Um ataque cibernético pode ser usado para matar pessoas ou populações inteiras?

Autores: Marcelo Branquinho e Plataforma Safer

25/07/2025

Resumo: Este artigo explora se ataques cibernéticos podem resultar em danos físicos graves, incluindo mortes de indivíduos ou até populações inteiras. Com a crescente digitalização de sistemas médicos, veículos e infraestrutura crítica, há uma preocupante convergência entre o mundo virtual e o mundo físico. Discutimos vulnerabilidades em dispositivos médicos conectados (parte da Internet das Coisas), em veículos modernos e autônomos, e em serviços públicos como o abastecimento de água e energia. São apresentados casos reais e estudos que demonstram como invasões digitais já *colocaram vidas em risco*, desde um hacker que quase envenenou a água de uma cidade, até falhas de segurança em marcapassos e bombas de insulina que poderiam ser exploradas para causar morte de pacientes. Também examinamos ataques cibernéticos contra redes elétricas e instalações industriais que, embora não intencionalmente letais em todos os casos conhecidos, evidenciam o potencial de consequências catastróficas. Por fim, o artigo discute as principais técnicas de ataque usadas e as falhas exploradas, ressaltando a importância de reforçar a segurança cibernética em sistemas cuja falha pode resultar em perdas de vidas humanas.

Palavras-chave: Segurança Cibernética; Infraestrutura Crítica; Internet das Coisas; Dispositivos Médicos; Veículos Autônomos; Água e Saneamento; Ciberataques Físicos.

POWERED BY SAFER

Introdução

A integração ubiqua de tecnologia digital em dispositivos do cotidiano traz benefícios enormes, mas também riscos antes inimagináveis. Tradicionalmente, ataques cibernéticos eram associados a roubo de dados, fraude financeira ou interrupção de serviços de informática. No entanto, à medida que computadores passam a controlar **dispositivos físicos** – como bombas de insulina, freios de carros ou válvulas de usinas – surge a possibilidade real de um ataque digital causar **danos corporais ou mortes** no mundo real. Em outras palavras, hackers podem transformar bits e bytes em armas tangíveis. Mas *até que ponto um ataque cibernético pode realmente matar pessoas ou mesmo grupos populacionais inteiros?* Nesta introdução, apresentamos uma visão geral dessa questão inquietante, preparando o terreno para discutir exemplos práticos e evidências documentadas.

Nos últimos anos, pesquisadores e órgãos de segurança vêm alertando que **ciberataques podem ter consequências cinéticas**, ou seja, físicas. A expressão "ciber-físico" passou a designar sistemas em que o componente informático controla processos físicos críticos. Isso inclui desde equipamentos médicos implantáveis, veículos modernos cheios de sensores e atuadores, até infraestruturas públicas como redes elétricas e sistemas de abastecimento de água. A ameaça não é meramente teórica: há casos *reais* documentados de ataques ou falhas de segurança que, se explorados com intenção maliciosa, poderiam causar ferimentos ou óbitos. Este artigo examinará esses cenários em detalhes, abordando: (1) Dispositivos médicos conectados (Internet das Coisas médica) vulneráveis a ataques; (2) Veículos e transportes autônomos suscetíveis à invasão digital; (3) Sistemas de água potável e saneamento que podem ser sabotados; e (4) Outras infraestruturas críticas, como rede elétrica e instalações industriais, que podem amplificar efeitos de um ataque cibernético a nível populacional.

Dispositivos médicos conectados e vulneráveis (IoT médico)

A medicina moderna depende cada vez mais de dispositivos eletrônicos conectados – sejam **marcapassos** (pacemakers) implantados, **bombas de insulina** eletrônicas ou outros aparelhos

hospitalares em rede. Esses dispositivos salvam vidas, mas, se não forem seguros, podem se tornar armas involuntárias. Em 2017, quase **meio milhão de marcapassos** fabricados pela Abbott (St. Jude Medical) tiveram de receber uma atualização emergencial de firmware após a FDA dos EUA identificar que hackers poderiam invadir o dispositivo à distância para **alterar os batimentos cardíacos ou descarregar a bateria**, potencialmente levando pacientes à morte. Essa medida preventiva ilustra uma realidade preocupante: as vulnerabilidades digitais não são apenas falhas técnicas, mas brechas com impacto direto na saúde humana.

