ESTUDOS UNIVERSITÁRIOS
UFPE PROEXT Pró-Reitoria de Extensão

As novas tecnologias e a securitização do meio ambiente: uma análise sobre os impactos da inteligência artificial

New Technologies and Environmental Securitization: An Analysis of the Impacts of Artificial Intelligence

Marcos Aurelio Guedes de Oliveira
Universidade Federal de Pernambuco (UFPE)
Recife, Pernambuco, Brasil
Doutor em Government
E-mail: marcosaurelioguedes@gmail.com
https://orcid.org/0000-0001-9792-5453
http://lattes.cnpq.br/5438547075969282

Renato Victor Lira Brito
Universidade Federal de Pernambuco (UFPE)
Recife, Pernambuco, Brasil
Mestre em Ciência Política
E-mail: renato.lirabrito@ufpe.br
https://orcid.org/0000-0001-6012-8469
http://lattes.cnpq.br/5778835197310224

Júlia Costa Amancio Santos Coriolano
Universidade Federal de Pernambuco (UFPE)
Recife, Pernambuco, Brasil
Bacharel em Ciência Política
E-mail: julia.amancio@ufpe.br
https://orcid.org/0009-0008-2226-9031
http://lattes.cnpq.br/9229400446279323

Júlia Cardoso Lima Pastick
Universidade Federal de Pernambuco (UFPE)
Recife, Pernambuco, Brasil
Bacharel em Ciência Política
E-mail: julia.pastick@ufpe.br
https://orcid.org/0009-0008-1506-1769
http://lattes.cnpq.br/0620506711999889

Maria Clara Miranda Bezerra Dias
Universidade Federal de Pernambuco (UFPE)
Recife, Pernambuco, Brasil
Graduanda em Ciência Política
E-mail: clara.miranda@ufpe.br
https://orcid.org/0009-0005-8361-6365
http://lattes.cnpq.br/9154583385721140

Taís Barbosa Gusmão
Universidade Federal de Pernambuco (UFPE)
Recife, Pernambuco, Brasil
Graduanda em Ciência Política
E-mail: tais.gusmao@ufpe.br
https://orcid.org/0009-0000-4654-1409
http://lattes.cnpq.br/8040759100696661

Resumo

Como as novas tecnologias podem contribuir para a securitização do meio ambiente? Respondemos a essa pergunta com a utilização de métodos mistos. Os desafios contemporâneos surgidos com o advento da Internet das Coisas (IoT) e da Inteligência Artificial (IA) alçaram as questões climáticas e o debate sobre sustentabilidade ao

campo da segurança internacional. Os ataques cibernéticos de alta significância em infraestruturas críticas denotam a indissociabilidade atual entre meio ambiente e o ecossistema cibernético; ciberataques podem, por exemplo, ser empregados por IA e atingir sistemas de tratamento de água e esgoto, degradando a qualidade da água e sabotando os alertas de poluição. O desenho da pesquisa compreende técnicas quantitativas. Em síntese, mapeamos os incidentes altamente significativos com potencial impacto sobre o meio ambiente, descrevendo as suas principais tendências. Entre os principais resultados, identificamos que, embora a produção sobre o tema seja incipiente, há uma presença massiva de incidentes de alta significância, com efeito em infraestruturas críticas e potencial impacto no meio ambiente.
Palavras-chave: inteligência artificial; meio ambiente; métodos quantitativos; securitização; novas tecnologias

Abstract

How can new technologies contribute to the securitization of the environment? We address this question using mixed methods. The contemporary challenges brought by the advent of the Internet of Things (IoT) and Artificial Intelligence (AI) have elevated climate issues and the sustainability debate to the field of international security. High-impact cyberattacks on critical infrastructures reveal the current inseparability between the environment and the cyber ecosystem; for instance, AI-driven cyberattacks can target water and sewage treatment systems, degrading water quality and sabotaging pollution alerts. The research design includes quantitative techniques. In summary, we mapped highly significant incidents with potential environmental impact, describing their main trends. Among the key findings, we identified that, although research on this topic is still emerging, there is a massive presence of

high-significance incidents affecting critical infrastructures and potentially impacting the environment.

Keywords: artificial intelligence; environment; quantitative methods; securitization; new technologies

INTRODUÇÃO

Na última década, o debate global sobre os riscos decorrentes das mudanças climáticas cresceu significativamente, sendo estas apontadas pela Organização Mundial da Saúde (OMS) como a principal ameaça à saúde da humanidade no século XXI. A centralidade que a questão ambiental possui nas agendas das organizações internacionais e entre os países tem ampliado as discussões sobre a securitização do meio ambiente (Biswas, 2011), processo que ocorre quando existe um movimento de construção discursiva do campo como uma ameaça existencial para os Estados (Buzan; Waever; De Wilde, 1998). No entanto, há ainda um dissenso entre os especialistas sobre os efeitos das ações securitizadoras nessa seara.

Embora a securitização do meio ambiente proporcione embates acadêmicos, a centralidade dessa agenda é inegável, especialmente no contexto do Antropoceno. O campo das Relações Internacionais (RI) foi historicamente dominado por questões de segurança na era nuclear, mas hoje a sobrevivência do Estado não é mais percebida como ameaçada apenas pelos arsenais de superpotências, mas também por outra série de arranjos políticos e técnicos. Conforme argumenta Simon Dalby (2022), a crise da segurança ambiental reside na contradição de que os próprios sistemas industriais movidos a combustíveis fósseis que prometem segurança estão minando as condições ecológicas para a sua existência.

Essa recontextualização exige que o poder seja repensado em termos ecológicos, focando no florescimento de sistemas adaptáveis, em vez da dominação física. Portanto, a securitização do meio ambiente da qual tratamos neste artigo se enquadra na urgência de confrontar o risco sistêmico trazido pelo sistema econômico contemporâneo.

A Inteligência Artificial (IA) insere-se de forma ambígua nesse novo quadro. Cientistas e formuladores de políticas reconhecem a IA como uma ferramenta potencial para resolver problemas de sustentabilidade, alinhada aos Objetivos de Desenvolvimento Sustentável (ODS). Contudo, essa tecnologia apresenta um dilema, uma faca de dois gumes. A análise da IA para segurança ambiental deve ser feita sob múltiplas perspectivas (*e.g.*: nacional, internacional, humana e ecológica) e deve considerar que a IA, se usada sem princípios éticos e segurança cibernética, pode ter consequências hostis, como o enfraquecimento de movimentos ambientalistas através de guerra psicológica e desinformação. Esta inseparabilidade entre o meio ambiente e o ecossistema cibernético é a chave para a nossa análise da securitização (Francisco, 2023).

