predatory Sparrow*, em particular, surge recorrentemente ligado a ataques contra siderúrgicas, sistema de combustíveis e instituições financeiras, sendo descrito por vários analistas como um ator híbrido, situado na interseção entre hacktivismo e operações estatais (Greenberg, 2024). Essa opacidade deliberada quanto à autoria reforça a dificuldade de atribuição típica do domínio cibernético e funciona, ao mesmo tempo, como mecanismo de gestão de riscos de escalada entre Estados (CSIS, 2019).

A Operação *Epic Fury/Roaring Lion*, em 2026, representa um avanço na integração entre operações cibernéticas e ofensivas militares convencionais. Relatos indicam que, nas fases iniciais da campanha, foram conduzidas ofensivas cibernéticas e espaciais visando degradar comunicações, sensores e redes de comando iranianas, seguidas por ataques com mísseis e aviões tripulados e não tripulados (Nextgov, 2026). Essa sequência, descrita em relatórios como "ciberataque como prelúdio de ataque cinético", consolida o uso do ciberespaço como primeiro vetor de choque em campanhas de alta intensidade, indo além do padrão de ações discretas observado em anos anteriores (ICT, 2026).

Do lado iraniano, a reação à *Epic Fury* inclui uma campanha de retaliação que combina ataques de negação de serviço, tentativas de intrusão em infraestruturas de energia e campanhas de ransomware e wiper contra alvos em países aliados dos Estados Unidos e de Israel, o que tem sido descrito por empresas de segurança como "ofensiva híbrida coordenada" (Tenable, 2026). A literatura recente destaca que grupos tradicionalmente vinculados a órgãos estatais iranianos passaram a operar com maior frequência sob a aparência de infraestrutura cibercriminosa, utilizando técnicas e canais do crime organizado para diluir a responsabilidade direta do Estado (Flashpoint, 2026). Isso reforça a característica de "negação plausível" como elemento central na estratégia cibernética iraniana.

Em termos estratégicos, o conjunto de ataques analisados sugere que o Irã ocupa simultaneamente as posições de alvo recorrente e de protagonista ativo em um ciclo de ação e reação cibernética que envolve potências regionais e globais (CSIS, 2019). O país é alvo de operações sofisticadas que degradam sua capacidade de comando e controle e atingem setores sensíveis da economia, ao mesmo tempo em que responde com campanhas ofensivas e de influência que buscam impor custos a adversários e fortalecer sua posição como potência cibernética emergente (Shafa, 2014).

5.1 DISTRIBUIÇÃO SETORIAL DOS INCIDENTES MAPEADOS

Considerando o conjunto de principais incidentes sintetizados neste estudo, selecionados pela relevância estratégica e pelo nível de documentação disponível em fontes abertas, observa-se predominância de ataques contra setores de energia e combustíveis, transporte, indústria pesada e instalações governamentais sensíveis. Ainda que o número total de casos analisados seja limitado e

não pretenda esgotar o universo de operações cibernéticas contra o Irã, ele permite identificar algumas tendências relevantes.

No subconjunto de incidentes mapeados, os ataques contra energia e combustíveis aparecem de forma recorrente, abrangendo a sabotagem de instalações de petróleo em 2012, a paralisação do sistema de subsídios em 2021 e a interrupção da rede de postos de gasolina em 2023, enquanto os setores de transporte e logística, representados pela rede ferroviária e pelo porto de Shahid Rajaee, também se destacam como alvos preferenciais, refletindo a importância desses nós para a economia e para a projeção regional do Irã (Greenberg, 2021; Zetter, 2021; Security Affairs, 2022; BBC, 2021).

Em janeiro de 2024, a plataforma privada de transporte e tecnologia *Snapp* (incluindo sua subsidiária de *delivery SnappFood*) sofreu um massivo vazamento de dados que resultou na exfiltração e comercialização ilícita de sua base de dados no mercado negro. A intrusão, atribuída a um ator cibercriminoso de motivação puramente financeira e não identificado publicamente, comprometeu informações cadastrais sensíveis, credenciais de acesso, detalhes de pagamento e registros de viagens de cerca de 80 milhões de cidadãos iranianos, evidenciando as profundas fragilidades de segurança digital mesmo em grandes conglomerados do setor privado do país (Iran International, 2025).

