OBSERVARE
Universidade Autónoma de Lisboa
e-ISSN: 1647-7251
VOL15 N2, DT3
Dossiê Temático – *Clima e Segurança*
Abril 2025

JANUS.NET
e-journal of International Relations

O CIBERESPAÇO COMO CENÁRIO DE SEGURANÇA E DEFESA FACE ÀS ALTERAÇÕES CLIMÁTICAS

HELDER FIALHO JESUS
hmfj2009@gmail.com
Comandante da Marinha portuguesa, na reserva, com mais de trinta anos de experiência. Serviu embarcado em várias classes de navios, especializado em Comunicações e Guerra Eletrónica, com uma Pós-graduação em Sistemas de Informação, é auditor da Defesa Nacional e é o Vice-Presidente do Observatório dos Ecossistemas e Infraestruturas Digitais, OEID (Portugal). Foi o coordenador da Área da Marinha, no Instituto Universitário Militar (IUM) (2020-2023); Chefe do Centro de Ciberdefesa das Forças Armadas (2017-2020), primeiro representante nacional no Steering Committee do NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), na Estónia; e Chefe da Divisão de Comunicações e Sistemas de Informação do Comando Naval e Director do Centro de Comunicações, de Dados e de Cifra da Marinha (2015-2017). Tem uma comissão na NATO, no SHAPE - Bélgica (2009-2012), na área das Comunicações e Sistemas de Informação para as Operações Militares.

Resumo

Nos últimos anos, o ciberespaço tem-se consolidado como um elemento em destaque nas relações internacionais e na segurança global. Ao ser um componente fundamental na profunda interdependência da sociedade e com uma natureza dinâmica e sem fronteiras físicas, o ciberespaço desempenha um papel central em diversas dimensões da vida contemporânea, incluindo a gestão de crises climáticas. Neste contexto, as interseções entre cibersegurança, defesa nacional e alterações climáticas emergem como áreas importantes para políticas públicas e estratégias nacionais e internacionais, às quais os recentes desenvolvimentos em inteligência artificial vieram trazer soluções e complexidade.

Palavras-chave

Cibersegurança, tecnologia, resiliência, ciberataque, inteligência artificial.

Abstract

Recently, cyberspace has established itself as a prominent element in international relations and global security. Cyberspace, a fundamental component in the deep interdependence of society, plays a central role in several dimensions of contemporary life, including the management of climate crises. In this situation, the areas where cybersecurity, national defense, and climate change meet seem to be crucial for national and international public policies and strategies. New developments in artificial intelligence have added both ease and complexity to these areas..

Keywords

Cybersecurity, technology, resiliency, cyber-attack, artificial intelligence.

Como citar este artigo
Jesus, Helder Fialho (2025). O ciberespaço como cenário de segurança e defesa face às alterações climáticas. *Janus.net, e-journal of international relations*. VOL15 N2, TD3 – Dossiê Temático – Clima e Segurança. Abril de 2025, pp. 71-87. DOI https://doi.org/10.26619/1647-7251.DT0225.4.

Artigo submetido em 8 de março de 2025 e aceite para publicação em 23 de março de 2025.

O CIBERESPAÇO COMO CENÁRIO DE SEGURANÇA E DEFESA FACE ÀS ALTERAÇÕES CLIMÁTICAS

HELDER FIALHO JESUS

"People everywhere are hoping for a future of peace, dignity, and prosperity."

António Guterres, *Opening remarks to the summit of the future*, New York, 22 September 2024

O papel do ciberespaço no contexto das alterações climáticas

As alterações climáticas são um processo global multifacetado, caracterizado por alterações substanciais nos padrões climáticos e nas temperaturas ambiente durante períodos prolongados, induzidas principalmente pelo aumento de gases com efeito de estufa e pelo esgotamento dos recursos naturais. O aquecimento global resultante e os fatores de risco associados têm repercussões extensas e complexas, afetando significativamente a sociedade, sendo as alterações climáticas amplamente reconhecidas como uma das maiores ameaças globais do século XXI (Nações Unidas, s.d.). O Acordo de Paris, de 2015, constitui-se como uma referência visando limitar o aquecimento global e fazer face aos respetivos impactos, vinculando juridicamente os seus signatários a agirem para combater as alterações climáticas (Conselho Europeu, 2024). Eventos climáticos extremos, como furacões, inundações e secas prolongadas, têm-se intensificado, colocando em risco populações, ecossistemas e infraestruturas críticas. O ciberespaço, por sua vez, oferece ferramentas essenciais para a gestão e mitigação desses impactos. Com a implementação de sistemas digitais consegue-se fazer a recolha e análise de dados meteorológicos, a monitorização de desastres naturais em tempo real e a coordenação de respostas rápidas e integradas. De acordo com o *World Economic Forum* (WEF) seis tecnologias são críticas para a adaptação ao clima, sendo elas a inteligência artificial, os drones, a observação da Terra, a computação avançada, a Internet das Coisas e a realidade virtual e aumentada (Masterson, 2024).

Entretanto, essa dependência de tecnologias digitais torna as nações vulneráveis a ciberataques. Assim, as infraestruturas críticas, como as redes elétricas, os sistemas de abastecimento de água e as plataformas de comunicação, podem ser alvo de sabotagem durante crises climáticas, agravando os impactos desses eventos. A convergência entre o ciberespaço e as alterações climáticas exige, assim, uma abordagem integrada que contemple tanto a mitigação dos riscos ambientais quanto a proteção contra ameaças digitais ou físicas. E aqui, o conceito Proteção, Segurança e Defesa (PSD) tem a sua aplicabilidade, ao adotar uma visão holística para a proteção física das Infraestruturas

críticas, para a segurança dos seus sistemas, dados e informação, bem como na sua defesa contra agentes externos (Jesus, 2023).