Felizmente, até o momento não há casos confirmados de assassinato deliberado via hack de dispositivos médicos. Contudo, **pesquisas de segurança** demonstraram em laboratório que isso é possível. Em 2018, um relatório destacou que embora *ninguém (até onde se sabe) tenha sido morto por invasão de marcapasso ou bomba de insulina, vários pesquisadores já provaram ser viável* realizar tal ataqueglobalnetwork.io. Por exemplo, em 2019 especialistas em segurança exibiram um aplicativo capaz de invadir remotamente certas **bombas de insulina Medtronic** e administrar doses letais de insulina ou bloquear sua liberação, causando hipoglicemia ou hiperglicemia fataiswired.com. Os pesquisadores Billy Rios e Jonathan Butts criaram essa prova de conceito extrema depois de meses alertando a fabricante e reguladores sem obter ação efetiva. A falha explorada era relativamente simples: as comunicações sem fio entre o controle remoto e a bomba **não eram criptografadas nem autenticadas**, permitindo que um atacante enviasse comandos falsos à bombawired.com. Essa demonstração forçou a fabricante a recolher ou substituir os modelos vulneráveis, evidenciando que *uma brecha cibernética pode literalmente ter consequências mortais*.

Outras vulnerabilidades médicas chamaram atenção. Marcapassos e desfibriladores implantáveis já tiveram comunicações sem fio interceptadas em pesquisas, levantando temores de **"assassinato digital"** – preocupação essa que levou, por exemplo, os médicos do ex-vice-presidente dos EUA **Dick Cheney** a desativar o recurso wireless do seu desfibrilador cardíaco por precaução contra hackers. Também hospitais foram alvos indiretos: ataques de **ransomware** (sequestro de

dados) em redes hospitalares causaram interrupções de atendimento; em 2020, um hospital na Alemanha não pôde aceitar um paciente em estado crítico devido a sistemas fora do ar, e a paciente faleceu após desvio – possivelmente a primeira morte ligada a um ciberataque em setor de saúde. Esses incidentes, diretos ou indiretos, reforçam que dispositivos e sistemas médicos inseguros representam uma nova fronteira de risco. É crucial que fabricantes fortaleçam a **segurança de IoT médico**, pois do contrário um hacker habilidoso poderia literalmente transformar aparelhos de suporte à vida em agentes de morte.

Veículos conectados e transporte autônomo

Os automóveis modernos são essencialmente **redes de computadores sobre rodas**. Sistemas de infotainment conectados à internet, sensores e atuadores controlados por software e, no caso de veículos autônomos, inteligência artificial guiando decisões de direção – tudo isso expande a superfície de ataque. Em 2015, dois pesquisadores (Charlie Miller e Chris Valasek) demonstraram de forma dramática a invasão remota de um **Jeep Cherokee** em movimento, controlado à distância via internet. Eles exploraram uma vulnerabilidade no sistema de entretenimento Uconnect do veículo, conseguindo enviar comandos do laptop para o ônibus de controle interno (CAN bus) do carro. Na prática, foi possível acionar freios, desligar o motor e até alterar a direção do volante sem qualquer intervenção do motorista. O jornalista da *Wired* que voluntariamente dirigiu o Jeep enquanto era "hackeado" relatou o terror de ter o carro subitamente paralisado em plena rodovia, sem conseguir retomar o controle, enquanto caminhões se aproximavam buzinandowired.com. Felizmente, esse experimento controlado não causou acidentes, mas provou que *um ataque cibernético pode, sim, colocar vidas em risco nas estradas*.

A repercussão foi imediata. Dias após a divulgação, a montadora Fiat-Chrysler **emitou um recall de 1,4 milhão de veículos** para corrigir a falha de software explorada pelos pesquisadoreswired.com. Esse caso emblemático revelou como **veículos conectados podem ser**

vulneráveis: a falha permitia acesso remoto via rede celular ao módulo de infotainment, e deste ao sistema crítico do carro, devido à falta de segregação adequada entre as redes interna e externa do veículo. Em outras palavras, algo tão simples quanto o rádio conectado tinha portas abertas para a internet que davam passagem até os freios – uma falha de arquitetura grave de segurança.

Os carros autônomos e sistemas de transporte inteligentes ampliam ainda mais o potencial de ataques com consequências físicas. Imagine frotas de **carros autônomos** hackeados simultaneamente para acelerarem ou frearem abruptamente – os cenários de caos e colisões em massa não são difíceis de conceber. Embora esses veículos contem com múltiplos sensores e algoritmos de correção, um invasor determinado poderia tentar corromper os softwares de navegação ou explorar pontos cegos (como interferir em sinais de GPS ou enganar sistemas de visão). Até o momento, não há registro público de um acidente letal causado deliberadamente por um hacker, mas a possibilidade tem sido levada a sério por fabricantes e autoridades. Propostas de leis de segurança veicular foram inspiradas justamente por casos como o do Jeep Cherokee hackeado, visando estabelecer padrões mínimos de cibersegurança automotiva.