Em fevereiro de 2024, a Assembleia Consultiva Islâmica (o Parlamento do Irã) foi alvo de uma invasão cibernética altamente prejudicial direcionada aos seus sistemas governamentais e legislativos, reivindicada pelo grupo hacktivista de oposição "*Rebellion Until Overthrow*" (vinculado ao grupo exilado MEK/PMOI). A operação do tipo *hack-and-leak* causou sabotagem operacional direta ao desativar o painel eletrônico de votação interna, forçando os parlamentares a realizarem sessões fechadas e votações manuais, e vazou uma vasta quantidade de e-mails e documentos oficiais confidenciais que detalhavam as táticas estatais de controle, censura da internet e vigilância de opositores (IranWire, 2024).

Em junho de 2025, ocorrendo em paralelo com picos de hostilidades cinéticas na região, o grupo hacker pró-Israel *Predatory Sparrow* (*Gonjeshke Darande*) executou uma campanha de sabotagem cibernética contra o núcleo financeiro e de criptoativos do Irã, tendo como alvos o estatal *Bank Sepah* e a *Nobitex*, a maior corretora de criptomoedas do país. Os invasores desdobraram um malware destrutivo do tipo *wiper* para paralisar as operações de atendimento físico, caixas eletrônicos e processamento de salários militares do Bank Sepah, enquanto violavam as carteiras virtuais (*hot wallets*) da Nobitex para confiscar e permanentemente inutilizar ("queimar") cerca de 90 milhões de dólares em stablecoins que eram utilizadas pelo regime para contornar sanções globais e financiar forças aliadas (Elliptic, 2025).

Infraestruturas industriais e militares aparecem em menor número de casos, mas com alto impacto potencial, como nos ataques às siderúrgicas em 2022 e na campanha integrada de 2026, que atingiu instalações das forças armadas, da inteligência e do programa nuclear (BBC, 2022; ICT, 2026).

Ao mesmo tempo, incidentes dirigidos a órgãos governamentais e a sistemas de vigilância, como o comprometimento das câmeras da prisão de Evin, evidenciam a dimensão simbólica e informacional da disputa, voltada à exposição de abusos e à erosão da confiança no regime (Zetter, 2021).

De maneira sintética, o Quadro 1 apresenta os principais ataques considerados, indicando o setor afetado, o tipo de operação e a atribuição predominante em fontes abertas:

QUADRO 1 – Principais ataques cibernéticos sofridos pelo Irã e setores afetados (2010–2026).

Ano	**Incidente**	**Setor principal**	**Tipo de operação**	**Atribuição predominante**
2010	Stuxnet (Natanz)	Nuclear/ indústria	Sabotagem a ICS/SCADA, dano físico	EUA e Israel (atribuição amplamente aceita) (Sanger, 2012)
2012	"Viper" – Ministério do Petróleo	Energia e combustíveis	Ataque a sistemas de TI, wiper	Autor desconhecido, suspeita de ator estatal (Reuters, 2012)
2012	Flame	Governamental/inteligência	Espionagem em larga escala	Campanha ligada a mesmos ecossistemas de Stuxnet/Duqu (Gostev, 2012)
2020	Ataque ao porto de Shahid Rajaee	Transporte/ logística	Disrupção de operações portuárias	Israel (fontes ocidentais); minimizado por Teerã (Nakashima, 2020)
2021	Ataque à rede ferroviária ("Meteor")	Transporte terrestre	Wiper e sabotagem de sistemas de gestão	Grupo de APT não identificado; suspeita de ator estatal (Naraine, 2021)
2021	Ataque ao sistema de combustíveis	Energia e combustíveis	Ataque a sistema de subsídios e POS	Grupo hacktivista ligado a Predatory Sparrow (Reuters, 2021)
2021	Vazamento de imagens da prisão de Evin	Governamental/simbólico	Intrusão em CFTV e divulgação de vídeos	Grupo Adalat Ali (Zetter, 2021)
2022	Ataques às siderúrgicas	Indústria pesada/ manufatura	Sabotagem a ICS com dano físico	Predatory Sparrow (BBC, 2022)
2023	Ataque à rede de postos de gasolina	Energia e combustíveis	Disrupção da rede de abastecimento	Grupo ligado a Predatory Sparrow, com suspeita de apoio estatal (Reuters, 2023)
2024	Vazamento de dados da plataforma Snapp	Transporte e Tecnologia (Serviço Privado)	Exfiltração e comercialização ilícita de banco de dados.	Ator cibercriminoso financeiro não identificado.