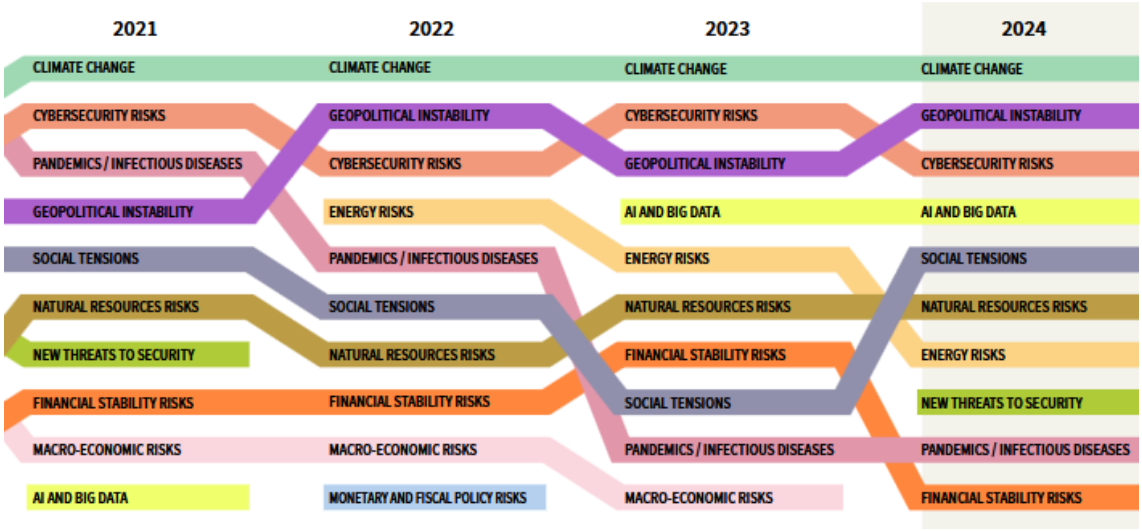
Cibersegurança e alterações climáticas: novos paradigmas

A compreensão das três camadas características do ciberespaço[1] é fundamental para estruturar as análises a este ambiente. No presente contexto, a segurança no ciberespaço envolve a proteção, a segurança e a defesa de infraestruturas estratégicas que sustentam as sociedades modernas. Num cenário de alterações climáticas, a segurança nacional enfrenta desafios adicionais, na medida em que as crises ambientais podem ser exploradas por atores mal-intencionados, estatais ou não estatais. No entanto, não existe uma relação causal direta entre as alterações climáticas e a cibersegurança (Shea, 2023), podendo sim, haver um aproveitamento por cibercriminosos de situações criadas pelas alterações climáticas, com preocupações na área financeira já notadas (Aspinall, s.d.). Por exemplo, uma disrupção que surja durante um furacão pode interromper sistemas de energia e comunicação, dificultando os esforços de socorro (camada física e lógica). Além disso, a desinformação disseminada nas redes sociais pode minar a confiança pública nas autoridades e nas medidas adotadas, comprometendo ainda mais a capacidade de resposta (camada semântica), naquilo que Thiago Braga considera como "crise informacional global e outras crises interconectadas (como a ambiental, a geopolítica e a guerra) que formam uma espécie de policrise" (Agência Gov, 2024).
Para mitigar esses riscos, é importante o investimento em sistemas resilientes e seguros e aproveitar os desenvolvimentos tecnológicos, como por exemplo os seis acima referidos pela WEF para reforçar a proteção de dados, da informação e prever padrões de disrupção intencional. Por sua vez, o Chefe da Defesa das Forças Armadas Holandesas, General Tom Middendorp, no seu livro "*The Climate General- Stepping up the fight*", apresenta a ligação entre as alterações climáticas e a segurança global e o seu efeito na sociedade, tanto do ponto de vista da defesa nacional como da cibersegurança (Middendorp e Campen, 2023).

O relatório que a AXA publica anualmente relativo aos riscos (Axa, 2024) mostra que as alterações climáticas estão no topo das preocupações desde o relatório de 2021, onde as preocupações com a cibersegurança e a instabilidade geopolítica vão alternando de ano para ano, conforme figura abaixo, mostrando a importância destes temas.

[1] Três camadas: Física, lógica e semântica. Cyberspace Operations, Joint Publication 3-12 https://irp.fas.org/doddir/dod/jp3_12.pdf https://irp.fas.org/doddir/dod/jp3_12.pdf

Figura 1 - Evolução da percentagem de seleção dos principais riscos por parte dos especialistas (2018-2024)



Fonte: AXA Future Risks Report 2024

Alterações climáticas como multiplicador de ameaças no Ciberespaço

As alterações climáticas atuam como multiplicadoras de ameaças ao intensificar as tensões sociais e económicas em diferentes regiões. Secas prolongadas, escassez de recursos hídricos e deslocamentos populacionais em massa criam cenários propícios para conflitos. No ciberespaço, esses cenários são ampliados pela possibilidade de manipulação de informação (camada semântica), espionagem (camada lógica) e ataques a sistemas críticos (camada lógica e física).

As alterações climáticas já fazem parte da agenda da área da defesa (JRC, 2023). Por sua vez, as Forças Armadas de diversos países já reconhecem o impacto das alterações climáticas no contexto da sua defesa, com o estabelecimento de procedimentos de interagência ao mais alto nível (DOD, 2016). Por outro lado, alterações climáticas originando crises humanitárias obrigam a uma grande mobilização de recursos logísticos e tecnológicos, pelo que o ciberespaço é um elemento indispensável para prever, planear e executar atividades em contextos de alta complexidade. Nesse sentido, o *International Military Council on Climate and Security* (IMCCS) pode constituir-se como um exemplo, ao ser uma rede de líderes militares visado apoiar a elaboração de políticas com implicações de segurança num contexto de alterações climáticas.

No caso dos EUA, é assumido que as missões e operações do Departamento de Defesa (DOD) são negativamente afetadas pelas alterações climáticas através da amplificação das exigências operacionais da força, da degradação das instalações, infraestruturas e sistemas e do aumento dos riscos para a saúde dos militares e civis envolvidos (DoD, 2024). O setor da defesa é composto por mais de 200.000 empresas e agências (GAO, 2022), e cada uma desempenha naturalmente um papel importante na sensibilização para as alterações climáticas e na cibersegurança por detrás de sistemas críticos. Assim, ao serem implementadas medidas de cibersegurança para proteger as energias

renováveis, a monitorização climática e a análise de dados, reconhece-se a dificuldade das ameaças, cuja complexidade aumenta com as alterações climáticas. O planeamento estratégico envolve a realização de análises completas dos riscos climáticos para compreender os potenciais impactos nas estratégias de defesa e integrar as considerações climáticas em todos os níveis de planeamento.