Em 2020, com o surgimento da pandemia da Covid-19, houve uma maior projeção acerca da relação entre os impactos da ação humana no meio ambiente e a proliferação de pandemias (Melo; Andrade, 2024). Além disso, os Estados vivenciaram o que foi denominado como a pandemia na pandemia. Com o advento do *lockdown* como medida emergencial durante os primeiros anos da pandemia, o mundo do trabalho passou a ser

intermediado pela dinâmica do *home office*, o que afetou positiva e negativamente o meio ambiente. Enquanto houve a redução geral da emissão de gases do efeito estufa, registrou-se também o aumento exponencial de crimes e ataques cibernéticos, evidenciando a prevalência do ecossistema cibernético na atualidade (Nagli, 2022).

Nesse sentido, observa-se um contexto cada vez mais interconectado e, portanto, dependente desses recursos e modos de relações, ao mesmo tempo em que tem se tornado patente a situação incontornável na qual se encontra a agenda ambiental. Entrementes, a interseção entre essas dimensões, representada pelas mudanças resultantes das novas tecnologias, especialmente a Inteligência Artificial, lança outros desafios para as mais diversas parcelas da sociedade, dentre elas: pesquisadores, líderes políticos, organizações internacionais e formuladores de políticas públicas.

No dia 5 de março de 2024, a Assembleia Geral da Organização das Nações Unidas (ONU) adotou a primeira resolução global da história sobre a Inteligência Artificial, objetivando, entre outras coisas, o desenvolvimento sustentável e a promoção de sistemas de IA seguros, protegidos e confiáveis. Essa resolução é uma das mobilizações recentes em observância aos 17 Objetivos da ONU para o Desenvolvimento Sustentável, projetados para serem alcançados até 2030.

Embora haja uma sinalização internacional por parte de líderes políticos e especialistas desses setores, ainda é notório o *gap* na produção empírica das Ciências Sociais quando o objeto de estudo é a relação entre o meio ambiente e as novas tecnologias — lacuna identificada já

na etapa de pré-análise. Em geral, a maioria das pesquisas concentra-se em questões referentes à Ciência da Informação e à Ciência da Computação, enquanto os trabalhos com maior enfoque na temática ambiental apresentam predominantemente discussões teóricas e apenas tangenciam o debate sobre as novas tecnologias.

Diante dessa contradição entre o horizonte dos decisores políticos e do debate acadêmico, o *puzzle* (Gustafsson; Hagström, 2018) que move a nossa pesquisa é direcionado pela necessidade de contribuições empíricas mais pontuais e específicas acerca da relação entre meio ambiente e as novas tecnologias.

A transição global para a Agricultura 4.0, caracterizada pelos avanços em Internet das Coisas (IoT), sensores, robótica, Big Data e Inteligência Artificial, é vista como uma solução crucial para aumentar a produtividade, a eficiência e a sustentabilidade dos sistemas agroalimentares. O objetivo central desta quarta revolução agrícola é garantir as necessidades futuras da população global de maneira justa, resiliente e sustentável.

A digitalização é intensa em toda a Cadeia de Suprimentos Agroalimentar (AFSC), desde o monitoramento de gases de efeito estufa e o uso de robôs para colheita, até a otimização logística e a rastreabilidade por meio de tecnologias como Blockchain. Contudo, essa interconectividade digital expõe a AFSC a desafios e vulnerabilidades até então desconhecidos. A segurança cibernética é um desafio crítico, e a dependência de sistemas IoT e IA aumenta a superfície de ataque.

A vulnerabilidade da agricultura tem implicações diretas na segurança humana, pois um ataque cibernético a um sistema de irrigação ou a uma rede de sensores para diagnóstico de doenças pode comprometer a produção. Da mesma forma que a IA oferece oportunidades para diagnosticar doenças de culturas ou gerenciar a qualidade da água, sua vulnerabilidade pode afetar a segurança alimentar. Portanto, o mapeamento dos incidentes de alta significância, com foco em infraestruturas críticas como os setores de energia e água, torna-se essencial para dimensionar o risco digital em uma dimensão fundamental para a segurança alimentar global.

Com base nessa lacuna identificada, a questão de pesquisa que move este trabalho é “Como as novas tecnologias podem contribuir para a securitização do meio ambiente?”. Respondemos a essa pergunta com a utilização de técnicas quantitativas.

Na próxima seção, apresentaremos a metodologia e os pressupostos epistemológicos e ontológicos do trabalho, bem como as técnicas empregadas neste estudo. Em seguida, realizamos um mapeamento dos incidentes altamente significativos (CSIS, 2024) com impacto no meio ambiente, descrevendo as principais tendências estatísticas encontradas.

METODOLOGIA

Esta pesquisa é, precipuamente, estruturada a partir de uma perspectiva ontológica fundacionista, cujo pressuposto é o de que existe uma realidade objetiva para além da linguagem e da percepção. Em termos

epistemológicos, estamos alinhados ao realismo, que tem como premissa a identificação de que nem tudo o que existe pode ser assimilado e apreendido, principalmente no que se refere aos objetos de pesquisa das Ciências Sociais e da Ciência Política, mas que deve-se buscar uma aproximação da realidade, encontrando os mecanismos adequados, criando modelos e sempre reconhecendo a contingência do fazer científico (Bevir, 2008; Marsh; Furlong, 2017).

Dessa forma, na pesquisa, identificamos os incidentes cibernéticos altamente significativos com impacto no meio ambiente, a partir dos dados do *Center for Strategic & International Studies* para a série histórica de 2006 a 2024 (CSIS, 2024). Com base nessas informações, analisamos, através de estatísticas descritivas (Gerring, 2012) a trajetória histórica dos eventos, os países de origem, os tipos de atores responsáveis, países vítimas e tipos de vítimas, e tipificamos os padrões observados. Na Tabela 1, sumarizamos as informações das etapas da metodologia da pesquisa.

Estatísticas Descritivas	
Fonte	*Center for Strategic & International Studies (2024)*
Unidade de análise	Incidentes cibernéticos altamente significativos com potencial impacto no meio ambiente
Recorte temporal	2006 - 2024
Software de análise de dados	*RStudio*
Variáveis	Ano; mês; descrição do incidente; país de origem; tipo de ator responsável; país vítima; tipo de vítima; alvo do ataque

Tabela 1. Desenho de pesquisa
Fonte: Os autores (2024).