Ano	Incidente	Setor principal	Tipo de operação	Atribuição predominante
2024	Invasão de sistemas eleitorais	Governamental / Legislativo	Sabotagem operacional de sistemas internos e vazamento direcionado de dados (Hack-and-leak).	Grupo hacktivista de oposição "Rebellion Until Overthrow" (vinculado ao MEK/PMOI).
2025	Sabotagem destrutiva à infraestrutura de bancos	Financeiro (Bancário e Criptoativos).	Sabotagem operacional via *wiper malware* e destruição lógica de fundos financeiros em stablecoins.	Grupo pró-Israel Predatory Sparrow (Gonjeshke Darande).
2026	Operação Epic Fury/Roaring Lion (fase cyber)	Militar/defesa/ múltiplos setores	Campanha integrada de degradação de C2, telecom e sensores	EUA e Israel (operações declaradas em contexto de conflito) (ICT, 2026)

Fonte: os autores.

Essa síntese reforça que, mesmo em um conjunto reduzido de casos, a maior parte dos ataques se concentra em infraestruturas civis estratégicas, especialmente energia/combustíveis e transporte, enquanto alvos nucleares e militares aparecem em momentos de maior escalada, como em 2010 e 2026. Isso corrobora a leitura de que a ciberguerra travada em torno do Irã combina, de forma crescente, instrumentos de coerção econômica e social com operações de degradação militar de alta intensidade.

6 CONCLUSÃO

A análise dos incidentes ocorridos entre 2010 e 2026 revela uma transformação na natureza das hostilidades no ciberespaço iraniano. O que começou como uma operação de sabotagem industrial altamente específica e silenciosa, exemplificada pelo *Stuxnet*, evoluiu progressivamente para um padrão de ataques recorrentes contra serviços essenciais que afetam diretamente o cotidiano da população civil. Essa trajetória confirma o primeiro objetivo proposto pelo estudo: o mapeamento dos incidentes demonstrou que as operações não seguiram uma lógica aleatória, mas uma escalada deliberada em termos de alvos, impacto social e grau de integração com outras formas de conflito.

A descrição dos alvos e efeitos evidenciou que a transição para infraestruturas como redes de combustíveis, sistemas de transporte e instalações industriais reflete o uso do ciberespaço como instrumento de coerção social. Ao expor a incapacidade do regime iraniano de manter serviços básicos operacionais, essas operações produzem efeitos que transcendem o dano técnico imediato, atingindo a legitimidade política do Estado perante sua própria população. O caso da prisão de Evin reforça essa

dimensão: a ciberguerra travada em torno do Irã não se limita à sabotagem de infraestruturas físicas, mas inclui operações de exposição, desmoralização e guerra de informação.

Em perspectiva estratégica, o ciclo de ataques sofridos pelo Irã consolidou o domínio digital como vetor primário dos conflitos modernos na região. A Operação *Epic Fury*, em 2026, representou um ponto de inflexão, onde pela primeira vez no contexto iraniano, ofensivas cibernéticas e cinéticas foram executadas de forma plenamente integrada, com o ciberespaço funcionando como primeiro escalão de uma campanha militar convencional.

Paradoxamente, essa condição de alvo prioritário forçou o Irã a acelerar sua maturidade institucional e técnica, transformando vulnerabilidades em aprendizado estratégico e posicionando-o como potência cibernética emergente. O caso iraniano ilustra, portanto, como potências médias submetidas a pressões externas e sanções persistentes podem empregar o ciberespaço para compensar assimetrias militares convencionais, transformando a defesa reativa em dissuasão ativa e projeção de poder regional.