Apesar de serem domínios separados, o ciberespaço e a atmosfera apresentam problemas análogos de sobre-exploração, dificuldade de aplicação da lei e obstáculos relacionados com a inação coletiva e o comportamento de aproveitamento (Shackelford, 2020). As alterações climáticas são um problema global, caracterizado por alterações nos padrões climáticos, aumento do nível do mar e temperaturas projetadas que ultrapassam os 1,5 graus Celsius até 2100. No entanto, as suas vantagens são amplamente distribuídas, enquanto os seus prejuízos são frequentemente concentrados. Da mesma forma, uma parte significativa das despesas associadas aos ciberataques está concentrada em poucos países, enquanto outros estão a emergir como santuários para os cibercriminosos. No entanto, também é verdade que as atividades realizadas por vários indivíduos em pequena escala podem influenciar tanto a questão das alterações climáticas globais como o avanço de uma cultura mundial de cibersegurança.

Cooperação internacional e resiliência digital

A colaboração em matéria de cibersegurança e de conservação ambiental exige vários tipos de ligações, como as que existem entre governos, agências de segurança pública e as partes interessadas (Cassotta & Pettersson, 2019). Estas várias modalidades de cooperação podem manifestar-se como cooperação bilateral, exemplificada pelos acordos multilaterais de auxílio jurídico mútuo, cooperação bilateral informal, como contactos policiais individuais, ou cooperação multilateral formal, como se verificou no Conselho da Europa, com a Convenção Europeia sobre Cibercrime, vulgarmente designada por "Convenção de Budapeste"[2]. Tanto na cibersegurança como nas estruturas de proteção ambiental, a obrigação de cooperar, enquanto princípio fundamental do direito internacional, é pertinente, particularmente no contexto dos bens comuns globais, que tem em Elinor Ostrom, Prémio Nobel da Economia em 2009, a sua grande referência. Um exemplo ilustrativo de um acordo multilateral é a Convenção das Nações Unidas sobre o Direito do Mar (CNUDM), que constitui a moldura jurídica de referência do direito internacional do mar contemporâneo, onde que a necessidade de cooperação é articulada no seu artigo 197.º.[3]

Mas já em 2008, na "Declaração para o futuro da economia da internet", mais conhecida por "Declaração de Seul"[4], as preocupações com a cibersegurança, as alterações climáticas e a importância da cooperação estavam presentes, ao ser referido que importava promover os objetivos estabelecidos nessa Declaração, através da cooperação

[2] Convenção aprovada pela Resolução da Assembleia da República n.º 88/2009, de 15/09; e ratificada pelo Decreto do Presidente da República n.º 91/2009, de 15/09. Disponível em https://www.ministeriopublico.pt/instrumento/convencao-sobre-o-cibercrime-0

[3] A convenção estabelece um regime jurídico para os mares e oceanos, definindo regras aplicáveis a todas as utilizações dos oceanos e respetivos recursos. Disponível em https://eur-lex.europa.eu/PT/legal-content/summary/united-nations-convention-on-the-law-of-the-sea.html

[4] Declaration for the Future of the Internet Economy (The Seoul Declaration) (2008), disponível em https://legalinstruments.oecd.org/public/doc/113/113.en.pdf

entre múltiplos stakeholders, e a necessidade de se identificar o impacto da Internet e das TIC no combate às alterações climáticas, bem como na melhoria da eficiência energética. Ainda sobre a cooperação, foi realçado que se deveria aumentar a cooperação transfronteiriça entre os governos e as autoridades responsáveis pela aplicação da lei nas áreas da melhoria da cibersegurança, do combate ao spam, bem como da proteção da privacidade, dos consumidores e dos menores.

Mais recentemente, a "Declaração para o futuro da internet"[5], publicado pelo Departamento de Estado dos EUA e por mais de 60 países signatários e parceiros, em abril de 2022, refere que a tecnologia desempenha um papel fundamental na "luta contra as alterações climáticas globais", o que torna a proteção da tecnologia ainda mais urgente, onde a cibersegurança será fundamental. Igualmente aqui é referido que se deve "cooperar para maximizar os efeitos facilitadores da tecnologia no combate às alterações climáticas e na proteção do ambiente, reduzindo ao máximo a pegada ambiental da Internet e das tecnologias digitais". Por sua vez, a cooperação deveria ser estendida em matéria de investigação, inovação e definição de normas, e reafirma o compromisso com a estrutura de comportamento estatal responsável no ciberespaço, tendo em vista combater o cibercrime e impedir atividades maliciosas no ciberespaço.

Por sua vez, a interdependência global no ciberespaço requer soluções coletivas para desafios comuns. Pelo impacto que as alterações climáticas têm na sociedade, as governanças do ciberespaço e climáticas devem ser pensadas de forma coordenada, reunindo esforços de governos, sociedade civil, setor privado e organizações regionais entre outros, conforme decorreu da cimeira do Futuro das Nações Unidades em setembro de 2024 (United Nations, 2024). A colaboração entre partes e iniciativas como parcerias público-privadas e tratados internacionais podem ajudar a definir normas para o uso ético e seguro do ciberespaço em contextos de alterações climáticas, ajudando à sua governação (Sol, 2024). Além disso, é fundamental promover a educação e conscientização sobre segurança digital e sustentabilidade ambiental. Uma população mais informada e preparada é menos vulnerável a desinformação e ciberataques, contribuindo assim para a confiança nas instituições e para sociedades mais resilientes (OECD, 2021).

Compromissos de sustentação tecnológica

De notar ainda que existem várias semelhanças entre os desafios representados pelas alterações climáticas e a cibersegurança, as quais requerem mudanças comportamentais, investimento em inovação, regulamentação rigorosa e colaboração entre setores e interesses, conforme é apresentado por Barbara Maigret (2022). Ao fazer o paralelismo entre as alterações climáticas e a cibersegurança, ela argumenta que ambas são preocupações prementes para os governos, empresas e indivíduos. A inovação é outra área onde estas questões críticas se cruzam. A tecnologia desempenha um papel crucial ao ajudar a sociedade a reestruturar os sistemas e as infraestruturas necessárias para alcançar e manter uma sociedade sustentável. Refere que a inovação tecnológica verde em todos os setores é essencial para enfrentar o desafio global das

[5] Declaration for the Future of the Internet (2022), disponível em https://www.state.gov/declaration-for-the-future-of-the-internet

alterações climáticas. As fontes de energia renováveis, os transportes sustentáveis, os processos de fabrico limpos, os edifícios ecológicos e os dispositivos com maior eficiência energética desempenham um papel fundamental na entrega de um desempenho ambiental consideravelmente melhorado.