Não só carros de passeio estão em risco – **outros transportes automatizados** também podem ser alvos. Em 2008, um incidente na Polônia mostrou que mesmo sistemas "analógicos" podem ser manipulados digitalmente para fins maliciosos. Um adolescente de 14 anos em Lodz construiu um controle caseiro (adaptando um controle remoto de televisão) para emitir sinais infravermelhos que alteravam os trilhos dos **bondes elétricos** da cidade. Ele tratou a cidade como uma maquete de trem: desviou intencionalmente os bondes de suas rotas, causando descarrilamentos de *quatro composições* e deixando pelo menos **12 pessoas feridas**. Por sorte, ninguém morreu nesse ataque caseiro; mas foi um alerta de que sistemas de transporte, dos trilhos aos semáforos, podem ser sabotados por agentes maliciosos com meios relativamente simples. Hoje, com a introdução de ônibus autônomos, trens controlados por IA e até aviões altamente digitalizados, garantir a segurança cibernética desses veículos é tão importante quanto sua manutenção mecânica – afinal, brechas de

software podem ter impacto tão mortal quanto falhas de freio ou explosão de pneu.

Ataques cibernéticos a sistemas de água e saneamento

Uma área particularmente sensível, por envolver potencial *envenenamento em massa*, são os sistemas de **abastecimento de água potável**. Em teoria, se um hacker obtiver controle de estações de tratamento, ele poderia alterar a dosagem de produtos químicos ou desativar filtragens, comprometendo a qualidade da água distribuída a milhares de pessoas. Infelizmente, essa teoria quase se tornou realidade em **Oldsmar, Flórida (EUA)**, em fevereiro de 2021. Um invasor desconhecido conseguiu acesso ao sistema de controle da estação de tratamento da cidade (possivelmente via acesso remoto não seguro) e tentou **aumentar drasticamente a concentração de hidróxido de sódio (soda cáustica)** na água. A soda cáustica, em pequenas quantidades, serve para equilibrar o pH da água, mas em nível elevado pode causar envenenamento severo. O operador da planta notou a movimentação anômala no cursor da tela e conseguiu reverter a alteração a tempo. Caso não tivesse percebido, o ataque poderia ter resultado em uma **"contaminação em massa" da água potável**, com milhares de moradores expostos a uma água altamente corrosiva e tóxica. O episódio de Oldsmar ganhou manchetes no mundo todo e evidenciou fragilidades gritantes: descobriu-se, por exemplo, que a instalação não possuía firewall adequado e utilizava **senhas compartilhadas e software desatualizado**, falhas básicas de segurança que facilitaram a invasão.

Casos de invasão digital em sistemas de água não são novidade – e nem todos ficaram apenas no “quase”. Em 2000, na Austrália, um ex-funcionário ressentido invadiu remotamente o sistema de gerenciamento de esgoto de Maroochy Shire após ser rejeitado em um emprego municipal. Ele manipulou bombas e válvulas para **despejar mais de 1 milhão de litros de esgoto não tratado** em rios, parques e até no terreno de um hotel, causando estragos ambientais e um odor insuportável. Embora esse ataque não tenha tido o intuito de envenenar pessoas, imagine se a mesma técnica fosse aplicada a um sistema de

água potável, ou se, em vez de esgoto, produtos químicos tóxicos fossem liberados em um rio usado para abastecimento. Os danos à saúde pública poderiam ser severos.

Além do risco de envenenamento, um agente malicioso poderia simplesmente sabotar a **distribuição de água** – fechando bombas, esvaziando reservatórios ou causando transbordamentos. As consequências podem incluir falta d'água prolongada (gerando pânico e condições insalubres) ou mesmo **alagamentos e inundações** controladas remotamente. Em um cenário extremo, hackers poderiam tentar coordenar um ataque simultâneo contra múltiplos sistemas de utilidades públicas (água, energia, comunicações), amplificando o caos. Vale lembrar que sistemas de tratamento de água de pequenas cidades, em especial, muitas vezes carecem de investimento em TI e operam com estruturas inseguras, tornando-os alvos relativamente fáceis conforme diversos relatórios de segurança vêm apontando. Dado que água contaminada ou a interrupção do saneamento básico afeta potencialmente **populações inteiras**, esse tipo de ameaça é considerado uma forma de *ciberterrorismo* com objetivo de provocar danos humanos em larga escala. Oldsmar foi um alerta — e felizmente não virou tragédia —, mas é imperativo que lições sejam aprendidas para evitar que futuros ataques desse tipo alcancem sucesso.