Os detalhes técnicos e metodológicos sobre cada uma das etapas da pesquisa, bem como seus protocolos de coleta e análise, serão explicitados nas suas respectivas seções, de forma a apresentar também um maior didatismo, seguindo uma abordagem *step-by-step* de produção empírica com métodos mistos. Ademais, disponibilizamos as bases de dados e códigos utilizados no *GitHub* (ver Lira Brito *et al*., 2024), alinhando a pesquisa ao debate internacional sobre transparência e replicabilidade nas Ciências Sociais (Freese; Rauf; Voelkel, 2022).

MAPEAMENTO DOS INCIDENTES CIBERNÉTICOS ALTAMENTE SIGNIFICATIVOS

O relatório do *Center for Strategic & International Studies* (2024) serviu como base para as análises descritas apresentadas nesta subseção por divulgar incidentes cibernéticos significativos ocorridos de 2006 até o presente momento. É importante mencionar que ciberataques podem ser empregados por meio de inteligência artificial (Davis, 2019), de forma automatizada (Sharikov, 2018). No entanto, uma das limitações do relatório é não especificar em quantos desses casos houve o emprego de IA na condução dos ataques. Outra limitação é que ele não deixa claro se os ciberataques realmente trouxeram um prejuízo direto ao meio ambiente. De qualquer modo, o mapeamento dos incidentes altamente significativos é importante para alertar sobre a possibilidade de ataques cibernéticos automatizados e conduzidos por IA, e o seu efeito em potencial sobre o meio ambiente, uma vez que estes podem superar, em grandes números, os ataques conduzidos por humanos.

Os ataques são classificados primeiramente pela equipe de pesquisadores do Centro que se concentram em ações estatais, de espionagem e ataques cibernéticos em que as perdas são superiores a um milhão de dólares (CSIS, 2024). Além disso, o relatório é um “documento vivo” (CSIS, 2024) com atualizações regulares de novos incidentes. O relatório disponibiliza o mês, ano e descrições dos ataques em forma de texto.

O processo de categorização do presente trabalho contou com uma primeira análise manual de todos os incidentes, identificando os que possuem pelo menos algum potencial tipo de implicação ambiental. A partir dessa primeira identificação, os ataques foram categorizados a partir do período em que ocorreram, os países e atores responsáveis e vítimas dos ataques, assim como o setor ambiental alvo do incidente. A análise manual do documento foi escolhida por possibilitar maior controle sobre o conteúdo, garantida por uma maior contextualização dos incidentes a partir da análise integral das descrições.

Dessa forma, foram encontrados 78 ataques cibernéticos com potencial impacto ao meio ambiente em todo o mundo, realizados entre 2009 e 2023. Quando analisados ao longo do tempo, conforme a Figura 1, há um aumento no número de casos nos últimos anos, com destaque para os anos de 2020 e 2021, que atingiram 16 e 14 casos, respectivamente. O ano de 2012 também se destaca pelo grande número de ataques cibernéticos (Agência Estado, 2013), alavancando também os casos com potenciais efeitos ao meio ambiente. Com uma tendência de crescimento de 2016, o ano de 2023, entretanto, apresentou uma diminuição nos ataques para taxas anteriores a esse período.

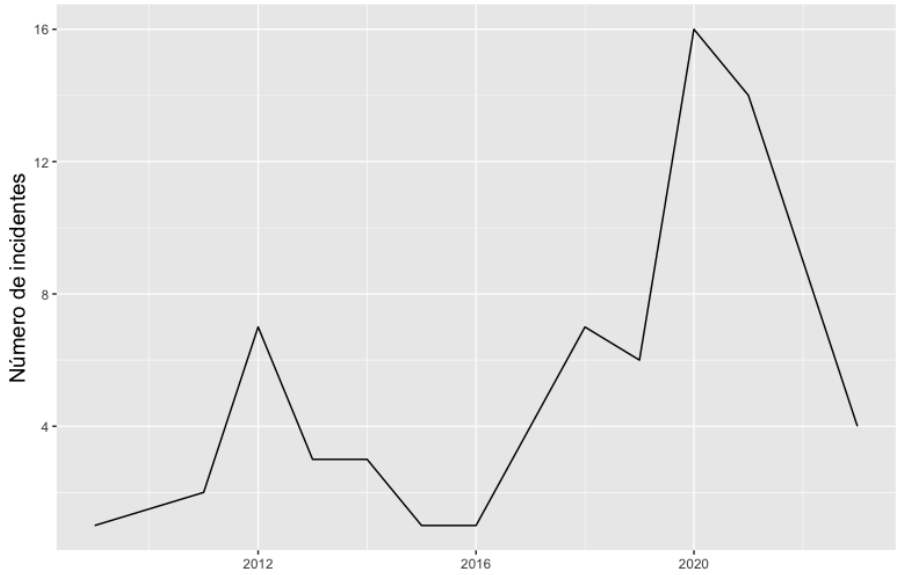

Figura 1. Número de ataques cibernéticos com potencial impacto ao meio ambiente
Fonte: Os autores, adaptado para o português de CSIS (2024).

Quando analisamos por tipo de ator, os governos são os que mais praticam e são vitimizados por esses ataques. A Figura 2 também mostra que, logo após os governos nacionais, *hackers* não identificados são os que mais aplicam os ataques cibernéticos com potenciais implicações ambientais. Em contrapartida, o setor privado é o segundo maior alvo desses ataques, seguido por indivíduos e Organizações Internacionais (OIs), com apenas 2 vítimas para cada em todo o período analisado.

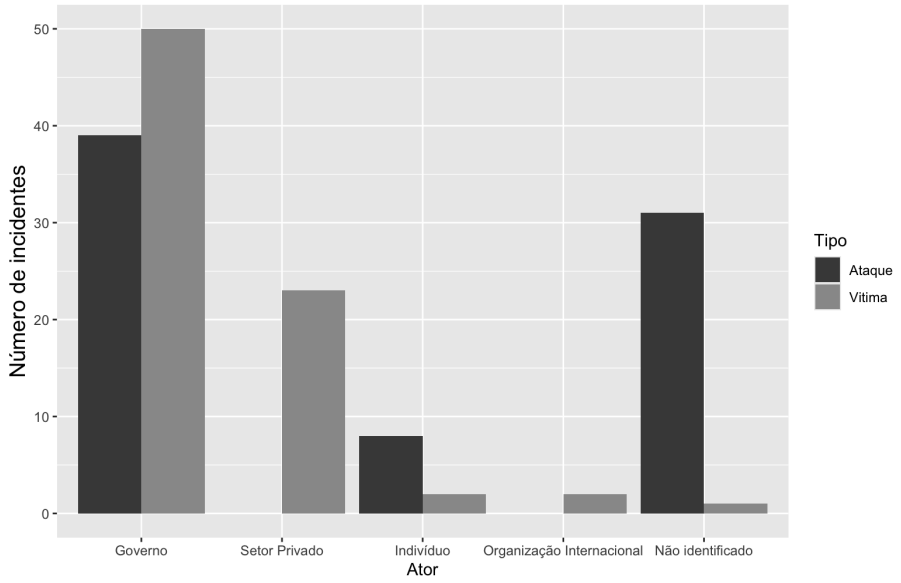

Figura 2. Número de ataques por tipos de atores
Fonte: Os autores, adaptado para o português de CSIS (2024).