Algumas limitações do presente estudo merecem reconhecimento, pois, grande parte das informações disponíveis sobre operações cibernéticas provém de fontes abertas, relatórios técnicos, cobertura jornalística e documentos institucionais, cuja confiabilidade varia e cuja capacidade de confirmar a autoria é, por definição, limitada. A atribuição de ataques a Estados ou grupos específicos permanece, em muitos casos, probabilística e contestada.

Para pesquisas futuras, recomenda-se o aprofundamento comparativo com outros casos de Estados em posição estratégica semelhante à do Irã, submetidos a sanções, com capacidades militares convencionais inferiores às de seus adversários e com histórico de uso assimétrico do ciberespaço, como Coreia do Norte e Venezuela. A análise dos impactos de longo prazo das operações de 2026 sobre a doutrina cibernética iraniana constitui outro caminho promissor, especialmente à medida que novos documentos e relatórios técnicos se tornarem disponíveis.

REFERÊNCIAS

BBC NEWS. Predatory Sparrow: Did hackers start this steel factory fire in Iran? BBC News Technology, 10 jul. 2022. Disponível em: https://www.bbc.com/news/technology-62099474. Acesso em: 6 abr. 2026.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. Iran and Cyber Power. Washington, DC: CSIS, 2019. Disponível em: https://www.csis.org/analysis/iran-and-cyber-power. Acesso em: 8 abr. 2026.

CLAYTON, Mark. Latest cyberattack on Iran targets oil export facilities. The Christian Science Monitor, 23 abr. 2012. Disponível em: https://www.csmonitor.com/USA/2012/0423/Latest-cyberattack-on-Iran-targets-oil-export-facilities. Acesso em: 25 maio 2026.

ELLIPTIC. Iranian Crypto Exchange Nobitex Hacked for Over $90 Million by Pro-Israel Group. London: Elliptic, 18 jun. 2025. Disponível em: https://cyberlaw.ccdcoe.org/wiki/Predatory_Sparrow%E2%80%99s_operations_against_Iranian_financial_cyber_infrastructure_(2025). Acesso em: 22 maio 2026.

FLASHPOINT. Escalation in the Middle East: Tracking "Operation Epic Fury" across military and cyber domains. Flashpoint, 5 maio 2026. Disponível em: https://flashpoint.io/blog/escalation-in-the-middle-east-operation-epic-fury/. Acesso em: 4 abr. 2026.

FREILICH, C. The Iranian Cyber Threat. INSS Memorandum 230. Tel Aviv: Institute for National Security Studies, 2024. Disponível em: https://www.inss.org.il/wp-content/uploads/2024/02/Memo230_IranianCyberThreat_ENG_digital.pdf. Acesso em: 7 abr. 2026.

GOSTEV, A. The Flame: Questions and Answers. Securelist/Kaspersky Lab, 28 maio 2012. Disponível em: https://securelist.com/the-flame-questions-and-answers/34344/. Acesso em: 3 abr. 2026.

GREENBERG, A. How a group of Israel-linked hackers has pushed the limits of cyberwar. Wired, 25 jan. 2024. Disponível em: https://www.wired.com/story/predatory-sparrow-cyberattack-timeline/. Acesso em: 16 abr. 2026.

IRANWIRE. Iranian Lawmakers Hold Closed-Door Session After Hack.14 fev. 2024. Disponível em: https://iranwire.com/en/news/125356-iranian-lawmakers-hold-closed-door-session-after-hack/. Acesso em: 22 maio 2026.

IRAN INTERNATIONAL. Iran interrogating software firm at epicenter of 'worst-ever' bank hack. 6 set. 2024. Disponível em: https://www.iranintl.com/en/202409048166. Acesso em: 22 maio 2026.

INTERNATIONAL INSTITUTE FOR COUNTER-TERRORISM (ICT). Operations "Epic Fury" & "Roaring Lion". Herzliya: ICT, 2026. Disponível em: https://ict.org.il/operations-epic-fury-roaring-lion/. Acesso em: 7 abr. 2026.

NARAINE, R. Researchers link mysterious 'MeteorExpress' wiper to Iranian train cyberattack. SecurityWeek, 29 jul. 2021. Disponível em: https://www.securityweek.com/researchers-link-mysterious-meteorexpress-wiper-iranian-train-cyberattack/. Acesso em: 6 abr. 2026.