Rede elétrica e infraestrutura industrial crítica

Se há algo capaz de afetar milhões de pessoas de uma só vez, para o bem ou para o mal, é a **infraestrutura de energia elétrica**. Apagões prolongados não apenas causam prejuízos econômicos, mas podem levar a situações letais – pense em hospitais sem geradores, sistemas de suporte vital desligados, aquecedores fora do ar em um inverno rigoroso ou aparelhos de ar condicionado inutilizados durante ondas de calor extremo. Nos últimos anos, ataques cibernéticos a redes elétricas deixaram de ser ficção. Em dezembro de 2015, a região de Ivano-Frankivsk, na Ucrânia, sofreu um blackout que desligou a luz (e o aquecimento) de aproximadamente **225 mil pessoas**. A causa, conforme investigação posterior, foi um ataque sofisticado: hackers penetraram os sistemas SCADA de distribuidoras de energia,

provavelmente com malware e acesso remoto, **abrindo disjuntores** e sabotando subestações de forma coordenada. Foi o primeiro caso confirmado no mundo de hackers causando um apagão elétrico. No ano seguinte, em 2016, outra investida digital atingiu a companhia de energia de Kiev, derrubando parte do fornecimento na capital ucraniana. Esses ataques – atribuídos a grupos ligados à Rússia – foram considerados testes de guerra cibernética, uma forma de demonstrar poder causando transtornos civis significativos, porém sem escalar a ponto de fatalidades diretas. Ainda assim, analistas alertam que *as lições aprendidas pelos ofensores poderiam ser reutilizadas em cenários de conflito*, potencialmente derrubando redes de energia de forma mais ampla e duradoura.

A vulnerabilidade da rede elétrica advém, em parte, da convergência entre sistemas antigos e tecnologia nova. Muitas instalações elétricas críticas usam equipamentos e protocolos legados, concebidos numa era pré-internet, agora interligados a redes corporativas e à internet para monitoramento e controle. Se um atacante consegue invadir a rede de TI de uma empresa de energia (por exemplo, via phishing ou explorando alguma porta remota mal protegida), ele pode se **mover lateralmente** até os sistemas de controle industrial (OT/SCADA). Uma vez lá, pode abrir ou fechar chaves, subestimar leituras de sensores, ou até danificar fisicamente transformadores e geradores. Em 2007, um experimento famoso do *Idaho National Lab* nos EUA, chamado **Aurora Generator Test**, mostrou que era possível usar comandos maliciosos para sincronizar errado um gerador elétrico, levando-o à auto-destruição. Esse tipo de ataque, se feito em larga escala contra múltiplos pontos da rede, poderia causar danos físicos extensos e prolongar uma falta de energia – em teoria, colocando em risco a vida de muitas pessoas dependentes de eletricidade.

Além da eletricidade, **outras infraestruturas industriais** apresentam riscos ciber-físicos. A indústria petroquímica, por exemplo, lida com substâncias inflamáveis e tóxicas; um ataque que desabilite os sistemas de segurança dessas plantas pode causar explosões ou vazamentos letais. Em 2017, foi descoberta na Arábia Saudita a **malware Triton (também chamada TRISIS)**, projetada especificamente para atacar os controladores de segurança de

processos industriais. O Triton foi capaz de reprogramar dispositivos *Triconex* (da Schneider Electric) responsáveis por atuar como última barreira de segurança em caso de condições perigosas na planta. Se não fosse identificado a tempo, esse malware poderia ter desativado sistemas de emergência e permitido que uma reação química saísse de controle, possivelmente levando a uma explosão ou liberação de gases tóxicos. Por essa razão, o Triton foi apelidado por alguns especialistas como *"o malware mais assassino do mundo"*, justamente por visar diretamente mecanismos cuja falha coloca vidas humanas em risco. A investigação mostrou que os atacantes exploraram uma vulnerabilidade em computadores Windows da rede industrial para implantar o Triton. Trata-se de um **marco preocupante na ciberguerra**: ao invés de roubar dados ou espionar, o objetivo era causar danos físicos e potencialmente matar pessoas, sabotando deliberadamente os sistemas de segurança de uma instalação química.

Outro caso notório, embora com objetivo distinto, foi o **Stuxnet** – o vírus descoberto em 2010 que sabotou centrífugas nucleares do programa iraniano. O Stuxnet não visava matar pessoas, mas sim danificar equipamentos (as centrífugas giravam em velocidades anormais até quebrar). Ainda assim, ele demonstrou que software malicioso bem desenvolvido pode destruir máquinas industriais com precisão. Se essa ideia for aplicada intencionalmente contra infraestruturas civis (usinas, fábricas químicas, redes de gás), as consequências podem ser severas. Imagine um ataque a um gasoduto que cause aumento repentino de pressão: explosões em série poderiam ocorrer. Ou a hackers abrindo comportas de uma represa hidroelétrica repentinamente: enxurradas inundando comunidades. Essas possibilidades colocam **populações inteiras em perigo** sem que seja necessário um único tiro – a arma é o código de computador.