Em relação apenas aos ataques, independentemente do ator responsável, os russos são supostamente os principais agressores. China e Coreia do Norte vêm logo em seguida, cada um com dez ataques com implicações ambientais reportados pelo CSIS (2024). Irã, Israel, Síria, Ucrânia e Vietnã também foram responsabilizados por pelo menos algum incidente cibernético. O número total de incidentes para cada um desses países pode ser observado na Figura 3.

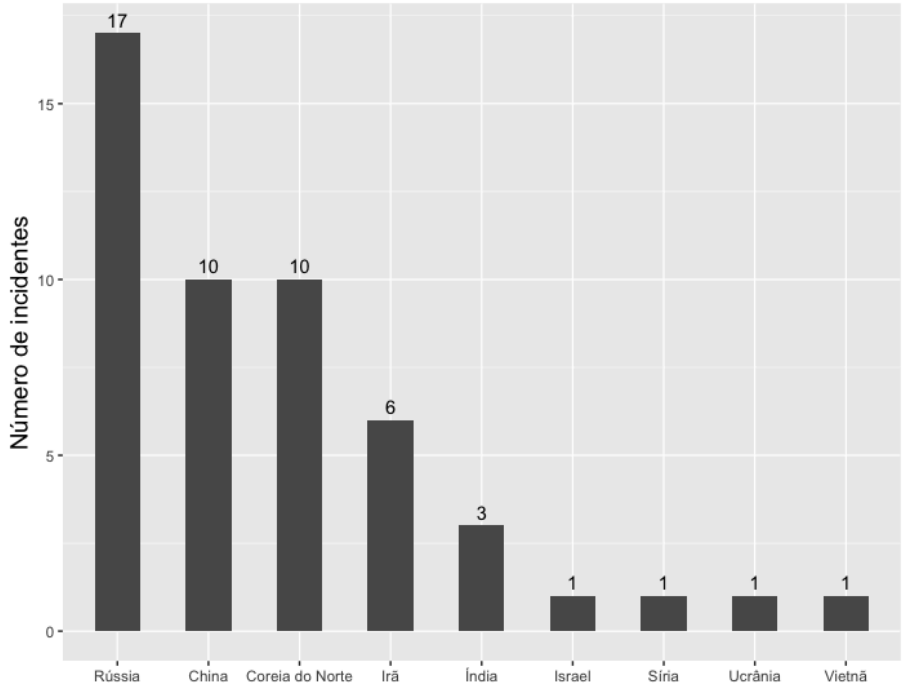

Figura 3. Número de incidentes por países responsáveis por ataques
Fonte: Os autores, adaptado para o português de CSIS (2024).

Além dos países apresentados, algumas regiões, como o Leste Europeu e o Oriente Médio também foram reportados como responsáveis por ataques, cada um em apenas um incidente. Entretanto, pela falta de precisão, os países que compõem essas regiões não foram contabilizados para esta análise. Também é necessário pontuar que 26 casos não possuem nenhuma identificação em relação a um possível país de origem dos incidentes.

As nacionalidades dos atores-alvo desses mesmos ataques tendem a ser mais diversas. Enquanto os atacantes se resumem a apenas nove nações, as vítimas estão distribuídas em 44 países diferentes. Entretanto, a

maior parte desses países sofreu apenas 1 ataque cibernético com implicação ambiental ao longo dos 19 anos analisados. Para fins de análise e apresentação, esses casos únicos foram categorizados como “outros”, como apresentado na Figura 4.

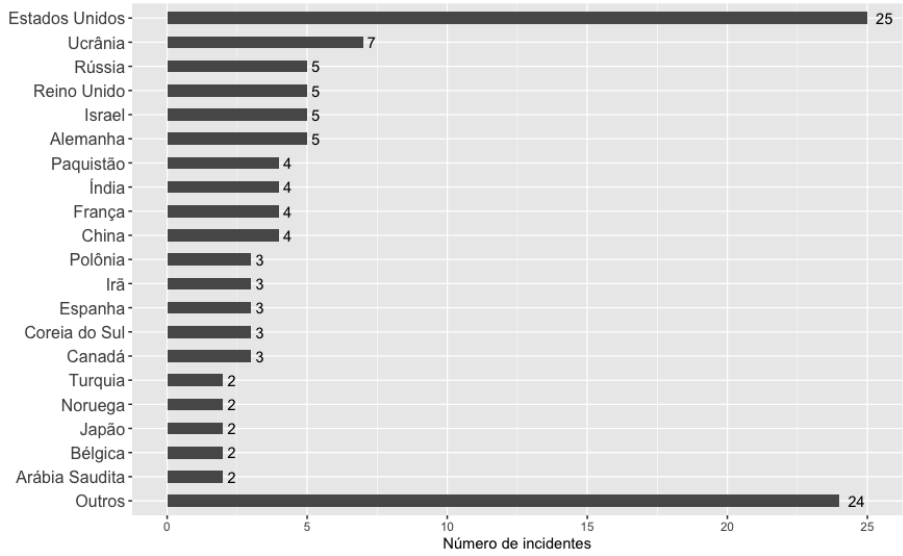

Figura 4. Número de incidentes por países vítimas de ataques
Fonte: Os autores, adaptado para o português de CSIS (2024).

Apesar da grande quantidade de casos únicos, os ataques com alvo a atores estadunidenses conseguem superar essa marca. Os Estados Unidos da América (EUA), mesmo não tendo sido reportado como responsável por nenhum incidente cibernético com implicações ambientais, é o país que mais recebe esse tipo de ataque. A Ucrânia, segundo país com maior número de casos, foi alvo de ataques cerca de 4 vezes menos que os EUA. Desconsiderando os Estados Unidos, a distribuição de incidentes entre o restante dos países vítimas é mais

homogênea. Portanto, há uma discrepância de casos não só em relação aos países-alvo, mas também quando comparamos entre as nações atacantes e vítimas.