De acordo com a *World Meteorological Organization* apenas 0,5 por cento da água da Terra é água doce, verificando-se que as alterações climáticas estão a ter impacto nesse abastecimento. Nos últimos vinte anos, o armazenamento de água terrestre – incluindo a humidade do solo, a neve e o gelo – diminuiu a uma taxa de 1 cm por ano, com grandes ramificações para a segurança hídrica (WMO, 2021). A dependência crescente das sociedades do elemento digital, obriga naturalmente a um aumento de data centers[6] para dar as respostas necessárias, as quais são cada vez mais exigentes em termos tecnológicos como ambientais, onde a cibersegurança é um elemento preponderante para a confiança. Relativamente às questões ambientais, verifica-se que o crescimento destes centros tem impacto nas redes elétricas, nas emissões de gases com efeito de estufa e nas grandes necessidades de água para efeitos de arrefecimento (McGrath e Alamamos, 2024). No relatório ambiental de 2023 da Google, no que à água diz respeito, é referido que os seus data centers consumiram 5,2 mil milhões de galões de água durante 2023 (Google, 2023), correspondendo a cerca de 20 mil milhões de litros de água. Isto representa uma média de aproximadamente 500.000 litros de água por *data ce*nter por dia (Melamedov, 2024), o que é muito significativo. No presente contexto de alterações climáticas a inovação é fundamental para se encontrarem soluções criativas, sendo fundamental a monitorização dos consumos de águas, pois apenas 50% dos data centers o fazem. Outras soluções podem passar pela substituição dos seus sistemas legados de arrefecimento de modo a reduzir os consumos de água e energia, na localização dos data centers em regiões mais frias ou em zonas junto ao mar, tendo em vista auxiliar o arrefecimento, reduzindo assim a necessidade de sistemas de arrefecimento mecânico.

A relação entre desenvolvimento tecnológico, as alterações climáticas e a cibersegurança

Interessante de notar que o WEF *Global Risks Report* 2025 (WEF, 2025) infere que a cibersegurança, as alterações climáticas e o desenvolvimento tecnológico estão interligados de várias formas, criando riscos complexos e interdependências, enunciando-se por exemplo os ataques a infraestruturas críticas. As alterações climáticas podem causar eventos climáticos extremos que danificam infraestruturas críticas, tornando-as mais vulneráveis a ciberataques. Independentemente do tipo de infraestruturas (energia, água, transportes), a interrupção de serviços essenciais aumenta a dificuldade nos esforços de resposta a emergências. Por outro lado, são também referidas a desinformação e a polarização social, as quais impulsionadas pelo desenvolvimento tecnológico com novas plataformas digitais podem agravar as tendências em torno das alterações climáticas, dificultando a implementação de soluções eficazes. De referir, ainda, que a desinformação, está classificada em primeiro lugar nos

[6] Os data centers são uma infraestrutura com um grande grupo de servidores de computador que armazenam, gerem e processam dados.

"Riscos globais classificados por gravidade a curto e longo prazo", num horizonte de 2 anos, decorrente da preocupação nos setores privado e do governo e no meio académico. Um outro aspeto em alerta são os chamados avanços biotecnológicos, os quais, impulsionados pela IA, apresentam oportunidades para mitigar as alterações climáticas, mas também criam novos riscos. A utilização maliciosa da biotecnologia, facilitada por ciberataques, pode ter consequências devastadoras para a saúde humana e para os diversos ecossistemas da natureza. Como soluções são consideradas as respostas multilaterais, que são essenciais para abordar os riscos das alterações climáticas e do desenvolvimento tecnológico. Os tratados e acordos globais podem promover a partilha de informação, a coordenação de políticas bem como a criação de normas para mitigar estes riscos. Neste caso, seria necessário promover igualmente a literacia digital, melhorar a responsabilização e a transparência, e investir em soluções tecnológicas. Por fim, tendo em vista criar um futuro mais seguro e sustentável, é essencial a colaboração entre os setores público e privado, a sociedade civil e o meio académico.

A inovação tecnológica pode mitigar o impacto adverso dos riscos advindos pelas alterações climáticas no desempenho financeiro das empresas. Esta situação ficou demonstrada num estudo de Zhao & Parhizgari (2024), numa análise aos dados de 46 países, num período compreendido entre 2011 e 2018, na relação entre inovação tecnológica e alterações climáticas. Este estudo refere ainda que as empresas localizadas em países com alta taxa de inovação demonstram uma maior confiança no futuro, o que lhes permite estar menos preocupadas com o impacto das alterações climáticas, situação esta que tem consequências diretas nas questões ligadas à cibersegurança.

A segurança face à Inteligência artificial nas alterações climáticas

A cibersegurança está intrinsecamente relacionada com a integração da IA, na transição energética, uma vez que a crescente digitalização dos sistemas de energia torna-os mais vulneráveis a ciberataques. Isto porque a IA pode ajudar a melhorar a segurança e a estabilidade dos sistemas de energia, mas também pode ser alvo de ataques (Wang & al, 2025). E podem apresentar-se algumas formas de relacionar a cibersegurança com a transição energética impulsionada pela IA, nomeadamente porque os ciberataques podem ter como alvo os algoritmos de *machine learning*, contornando os sistemas de segurança de IA, sendo mais subtis e perigosos do que os ataques comuns. Por sua vez, a interligação entre o ciberespaço e o mundo físico pode levar a ataques ou falhas que se propagam de um domínio para outro, representando riscos significativos no mundo real. Complementarmente, os riscos e perdas podem alastrar-se por vastas áreas e até além-fronteiras. De acordo com este trabalho de Wang, entre 2011 e 2017, o setor energético dos EUA sofreu mais de 400 intrusões e um outro estudo aqui referido demonstra que o impacto de um ciberataque em grande escala na rede de energia de Londres pode atingir 111 milhões de libras esterlinas, com possíveis perturbações na eletricidade, caminhos de ferro, telecomunicações e água potável. Relativamente aos métodos de ataque que visam especificamente os algoritmos de *machine learning* (ML) existem várias técnicas, entre elas os ataques a *Generative Adversarial Networks* (GAN)[7].