Conclusão

Então, afinal, um ataque cibernético pode ser usado para matar pessoas ou populações inteiras? **Infelizmente, a resposta é sim** – embora, até o presente, a maioria dos casos conhecidos envolva

tentativas frustradas, demonstrações controladas ou consequências indiretas. Analisando os exemplos apresentados, fica claro que a linha que separa o mundo digital do físico se tornou tênue. Marcapassos e bombas de insulina com falhas de segurança podem ser explorados para assassinar silenciosamente pacientes individuais. Carros autônomos ou conectados sem proteções robustas podem ser convertidos em armas contra seus ocupantes ou pedestres. Sistemas de água e alimentos podem ser envenenados em larga escala se invadidos por mãos maliciosas. Redes elétricas e fábricas podem ser sabotadas para gerar apagões, explosões ou desastres ambientais, com potencial de ceifar vidas de maneira indireta ou diretamente.

Importante notar que, em muitos casos discutidos, não houve *intenção confirmada de matar* – por exemplo, o ataque de Oldsmar na água foi neutralizado a tempo, e os hackers que desligaram a luz na Ucrânia pareceram mais interessados em causar perturbação que fatalidades imediatas. Porém, isso não diminui a gravidade do risco; pelo contrário, mostra que **tivemos sorte** em vários incidentes por não ter ocorrido o pior cenário. A tendência de digitalização continuará a avançar (mais IoT nas nossas casas, cidades inteligentes, veículos autônomos nas ruas, dispositivos médicos conectados ao nosso corpo), o que significa que a **superfície de ataque** para agentes maliciosos também se expande.

Para proteger vidas humanas, será fundamental adotar uma mentalidade de segurança "by design" nesses sistemas. Isso inclui: desenvolvimento de softwares mais seguros, **autenticação forte** e criptografia em dispositivos críticos, isolamento de redes de controle (por exemplo, separar estritamente redes industriais ou veiculares da internet pública), monitoramento constante e planos de resposta a incidentes que considerem impactos físicos. Regulamentações governamentais também têm seu papel – como a FDA agiu no caso dos marcapassos, outras agências e setores precisarão definir padrões obrigatórios de cibersegurança para equipamentos cujo mau funcionamento ameaça vidas.

Em suma, ataques cibernéticos evoluíram de meros inconvenientes digitais para **ferramentas potencialmente letais** nas mãos erradas. A pergunta não é mais se sistemas computacionais podem causar danos

físicos – sabemos que podem. A pergunta agora é *como vamos nos preparar* para impedir que o próximo ataque cibernético deliberado tenha consequências trágicas. A resposta envolverá esforços conjuntos de engenheiros, profissionais de TI, gestores de risco e formuladores de políticas, trabalhando para que a promessa da tecnologia não seja ofuscada pelo pesadelo de sua exploração maliciosa.

Referências Bibliográficas:

1. Peter Elkind, Jack Gillum. "America's Drinking Water Is Surprisingly Easy to Poison." *ProPublica*. (17 de março de 2021) propublica.org
2. Peter Elkind, Jack Gillum. *Ibid*. propublica.org
3. Lily Hay Newman. "These Hackers Made an App That Kills to Prove a Point." *Wired*. (16 de julho de 2019) wired.com
4. Alex Hern. "Hacking risk leads to recall of 500,000 pacemakers due to patient death fears." *The Guardian*. (31 de agosto de 2017) theguardian.com
5. Isabel Skierka. "Murder by Health Hack." *Global Network Perspectives*. (6 de fevereiro de 2018) globalnetwork.io
6. Andy Greenberg. "Hackers Remotely Kill a Jeep on the Highway—With Me in It." *Wired*. (21 de julho de 2015) wired.com
7. Andy Greenberg. *Ibid*. wired.com
8. Chuck Squatriglia. "Polish Teen Hacks His City's Trams, Chaos Ensues." *Wired*. (11 de janeiro de 2008) wired.com
9. Pavel Polityuk, et al. "Ukraine's power outage was a cyber attack - Ukrenergo." *Reuters*. (18 de janeiro de 2017) reuters.com
10. Wikipedia. "Triton (malware)." Última atualização em 30 de junho de 2019 en.wikipedia.org