Analisando mais especificamente os setores impactados pelos incidentes cibernéticos, observa-se que o setor energético é o mais atingido por incidentes com implicação ambiental. Além do setor de energia em geral, a Figura 5 também indica uma maior concentração de ataques nos setores petrolífero e de energia nuclear. Em seguida, infraestruturas hídricas — como as de abastecimento e tratamento de água — também são alvo de ataques cibernéticos. Outros setores, como centros de pesquisa, setor elétrico, marítimo, de saúde e de meio ambiente, também foram atingidos. A categoria 'Outros' agrega ataques a infraestruturas de setores diversos que, individualmente, apresentam valores menos significativos em relação aos anteriores.

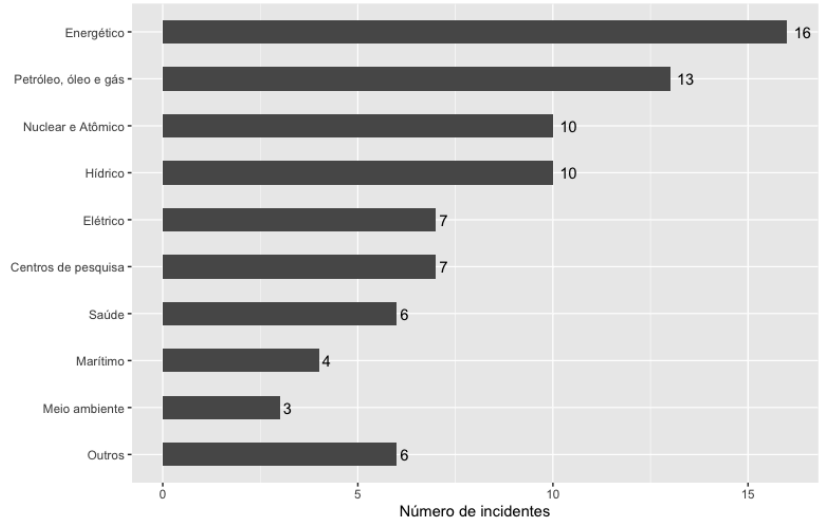

Figura 5. Número de ataques por setor
Fonte: Os autores, adaptado para o português de CSIS (2024).

O Quadro 1, abaixo, apresenta as descrições originais do CSIS para cada um dos setores com implicação ambiental identificados a partir da análise manual do relatório. Esses excertos foram escolhidos para exemplificar como os ataques cibernéticos foram realizados no âmbito de cada uma das áreas e como o CSIS tende a descrever os incidentes em geral. Dessa forma, além de *hackers* utilizarem diferentes táticas, o relatório também apresenta as descrições dos ataques em diferentes graus de detalhamento. Enquanto o incidente exemplificativo para o setor hídrico especifica a quantidade de computadores e dados utilizados no ataque, o caso energético não possui um responsável pelo ataque identificado, por exemplo.

Setor	Mês e ano	Descrição de ataques
Hídrico	12/2023	*Hackers* do Estado ucraniano paralisaram a maior empresa de abastecimento de água da Rússia, encriptando mais de 6.000 computadores e apagando mais de 50 TB de dados. Os *hackers* alegaram que o seu ataque foi uma retaliação ao ciberataque russo *Kyivstar*.
Centros de pesquisa	05/2020	Jean-Pascal van Ypersele, vice-presidente do Painel Intergovernamental sobre Mudança do Clima das Nações Unidas, atribuiu à Rússia a invasão e a divulgação de milhares de e-mails da Unidade de Pesquisas Climáticas da Universidade de East Anglia, como parte de uma conspiração para minar as negociações de Copenhague sobre o clima.
Elétrico	12/2017	A companhia francesa Schneider Electric precisou encerrar as operações de uma central elétrica no Oriente Médio após um *malware* comprometer os seus sistemas de controle industrial. Análises de pesquisadores em segurança indicaram que o ataque foi patrocinado por um Estado.
Energético	04/2020	O governo e entidades do setor de energia do Azerbaijão foram alvos de um grupo não identificado focado no sistema *SCADA* de turbinas eólicas.
Marítimo	05/2020	*Hackers* israelenses interromperam as operações em um porto iraniano por vários dias, causando falhas e atrasos massivos. Autoridades caracterizam o ataque como uma retaliação contra um ataque iraniano malsucedido realizado em abril que visava os sistemas de comando e controle dos sistemas de distribuição de água de Israel.

Meio ambiente	12/2020	Na véspera de natal, *hackers* atacaram a Agência Escocesa de Proteção ao Meio Ambiente com um ataque de *ransomware*. Após decidirem não pagar o resgate, os *hackers* publicaram os dados roubados.
Nuclear e Atômico	10/2019	A Índia anunciou que o *malware* norte-coreano criado para extração de dados foi identificado nas redes de uma usina de energia nuclear.
Petróleo, óleo e gás	12/2019	Um *malware* iraniano foi implantado na rede de Bapco, a companhia petrolífera nacional de Bahrain
Saúde	02/2021	*Hackers* norte-coreanos tentaram invadir os sistemas computacionais da companhia farmacêutica Pfizer para acessar informações sobre vacinas e tratamentos para a COVID-19.
Outros	07/2018	*Hackers* comprometeram contas pertencentes a autoridades do Partido Verde Alemão, incluindo as contas utilizadas por Annalena Baerbock e Robert Habeck, que agora ocupam os cargos de Ministra das Relações Exteriores e Ministro de Assuntos Econômicos e Ação Climática.

Quadro 1. Exemplos de ataques por setor
Fonte: Os autores, adaptado para o português de CSIS (2024).

Outra diferença entre os casos é o nível de implicação na questão ambiental. Por exemplo, no caso da saúde, um ataque voltado à obtenção de informações sobre vacinas e tratamentos para a Covid-19 possui implicações ambientais indiretas, uma vez que os impactos ambientais de pandemias ocorrem de forma mais complexa, mediadas por mudanças econômicas e sociais. Por outro lado, centros de pesquisa podem gerar impactos

ambientais diretos, como exemplificado na descrição presente no Quadro 1.