[7] *Generative Adversarial Network* (GAN) - corresponde a uma arquitetura de *deep learning*, que treina duas redes neurais para competirem entre si de modo a gerarem novos dados mais autênticos a partir de um

Ainda na vertente da transição energética é igualmente interessante a análise à aplicação da IA e de *machine learning* em modelos energéticos e de alterações climáticas. Isto porque exploram como estas tecnologias conseguem melhorar a previsão da procura energética, a otimização das redes de distribuição e a manutenção de fontes de energia renováveis. Como exemplo, Shobanke, Bhatt & Shittu (2025) fizeram uma análise de como estas tecnologias têm apoiado e promovido os sistemas de gestão de energia e a modelação das alterações climáticas, avaliando igualmente os desafios, as limitações e as oportunidades da integração da IA nos sistemas energéticos, bem como o seu impacto nas estratégias de mitigação das alterações climáticas. Aqui incluem-se estudos de caso, modelos e conjuntos de dados para ilustrar os benefícios e as potenciais aplicações futuras da IA nestes domínios.

A Inteligência artificial e a segurança dos dados nas alterações climáticas

A IA oferece avanços significativos na ação climática e na cibersegurança, mas acarreta riscos inerentes à segurança dos dados. A proteção de dados sensíveis, a implementação de fortes medidas de cibersegurança e a consciencialização sobre as ameaças são cruciais para uma utilização responsável da IA (UNFCCC, 2024). A falta de proteção de dados, particularmente nos países em desenvolvimento, pode comprometer a confiança pública e a eficácia das iniciativas baseadas em IA. A colaboração entre decisores políticos, indústria e investigadores é essencial para o desenvolvimento de estratégias de segurança adaptáveis, bem como para garantir que a IA contribui de forma segura para a sustentabilidade ambiental global. A gestão de segurança da IA requer medidas de proteção contra acessos não autorizados e atividades maliciosas, incluindo a identificação de ameaças e o controlo de acessos.

A Segurança dos dados é uma preocupação, porque a utilização de IA para ação climática envolve a recolha e a análise de grandes volumes de dados (*Big Data*), o que gera preocupações significativas em relação à privacidade e segurança dos mesmos. Entre estes destaca-se o risco de acesso não autorizado, a má utilização ou exploração de dados sensíveis (por exemplo, dados sobre uso do solo, práticas agrícolas, informações comunitárias) que é real e pode comprometer a confiança pública. Um outro elemento de alerta é a falta de estruturas robustas de proteção de dados, especialmente em países em desenvolvimento, o que agrava este tipo de riscos. Relativamente à criação de efeitos através de ciberataques, e uma vez que os sistemas de IA são suscetíveis a ataques de *data poisoning*[8], pode verificar-se uma alteração do comportamento dos sistemas de

determinado conjunto de dados. E designa-se de adversária porque treina duas redes diferentes, colocando-as uma contra a outra. Assim, uma rede gera novos dados com base numa amostra de dados de entrada modificando-os o máximo possível. Por sua vez, a outra rede tenta prever se a saída de dados gerada pertence ao conjunto de dados original (https://aws.amazon.com/what-is/gan/).
Deep learning - método de IA que ensina os computadores a processar dados inspirados no cérebro humano. Os modelos de *deep learning* conseguem reconhecer padrões complexos em imagens, texto, sons e outros dados para produzir *insights* e previsões precisas. É possível usar métodos de *deep learning* para automatizar tarefas que normalmente exigem inteligência humana, como descrever imagens ou transcrever um arquivo de som em texto (https://aws.amazon.com/what-is/deep-learning/).
[8] *Data poisoning* - O envenenamento de dados é um ciberataque no qual os adversários alteram ou comprometem os dados de treino utilizados para o desenvolvimento de modelos de IA e de ML. As redes neuronais, os *large language models* e os modelos de *deep learning* dependem fundamentalmente da qualidade

forma imprevisível. Por outro lado, o armazenamento e processamento de dados por sistemas de IA, se não for efetuado de forma cuidadosa e segura, pode expor informação sensível a partes não autorizadas, tanto internas como externas às organizações, com os problemas que daí podem advir.

Os dados relacionados com o clima devem ser geridos com a devida diligência. Os dados devem ser adquiridos, processados e disseminados de uma forma que preserve a confiança, mas respeitando adequadamente a privacidade e a segurança. Alguns dados pertinentes relativos às aplicações climáticas podem ser significativamente sensíveis em relação a questões de privacidade. Existe a preocupação de que o acesso ou a gestão irresponsável de dados em projetos de IA relacionados com o clima possa corroer a confiança na IA em setores específicos. Além disso, os ecossistemas de dados abertos devem ser estruturados de forma a honrar as necessidades e os interesses das comunidades das quais os dados têm origem, especialmente aquelas que foram historicamente desfavorecidas ou menorizadas. E para isto, a aplicação de normas e regras de cibersegurança é fundamental.

Importará ainda referir que a recolha de dados relevantes para o clima é diferenciada. Isto porque a recolha de dados e a sua subsequente disponibilidade para algoritmos de IA estão predominantemente concentradas naquilo que agora se chama o Norte Global (Amiri & al, 2024). Assim, seria relevante que organizações internacionais considerassem facilitar o desenvolvimento de processos de recolha de dados nos países de baixo rendimento e no Sul Global, de modo a melhorar a distribuição geográfica dos dados.