NAKASHIMA, E. Officials: Israel linked to a disruptive cyberattack on Iranian port facility. The Washington Post, 18 maio 2020. Disponível em: https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html. Acesso em: 9 abr. 2026.

NEXTGOV/FCW. How Cyber Command contributed to Operation Epic Fury against Iran. Nextgov/FCW, 3 mar. 2026. Disponível em: https://www.nextgov.com/cybersecurity/2026/03/how-cyber-command-contributed-operation-epic-fury-against-iran/411818/. Acesso em: 5 abr. 2026.

NYE, J. S. Jr. Cyber Power. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010. Disponível em: https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/cyber-power.pdf. Acesso em: 6 abr. 2026.

REUTERS. Iran says cyberattack causes widespread disruption at gas stations. Euronews, 27 out. 2021. Disponível em: https://www.euronews.com/next/2021/10/27/iran-gasoline-cyberattack. Acesso em: 12 abr. 2026.

FRITZHAND, Troy O. Israel-linked hackers claim cyberattack that shuts down 70% of Iran's gas stations. Algemeiner, 18 dez. 2023. Disponível em: <https://www.algemeiner.com/2023/12/18/israel-linked-hackers-claim-cyberattack-shuts-down-70-irans-gas-stations/>. Acesso em: 13 abr. 2026.

RID, T. Cyber war will not take place. Journal of Strategic Studies, Londres, v. 35, n. 1, p. 5-32, fev. 2012. DOI: 10.1080/01402390.2011.608939.

ROTHER, E. T. Revisão sistemática X revisão narrativa. Acta Paulista de Enfermagem, São Paulo, v. 20, n. 2, p. v-vi, 2007. Disponível em: https://www.scielo.br/j/ape/a/z7zZ4Z4GwYV6FR7S9FHTByr/?lang=pt. Acesso em: 15 abr. 2026.

SANGER, D. E. Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power. New York: Crown/Random House, 2012.

SECURITY AFFAIRS. Iran railway attack: Meteor wiper linked to the incident. Security Affairs, jul. 2021. Disponível em: https://securityaffairs.com/120679/malware/meteor-wiper-irans-national-railway.html. Acesso em: 16 abr. 2026. - mudar para

SHAFA, E. K. Iran's Emergence as a Cyber Power. Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2014. Disponível em: https://ssi.armywarcollege.edu/SSI-Media/Recent-Publications/Article/3614420/irans-emergence-as-a-cyber-power/. Acesso em: 12 abr. 2026.

TENABLE. Operation Epic Fury: Potential Iranian cyber counteroffensive operations. Tenable Blog, 3 mar. 2026. Disponível em: https://www.tenable.com/blog/operation-epic-fury-potential-iranian-cyber-counteroffensive-operations. Acesso em: 6 abr. 2026. (Tenable, 2026a).

TENABLE. Iranian-linked actors are engaging in disruptive attacks. Tenable Blog, 11 mar. 2026. Disponível em: https://www.tenable.com/blog/cyber-retaliation-analyzing-iranian-cyber-activity-following-operation-epic-fury. Acesso em: 6 abr. 2026. (Tenable, 2026b).

THE IRAN PRIMER (USIP). The Invisible U.S.-Iran Cyber War. Washington, DC: United States Institute of Peace, 2022. Disponível em: https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war. Acesso em: 6 abr. 2026.

TIDY, J. What role has cyber warfare played in Iran? BBC News, 12 mar. 2026. Disponível em: https://www.bbc.com/news/articles/c5yr0576ygvo. Acesso em: 4 abr. 2026.

WIRED. Meet 'Flame,' the massive spy malware infiltrating Iranian computers. Wired, 28 maio 2012. Disponível em: https://www.wired.com/2012/05/flame/. Acesso em: 2 abr. 2026.

ZETTER, K. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown Publishing Group, 2014.

ZETTER, K. Hackers leak surveillance camera videos purportedly taken from inside Iran's Evin Prison. Zetter Zero Day, 24 ago. 2021. Disponível em: https://www.zetter-zeroday.com/hackers-leak-surveillance-camera/. Acesso em: 2 abr. 2026.