Em geral, as descrições de incidentes cibernéticos com possíveis implicações ambientais apresentam o papel de *hackers* como orquestradores desses eventos. A Figura 6 apresenta a nuvem de palavras com os termos mais frequentes nas descrições dos incidentes. As nuvens de palavras apresentadas a seguir foram elaboradas a partir de uma etapa de pré-processamento do texto, com a remoção de pontuações, números, símbolos, *stopwords* e palavras com menos de quatro letras. Esses ajustes foram realizados a fim de garantir a presença de palavras que contribuam substantivamente para o contexto dos ataques.

Figura 6. Nuvem de palavras agregada
Fonte: Os autores, adaptado do CSIS (2024).

Enquanto a nuvem de palavras de todos incidentes apresenta termos mais genéricos, como *hackers* e *targeted*, as análises setorizadas exibem palavras contextuais com mais frequência. Os setores energético (Figura 7) e hídrico (Figura 10) demonstram uma ênfase maior em termos próprios desse tema, com maiores menções para *energy* e *water*. Por outro lado, as palavras mais frequentes para os setores petrolífero (Figura 8) e nuclear (Figura 9) fazem referências às companhias petrolíferas e à Coreia do Norte — neste último caso, devido à maior atuação da Coreia do Norte no âmbito nuclear. Ainda assim, os termos referentes a ataques cibernéticos em geral estão presentes em todas as descrições. A análise automatizada de conteúdo foi escolhida para esta etapa.

Figura 7. Nuvem de palavras do setor energético
Fonte: Os autores, adaptado do CSIS (2024).

Figura 8. Nuvem de palavras do setor de petróleo, óleo e gás
Fonte: Os autores, adaptado do CSIS (2024).

Figura 9. Nuvem de palavras do setor nuclear e atômico
Fonte: Os autores, adaptado do CSIS (2024).

Figura 10. Nuvem de palavras do setor hídrico
Fonte: Os autores, adaptado do CSIS (2024).

Como evidenciado na Tabela 2, que detalha os alvos dos ataques e os atacantes por tipo de ator, identificamos que o setor energético é o mais crítico tanto para governos quanto para empresas. Em seguida, as infraestruturas elétricas aparecem como principais alvos para as empresas, enquanto o setor petrolífero é o segundo mais crítico para os governos. Ainda existem discrepâncias entre esses dois atores em relação às infraestruturas elétricas e a área de saúde. Enquanto elas são críticas para o setor privado, os governos as atacam mais. Centros de pesquisa, setores marítimos e de meio ambiente são os únicos setores que não possuem vítimas empresariais.

Setor	Atores	Atacante	Vítima
Água	Governo	3	5
	Setor Privado	-	2
Centros de pesquisa	Governo	5	5
Elétrico	Governo	7	2
	Setor Privado	-	5
Energia	Governo	7	12
	Setor Privado	-	6
Marítimo	Governo	3	5
Meio ambiente	Governo	1	3
Nuclear e Atômico	Governo	3	5
	Setor Privado	-	1
Petróleo, óleo e gás	Governo	4	8
	Setor Privado	-	4
Saúde	Governo	3	2
	Setor Privado	-	4
Outros	Governo	4	4
	Setor Privado	-	1

Tabela 2. Número de ataques por setor, ator e tipo de ataque
Fonte: Os autores, adaptado para o português de CSIS (2024).

Dessa forma, de acordo com a Tabela 2, as principais vítimas de incidentes cibernéticos com possíveis implicações ambientais são os governos nacionais e suas agências. Com o crescente número de ocorrências ao longo do tempo, esses achados reforçam o processo de securitização da agenda ambiental. Essa escalada dos

casos com impactos ao meio ambiente está inserida em um contexto de aumento de ataques cibernéticos não-militares (Buzan, 1997), que têm como alvo e causa as tensões sociais (Burton; Lain, 2020).

CONSIDERAÇÕES E DIMENSIONAMENTO DOS DANOS EM POTENCIAL

Vale mencionar que ao falarmos de danos ambientais potenciais, oriundos de ciberataques, precisamos qualificar os tipos de danos que seriam causados, por setor atingido. Por exemplo, se tratarmos sobre o setor hídrico, um ataque cibernético aos sistemas de tratamento de água pode ocasionar a perda de controle de qualidade da água, ocasionando sua contaminação, ou prejudicando os alertas de poluição (CI-ISAC, Austrália 2023). Além disso, poder-se-ia lançar 80 mil litros de esgoto em rios e parques, como ocorreu em Queensland, na Austrália, no ano de 2000 (Kesler, 2011); ou até mesmo ocasionar rupturas de barragens capazes de inundar cidades (Laux; Honea, 2018), forçando moradores a se deslocarem, e devastando o ecossistema local.

Nesse sentido, se considerarmos o setor de energia nuclear, podemos ter um ciberataque capaz de causar explosões, as quais, por sua vez, lançariam material radioativo na atmosfera, contaminando o meio ambiente. Em seu laboratório, e juntamente ao seu time, Stuart Madnick, professor de sistemas de engenharia do MIT (Massachusetts Institute of Technology), simulou ciberataques que resultaram em explosões (Williams,

2024), revelando a plausibilidade de ataques ciber-físicos impulsionados por IA. Madnick afirma:

> Se uma usina for interrompida por um ataque cibernético comum, ela poderá retornar às operações relativamente rápido. No entanto, se *hackers* provocarem uma explosão ou incêndio, a retomada não ocorrerá em um ou dois dias; levará semanas ou até meses, pois muitos componentes desses sistemas especializados são fabricados sob encomenda. Poucos percebem que os períodos de inatividade podem ser substanciais (n. p., tradução nossa)[1].

Se todos estes incidentes cibernéticos de alta significância, relatados pelo CSIS, foram conduzidos manualmente, é importante dimensionarmos o potencial de ciberataques automatizados, impulsionados e conduzidos por inteligência artificial. Por isso, podemos vislumbrar um aumento na frequência e sofistificação de ataques cibernéticos conduzidos por AI, os quais são capazes de superar, em número e em capacidade de danos, os ciberataques conduzidos por humanos.