Inteligência Artificial e riscos

Utilizar a IA traz riscos como preconceito, invasão de privacidade, vulnerabilidades de segurança, preocupações de segurança e aumento das emissões de gases com efeito de estufa (ICEF, 2023). Relativamente aos riscos relacionados com preconceitos no emprego de IA para mitigações climáticas, estes envolvem o favorecimento de grupos específicos devido a disparidades na acessibilidade dos dados. Os riscos relacionados com a privacidade incluem violações ilegais de dados de terceiros, a identificação de pessoas e questões de vigilância. Podem surgir vulnerabilidades de segurança à medida que os sistemas de IA alargam a superfície de ataque aos cibercriminosos, para além do que está presente nas aplicações de *software* tradicionais. Os riscos de segurança podem ser significativos quando os sistemas de IA apresentam avarias ou produzem resultados imprevistos. As emissões de gases com efeito de estufa provenientes de processos computacionais de IA são atualmente mínimas — substancialmente abaixo de 1% do total global. São necessários procedimentos de recolha e avaliação de dados melhorados para gerar uma estimativa mais precisa e com maior confiança. As projeções de emissões

e integridade dos dados de treino, que, em última análise, determinam as capacidades de um modelo. Estes dados de formação podem ter origem em diversas fontes, entre elas a internet, bases de dados governamentais, académicas ou empresariais e de fornecedores de dados externos. Os atores mal-intencionados podem modificar subtil ou significativamente o comportamento de um modelo introduzindo pontos de dados imprecisos ou enviesados (dados envenenados) nos conjuntos de dados de treino. A adulteração de dados através de envenenamento pode resultar numa classificação incorreta dos dados, diminuindo assim a utilidade e a precisão dos sistemas de IA e de ML. Além disso, estes ataques podem representar ameaças significativas à cibersegurança, particularmente em setores como a saúde e os veículos autónomos (https://www.ibm.com/think/topics/data-poisoning).

futuras de gases com efeito de estufa associadas à IA são pouco conhecidas. Em determinadas circunstâncias, projeta-se que as emissões de gases com efeito de estufa da IA diminuam nos próximos anos.

Inteligência Artificial e ambientes de segurança

A transversalidade dos assuntos de segurança e da IA é um elemento que estará cada vez mais na ordem do dia. Neste sentido, é interessante de se ver o trabalho realizado por Marie Francisco (2023), que fez uma análise ao papel da IA na segurança ambiental, analisando como diferentes perspetivas de segurança moldam a sua implementação. A autora examina como a IA se encaixa em discursos de segurança nacional, internacional, humana e ecológica, com o potencial para a militarização, para a cooperação global e para o alcance dos objetivos de desenvolvimento sustentável (ODS) da ONU, bem como para a alteração das perceções do ambiente.

Começando pelo primeiro ponto, da segurança nacional, considera que IA é vista como uma ferramenta para proteger os interesses do Estado em conflitos induzidos pelo clima, incluindo o seu uso para fins militares e de desinformação. Utiliza a Rússia como um exemplo de um país que utiliza a IA para semear instabilidade política nos seus adversários através da "*cyber-psychological warfare*". Relativamente à segurança Internacional considera que as organizações internacionais podem utilizar a IA para atingir os seus ODS, sendo um exemplo a gestão de migrações internacionais. No entanto, indica como potenciais impactos negativos no ambiente o facto de as empresas transnacionais poderem recorrer à IA para acelerar a extração de recursos. A autora considera ainda a situação da colaboração público-privada para fins militares, a qual poderá dificultar os movimentos ambientais. Sobre a Segurança Humana, cujo conceito é reconhecido pela primeira vez em 1994, no Relatório de Desenvolvimento Humano publicado no âmbito do Programa das Nações Unidas para o Desenvolvimento (PNUD 1994), Marie considera que IA pode ser vista como uma ferramenta para alcançar igualmente os ODS. Exemplifica com a utilização de aplicações específicas no contexto da análise dos dados para identificar a poluição da água, ou mesmo a utilização de smartphones para diagnosticar doenças em culturas agrícolas. No entanto, alerta para o risco de a IA incrementar as desigualdades, ou perpetuar os preconceitos de género e criar dependências entre países desenvolvidos e em desenvolvimento. O quarto e último ponto refere-se à segurança ecológica, centrando o seu discurso na forma como a IA molda a nossa compreensão do ambiente e como pode alienar-nos de outras visões do mundo. A construção de "florestas inteligentes" e a utilização de dados em tempo real podem esconder as implicações geopolíticas da construção e operação de sistemas de IA. Critica ainda o "pensamento algorítmico" por apresentar o conhecimento como objetivo e universal, marginalizando outras epistemologias.

Um olhar nacional sobre o tema

Portugal tem acompanhado a evolução das alterações climáticas, iniciando-se em 2004 com o Programa Nacional para as Alterações Climáticas (PNAC) (Schmidt, Delicado e Junqueira, 2021), e através de políticas e instrumentos de política pública para a ação

climática, de âmbito nacional e local (ADENE, s.d.). A participação em iniciativas internacionais, ao nível da ONU ou da EU, tem sido apanágio dos diversos governos, sendo o exemplo a mais recente a Conferência das Nações Unidas sobre as Alterações Climáticas, mais conhecida por COP29 (GovRP, 2024), em Baku, Azerbeijão. No entanto, foram os grandes incêndios de 2017, dos quais resultaram mais de uma centena de mortos, que se constituíram como o despertar do país coletivamente para as alterações climáticas, conforme referido na iniciativa "Cinco décadas de Democracia", quando foi discutido o tema de "Como preparar Portugal para as alterações climáticas?" (FFMS, 2024). E neste contexto, podem ainda elencar-se os relatórios das comissões técnicas independente a estes incêndios (AR, 2017 e AR, 2018) ao relevarem a evolução tecnológica e a necessidade de sistemas de comunicações mais atuais e robustos para as situações de emergência, onde o elemento de cibersegurança é fundamental para garantir a confidencialidade, integridade e disponibilidade das redes. De notar também no "Relatório Cibersegurança em Portugal - Riscos e Conflitos", promulgado pelo Centro Nacional de Cibersegurança (CNCS, 2024), a alusão às alterações climáticas, relativa ao risco de cibersabotagem e hacktivismo, em face do contexto internacional. Por sua vez, em março de 2024, o jornal Expresso organizou uma conferência subordinada ao tema "Desafios da Cibersegurança", tendo por base o *World Economic Forum*, que coloca a proteção digital das organizações ao nível de outros riscos globais como a inflação, as alterações climáticas ou os conflitos militares (Ferrão, 2024). Neste mesmo ano, em outubro, foi criado em Portugal o Observatório dos Ecossistemas e Infraestruturas Digitais (OEID)[9] pela importância do digital, da sua segurança e das infraestruturas a ele associadas.