Ainda, os ataques cibernéticos impulsionados por IA podem superar os humanos em complexidade, se considerarmos o poder de inteligências artificiais

[1] If you cause a power plant to stop from a typical cyberattack, it will be back up and online pretty quickly, but if hackers cause it to explode or burn down, you are not back online a day or two later; it will be weeks and months because a lot of the parts in these specialized systems are custom made. People don't realize downtimes can be substantial (Williams, 2024).

generativas; com simples *scripts* de comando, estas podem gerar códigos maliciosos muito mais eficientes e danosos. Tim Chase, CISO (Chief Information Security Officer — Diretor de Segurança da Informação) na plataforma de dados Lacework, afirma que *hackers* podem usar IA generativa para criar códigos capazes de provocar grandes danos em sistemas industriais, podendo causar manifestações físicas (Williams, 2024). Ademais, segundo Chase, a inteligência artificial é capaz de tornar ataques cibernéticos aos sistemas industriais uma tarefa muito mais fácil para um *hacker* mediano; para Chase, quanto mais fácil se tornar esses ataques, maior será a frequência com que ocorrerão.

No setor hídrico, a digitalização, impulsionada pelo paradigma da Agricultura 4.0 e pelo uso da IA no monitoramento da qualidade da água (ODS 6), expõe vulnerabilidades. Um ciberataque, seja em um sistema de irrigação inteligente, seja em uma infraestrutura de saneamento, pode levar à perda de controle de qualidade, contaminação ou lançamento de esgoto em rios e parques, devastando o ecossistema local. No limite, a ameaça de ruptura de barragens reitera o argumento de Dalby (2022) de que a segurança está agora ameaçada por arranjos políticos e técnicos que não são primariamente militares.

Portanto, e guardadas as devidas proporções, não é excessivo tomar-se medidas preventivas de cibersegurança as quais evitem um novo Caso *Stuxnet*[2],

[2] O Stuxnet é considerado por especialistas em segurança a primeira “arma cibernética” do mundo projetada para causar destruição física no mundo real. Descoberto em 2010, o vírus foi uma peça de *malware* altamente sofisticada,

mas com danos ambientais equiparáveis ao acidente de Chernobyl. Assim sendo, os cenários supracitados são extremos, mas inteiramente plausíveis.

CONSIDERAÇÕES FINAIS

A partir da pergunta “como as novas tecnologias podem contribuir para a securitização do meio ambiente?”, estruturamos um desenho de pesquisa baseado em métodos mistos, com o intuito de apresentar formas de explorar essa questão. Primeiramente, realizamos um mapeamento original dos ataques cibernéticos com potencial impacto no meio ambiente. Esses ataques, ainda que não especificados como ou comprovadamente conduzidos por IA, nos permitem imaginar os possíveis prejuízos oriundos de ataques cibernéticos empregados por inteligência artificial. A partir das análises descritivas de incidentes cibernéticos com potenciais implicações ambientais, esse trabalho contribui com uma recente virada nos estudos cibernéticos para uma produção mais empírica. Nossos principais achados reforçam a tendência de uma maior securitização da agenda ambiental devido ao aumento no número de ataques em anos recentes.

Apesar de uma perspectiva de securitização individualista ou de segurança humana em relação à questão do meio ambiente, a maior parte dos incidentes são promovidos e possuem como alvos os governos nacionais. A prevalência desses fatores pode ser explicada

desenhada especificamente para atacar os sistemas de controle industrial (SCADA) da Siemens, utilizados nas instalações de enriquecimento de urânio do Irã, em Natanz (Fildes, 2010).

tendo em vista que os setores mais impactados — o energético, petrolífero, nuclear e hídrico — tendem a ser administrados por órgãos e companhias estatais.

Dessa forma, os crescentes ataques aos governos nacionais com implicações ambientais implica uma maior necessidade de regulamentação e sistematização de processos de segurança voltados para a área. Nesse mesmo sentido, nossos achados reforçam uma demanda por uma maior produção acadêmica acerca de incidentes cibernéticos, segurança e defesa cibernéticas e meio ambiente.

Além disso, para garantir a sustentabilidade ambiental da IA, é fundamental antecipar e abordar os potenciais riscos e implicações associados à sua utilização, o que inclui preocupações de segurança cibernética, uma vez que os sistemas de IA podem ser vulneráveis a ataques e manipulações com consequências ambientais indesejáveis.

A utilização da IA no contexto ambiental é ambígua, podendo ser representada pela expressão “faca de dois gumes”. Se por um lado ela proporciona oportunidades sem precedentes de compreensão e resolução de questões ambientais complexas, por outro, a sua utilização sem respeito a princípios éticos e ao uso sustentável de energia pode ter consequências hostis para o meio ambiente e para a sociedade. Neste sentido, é crucial que os pesquisadores e os formuladores de políticas considerem tanto os benefícios como os desafios da IA para o meio ambiente, a fim de encontrar um caminho ponderado. O aprofundamento das discussões sobre Segurança Ambiental e o estudo das Ameaças

Digitais tornam-se, assim, imperativos para sustentar o processo de securitização da agenda ambiental na era do Antropoceno.

Para a agenda de pesquisa, identificamos a necessidade de mais pesquisas empíricas abordando a interseção entre os assuntos abordados neste trabalho, desde estudos comparativos sobre securitização na área em grupos de países distintos até estudos de caso sobre a estruturação das políticas ambientais em relação às novas tecnologias.

REFERÊNCIAS

AGÊNCIA ESTADO. Média diária de ataques cibernéticos cresceu 42% em 2012. *Estado de Minas*, Belo Horizonte, 16 abr. 2013. Disponível em: https://www.em.com.br/app/noticia/nacional/2013/04/16/interna_nacional,372394/media-diaria-de-ataques-ciberneticos-cresceu-42-em-2012.shtml. Acesso em: 12 nov. 2025.

BEVIR, Mark. Meta-methodology: Clearing the Underbrush. *In*: BOX-STEFFENSMEIER, Janet; BRADY, Henry E.; COLLIER, David (Eds.). *The Oxford Handbook of political methodology*. Nova York: Oxford University Press, 2008.

BISWAS, Niloy. Is the environment a security threat? Environmental security beyond securitization. *International Affairs Review*, Washington, D. C., v. 20, n. 1, p. 1-22, 2011. Disponível em: https://www.researchgate.net/publication/353356447_IS_THE_ENVIRONMENT_A_SECURITY_THREAT_Environmental_Security_beyond_Securitization. Acesso em: 12 nov. 2025.

BURTON, Joe; LAIN, Clare. Desecuritising cybersecurity: towards a societal approach. *Journal of Cyber Policy*, [*S. l.*], v. 5, n. 3, p. 449-470, 2020. Disponível em: https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1856903. Acesso em: 12 nov. 2025.

BUZAN, Barry. Rethinking Security after the Cold War. *Cooperation and Conflict*, [*S. l.*], v. 32, n. 1, p. 5-28, 1997. Disponível em: https://doi.org/10.1177/0010836797032001001. Acesso em: 12 nov. 2025.

BUZAN, Barry; WÆVER, Ole; WILDE, Jaap De. *Security*: A new framework for analysis. Colorado: Lynne Rienner Publishers, 1998.

CI-ISAC AUSTRALIA. Cyber threats to the Australian Water & Sewerage Sector. *LinkedIn*, [*S. l.*], 25 out. 2023. Disponível em: https://www.linkedin.com/pulse/cyber-threats-australian-water-sewerage-sector-ci-isac/. Acesso em: 12 nov. 2025.

CSIS. Significant Cyber Incidents. *CSIS*, Washington, D. C., 2025. Disponível em: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Acesso em: 12 nov. 2025.

DALBY, Simon. *Rethinking environmental security*. Cheltenham: Edward Elgar Publishing, 2022.

DAVIS, Zachary. Artificial Intelligence on the Battlefield: Implication for Deterrence and Surprise. *PRISM*, Arlington, v. 8, n. 2, p. 115-131, 2019. Disponível em: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM%208-2.pdf?ver=2019-10-28-122747-047. Acesso em: 12 nov. 2025.

FRANCISCO, Marie. Artificial intelligence for environmental security: national, international, human and ecological perspectives. *Current Opinion in Environmental Sustainability*, [*S. l.*], v. 61, p. 1-8, 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S1877343522001026?via%3Dihub. Acesso em: 12 nov. 2025.

FREESE, Jeremy; RAUF, Tamkinat; VOELKEL, Jan Gerrit. Advances in transparency and reproducibility in the social sciences. *Social Science Research*, Stanford, v. 107, p. 1-12, 2022. Disponível em: https://www.sciencedirect.com/science/article/pii/S0049089X2200076X?via%3Dihub#abs0010. Acesso em: 12 nov. 2025.

GERRING, John. Mere description. *British Journal of Political Science*, Cambridge, v. 42, n. 4, p. 721-746, 2012. Disponível em: https://www.cambridge.org/core/journals/british-journal-of-political-science/article/mere-description/833643C6242D3A45D48BAAC3EF0C33D0. Acesso em: 12 nov. 2025.

GUSTAFSSON, Karl; HAGSTRÖM, Linus. What is the point? Teaching graduate students how to construct political science research puzzles. *European political science*, [*S. l.*], v. 17, p. 634-648, 2018. Disponível em: https://link.springer.com/article/10.1057/s41304-017-0130-y. Acesso em: 12 nov. 2025.

FILDES, Jonathan. Irã foi alvo de 'guerra eletrônica', dizem especialistas. BBC Brasil, [*S. l.*], 23 set. 2010. Disponível em: https://www.bbc.com/portuguese/noticias/2010/09/100923_iran_virus_rc. Acesso em: 04 dez. 2025.

KESLER, Brent. The Vulnerability of Nuclear Facilities to Cyber Attack. *Strategic Insights*, Monterey, v. 10, n. 1, p. 1-11, 2011. Disponível em: http://large.stanford.edu/courses/2017/ph241/bunner2/docs/SI-v10-I1_Kesler.pdf. Acesso em: 12 nov. 2025.

LAUX, Jon; HONEA, Matthew. Silent Cyber Scenarios: Opening The Flood Gates. *AON*, [*S. l.*], 2018. Disponível em: https://www.aon.com/reinsurance/gimo/20181025-gimo-cyber. Acesso em: 12 nov. 2025.

LIRA BRITO, Renato Victor *et al.* As Novas Tecnologias e a Securitização do Meio Ambiente: uma análise de métodos mistos sobre os impactos da Inteligência Artificial. *In*: CONGRESSO ACADÊMICO SOBRE DEFESA NACIONAL (CADN), XIX., 2024, Rio de Janeiro. *Anais* [...] Rio de Janeiro: Zenodo, 2024. p. 1-20. Disponível em: https://zenodo.org/records/13334329. Acesso em: 12 nov. 2025.

MARSH, David; FURLONG, Paul. A skin not a sweater: ontology and epistemology in political science. *In*: LOWNDES, Vivien; MARSH, David; STOKER, Gerry (Eds.). *Theory and methods in Political Science*. Londres: Palgrave Macmillan, 2017.

MELO, Marlene; ANDRADE, Tatiana. Temas Controversos na Educação: Relações entre questões ambientais e surgimento de pandemias. *Periferia*, Rio de Janeiro, v. 16, n. 1, p. 1-30, 2024. Disponível em: https://www.e-publicacoes.uerj.br/periferia/article/view/75629. Acesso em: 12 nov. 2025.

NAGLI, Luiz. Pandemia na pandemia: a escalada de ataques cibernéticos pós COVID-19/Pandemic in pandemic: the climbing of post COVID-19 cyber attacks. *Brazilian Journal of Development*, Curitiba, v. 8, n. 4, p. 28482-28493, 2022. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/46768. Acesso em: 12 nov. 2025.

SHARIKOV, Pavel. Artificial Intelligence, Cyberattack, and Nuclear Weapons. *Bulletin of the Atomic Scientists*, Chicago, v. 74, n. 6, p. 368-373, 2018. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/00963402.2018.1533185. Acesso em: 12 nov. 2025.

WILLIAMS, Kevin. Cyber-physical attacks fueled by AI are a growing threat, experts say. *CNBC*, [*S. l.*], 3 mar. 2024. Disponível em: https://www.cnbc.com/2024/03/03/cyber-physical-attacks-fueled-by-ai-are-a-growing-threat-experts-say.html. Acesso em: 12 nov. 2025.

ESTUDOS UNIVERSITÁRIOS

UFPE PROEXT Pró-Reitoria de Extensão

Estudo

Texto recebido em: 14 out. 2025. Aprovado em: 31 out. 2025.

OLIVEIRA, Marcos Aurelio Guedes de; BRITO, Renato Victor Lira; CORIOLANO, Júlia Costa Amancio Santos; PASTICK, Júlia Cardoso Lima; DIAS, Maria Clara Miranda Bezerra; GUSMÃO, Taís Barbosa. As novas tecnologias e a securitização do meio ambiente: uma análise sobre os impactos da inteligência artificial. *Estudos Universitários*, Universidade Federal de Pernambuco/Pró-Reitoria de Extensão, Recife, v. 42, n. 1, e268280, jan./dez. 2025.

https://doi.org/10.51359/2675-7354.2025.268280

ISSN Edição Digital: 2675-7354