Conclusão

A globalização, a evolução tecnológica e a aposta numa inovação contínua são elementos que contribuem para o aumento do risco digital sistémico. O ciberespaço está no centro de um mundo em transformação, onde a segurança e a defesa não podem ser dissociadas das alterações climáticas, face à diversidade de ameaças.

Sendo a IA uma tecnologia cada vez mais em uso na sociedade, existe a necessidade de abordar os riscos interligados da IA, da cibersegurança e das alterações climáticas em toda a extensão na relação entre estas três partes. Pela sua importância e impacto geral, a proteção de infraestruturas críticas e sistemas de energia impulsionados pela IA têm uma atenção específica. Por outro lado, a importância de *frameworks* para a proteção dos dados tendo em vista assegurar a privacidade e a confiança pública no uso da IA na ação climática é igualmente um elemento de garantia de conformidade e certeza para os resultados atingidos.

[9] O OEID visa a apresentação de contributos para as políticas públicas, junto de empresas e na sociedade em geral, quer no âmbito nacional quer internacional, bem como colaborar com entidades Governamentais, Académicas e entidades Públicas e Privadas para a definição de políticas de segurança e prevenção dos Ecossistemas e Infraestruturas Digitais em Portugal. Pretende ainda contribuir assim para um melhor esclarecimento da opinião pública sobre infraestruturas digitais nacionais e globais e sobre o papel de Portugal no mundo da conectividade digital.
https://www.linkedin.com/in/o-e-i-d-observat%C3%B3rio-dos-ecossistemas-e-infraestruturas-digitais-2ba27b331/?originalSubdomain=pt

Para enfrentar os desafios destes cenários, é necessário adotar uma abordagem multidisciplinar, investindo em tecnologias inovadoras, fortalecendo a cooperação e parcerias globais, bem como promovendo a resiliência digital, onde o fator confiança é fundamental. Somente assim será possível proteger infraestruturas críticas, garantir a segurança dos seus sistemas, dados e informação, reduzir vulnerabilidades e assegurar um futuro mais seguro e sustentável para as próximas gerações.

Referências

Adene (s.d.). Instrumentos de Política Pública para a Ação Climática: Âmbito Nacional e Local. Academia ADENE [Em linha]. Consultado em 29Dec2024. Disponível em https://academia.adene.pt/instrumentos-de-politica-publica-para-a-acao-climatica/

Agência Gov (2024). Desinformação e mudanças climáticas são grandes ameaças globais do século 21 [Em linha]. Consultado em 29Dec2024. Disponível em https://agenciagov.ebc.com.br/noticias/202408/desinformacao-e-mudancas-climaticas-sao-grandes-ameacas-globais-do-seculo-21

Amiri, Zahra; Heidari, Arash; Navimipour Nima (2024). Comprehensive survey of artificial intelligence techniques and strategies for climate change mitigation. Energy. Published by Elsevier Inc. https://doi.org/10.1016/j.energy.2024.132827

AR, Assembleia da República (2017). Análise e apuramento dos factos relativos aos incêndios que ocorreram entre 17 e 24 de junho de 2017. Comissão Técnica Independente. Disponível em https://www.parlamento.pt/Documents/2017/Outubro/Relat%C3%B3rioCTI_VF%20.pdf

AR, Assembleia da República (2018). Avaliação dos incêndios ocorridos entre 14 e 16 de junho de 2017 em Portugal Continental. Comissão Técnica Independente. Disponível em https://www.parlamento.pt/documents/2018/marco/relatoriocti190318n.pdf

Aspinall, Mike (s.d.). Climate Change and Cyber Security: What to Expect in Financial Services. Rutherford [Em linha]. Consultado em 29Dec2024. Disponível em https://www.rutherfordsearch.com/blog/2021/09/climate-change-and-cyber-security-what-to-expect-in-financial-services

Cassotta, Sandra & Pettersson, Maria (2019). Climate Change, Environmental Threats and Cyber-Threats to Critical Infrastructures in Multi-Regulatory Sustainable Global Approach with Sweden as an Example. Beijing Law Review>Vol.10 No.3, June 2019, DOI**:** 10.4236/blr.2019.103035. disponível em https://www.scirp.org/journal/paperinformation?paperid=93271

CE, Conselho Europeu (2024). Acordo de Paris sobre as alterações climáticas [Em linha]. Consultado em 29Dec2024. Disponível em https://www.consilium.europa.eu/pt/policies/paris-agreement-climate/

CNCS, Centro Nacional de Cibersegurança (2024). Relatório Cibersegurança em Portugal. Riscos & Conflitos 5ª Edição. Disponível em https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercncs.pdf

DOD, Directive 4715.21 (2016). Climate change adaptation and resilience [Em linha]. Consultado em 29Dec2024. Disponível em https://dod.defense.gov/portals/1/documents/pubs/471521p.pdf

Ferrão, Fátima (2024). Ciber(in)segurança no topo dos riscos. Expresso [Em linha]. Consultado em 29Dec2024. Disponível em https://expresso.pt/iniciativaseprodutos/projetos-expresso/2024-03-04-Ciber-in-seguranca-no-topo-dos-riscos-460f6914

FFMS, Fundação Francisco Manuel dos Santos (2024). Como preparar Portugal para as alterações climáticas? Cinco Décadas de Democracia-23 episódios [Em linha]. Consultado em 29Dec2024. Disponível em https://ffms.pt/pt-pt/ffms-play/cinco-decadas-de-democracia/como-preparar-portugal-para-alteracoes-climaticas

Francisco, Marie (2023). Artificial intelligence for environmental security: national, international, human and ecological perspectives. Open Issue 2023: Sustainability Science, Digitization and AI. Published by Elsevier Inc. https://doi.org/10.1016/j.cosust.2022.101250

GPAI, Global Partnership on AI Report (2021). Climate change and AI: Recommendations for Government Action. In collaboration with Climate Change AI and the Centre for AI & Climate. Disponível em https://www.gpai.ai/projects/climate-change-and-ai.pdf

Google (2023). Environmental Report [Em linha]. Consultado em 29Dec2024. Disponível em https://sustainability.google/reports/google-2023-environmental-report/

GovRP, Governo da República Portuguesa (2024). Portugal na COP29: ambição climática e cooperação internacional [Em linha]. Consultado em 29Dec2024. Disponível em https://www.portugal.gov.pt/pt/gc24/comunicacao/noticia?i=portugal-na-cop29-ambicao-climatica-e-cooperacao-internacional

ICEF, Innovation for Cool Earth Forum (2023). Artificial Intelligence for Climate Change Mitigation Roadmap (2023). Disponível em https://www.icef.go.jp/wp-content/uploads/2024/02/AI-Climate-Roadmap-ICEF-Dec-1-2023.pdf

Jesus, Helder (2023). A aplicabilidade do conceito "Proteção, Segurança e Defesa" para a Ciber-resiliência no contexto do atlântico português, Anais do Clube Militar Naval, Vol. CLIII, janeiro-junho 2023, p. 75-120

JRC, Joint Research Centre (2023). Impacts of climate change on defence-related critical energy infrastructure. Science for Policy report (JRC) - European Commission [Em linha]. Consultado em 29Dec2024. Disponível em https://eda.europa.eu/docs/default-source/brochures/climate-report.pdf

Maigret, Barbara (2022). Addressing cybersecurity and climate change for a sustainable society. Disponível em https://www.itp.net/insight/addressing-cybersecurity-and-climate-change-for-a-sustainable-society

Masterson, Victoria (2024). 6 technologies to help the world adapt to climate change. Centre for Nature and Climate - World Economic Forum climáticas [Em linha]. Consultado em 29Dec2024. Disponível em https://www.weforum.org/stories/2024/02/ai-climate-adaptation-technologies/

McGrath, Triona e Alamamos, Angelos (2024). Water use by data centres: An Irish Context. A Report Prepared for the Water Forum [Em linha]. Consultado em 29Dec2024. Disponível em https://thewaterforum.ie/app/uploads/2024/10/McGrath-2024-Data-Centre-Water-Use-in-Ireland-.pdf

Melamedov, Maxim (2024). How to cut water usage in cloud data centres. Data Centre Dynamics Ltd [Em linha]. Consultado em 29Dec2024. Disponível em https://www.datacenterdynamics.com/en/opinions/how-to-cut-water-usage-in-cloud-data-centers/

Middendorp, Tom e Campen, Antonie (2023). The Climate General: Stepping Up the Fight, Éditions la Butineuse, Auray

Nações Unidas (s.d.). Causas e Efeitos das Mudanças Climáticas [Em linha]. Consultado em 29Dec2024. Disponível em https://www.un.org/pt/climatechange/science/causes-effects-climate-change

OECD, Organisation for Economic Co-operation and Development- (2021). The E-Leaders Handbook on the Governance of Digital Government. OECD Digital Government Studies [Em linha]. Consultado em 29Dec2024. Disponível em https://www.oecd.org/en/publications/the-e-leaders-handbook-on-the-governance-of-digital-government_ac7f2531-en.html

Schmidt, Luísa e Delicado, Ana e Junqueira, Luís (2021). Políticas de alterações climáticas em Portugal: posicionamentos e redes de relações dos atores institucionais. Análise Social, LVI (3.º), 2021 (n.º 240). https://doi.org/10.31447/as00032573.2021240.03. Disponível em https://revistas.rcaap.pt/analisesocial/article/download/29675/21189/126490

Shackelford, Scott (2020). On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems. 18 *Vanderbilt Journal of Entertainment and Technology Law* 653 (2020). Disponível em https://scholarship.law.vanderbilt.edu/jetlaw/vol18/iss4/1

Shea, Sharon (2023). Where climate change and cyber attacks intersect. Informa TechTarget [Em linha]. Consultado em 29Dec2024. Disponível em https://www.techtarget.com/searchsecurity/feature/Where-climate-change-and-cyber-attacks-intersect

Shobanke, Mobolaji; Bhatt, Mehul; Shittu, Ekundayo (2025). Advancements and future outlook of Artificial Intelligence in energy and climate change modeling. Advances in Applied Energy. Published by Elsevier Inc. https://doi.org/10.1016/j.adapen.2025.100211

Sol, Kaya (2024). Intersecting Frontiers: International Governance in Environmentalism & Cybersecurity. The Henry M. Jackson School of International Studies / College of Arts and Sciences / University of Washington [Em linha]. Consultado em 29Dec2024. Disponível em https://jsis.washington.edu/news/intersecting-frontiers-international-governance-in-environmentalism-cybersecurity/

United Nations (2024). Summit of the Future, Our Common Agenda [Em linha]. Consultado em 29Dec2024. Disponível em

https://www.un.org/sites/un2.un.org/files/our-common-agenda-summit-of-the-future-what-would-it-deliver.pdf

UNFCCC, United Nation Framework Convention on Climate Change (2024). Draft technical paper on AI for climate action. Technology Executive Committee (REC). TEC-CTCN Advisory Board Joint session - Twenty-nineth meeting. Framework Convention on Climate Change. Disponível em https://unfccc.int/ttclear/misc_/StaticFiles/gnwoerk_static/tn_meetings/0ec396b0ba7b4d0d853b77c7b83dc172/3ebbf2e8e7834a7f873b0ae9a86262f7.pdf

Wang, Qiang; Li, Yuanfan; Li, Rongrong (2025). Integrating artificial intelligence in energy transition- A comprehensive review. Energy Strategy Reviews. Published by Elsevier Inc. https://doi.org/10.1016/j.esr.2024.101600

WEF, World Economic Forum (2025). WEF Global Risks Report 2025. 20th Edition, Insight Report Cologny/Geneva, Switzerland. [Em linha]. Consultado em 29Dec2024. Disponível em https://www.weforum.org/publications/global-risks-report-2025/

WMO, World Meteorological Organization (2021). Wake up to the looming water crisis, report warns. Press Release [Em linha]. Consultado em 29Dec2024. Disponível em https://wmo.int/news/media-centre/wake-looming-water-crisis-report-warns

Zhao, Le e Parhizgari, A.M. (2024). Climate change, technological innovation, and firm performance. International Review of Economics and Finance. Published by Elsevier Inc. https://doi.org/10.1016/j.iref.2024.04.025