Defesa vulnerável nas alterações climáticas



Em 1996, a crise climática era pouco falada e a inteligência artificial vista como uma tecnologia futura. Agora, juntas, são um perigo com que o sector da defesa está a lidar num país como os EUA cujo presidente não é adepto do tema das mudanças climáticas.

Como controlar o clima em 2025 foi um objectivo antecipado pela defesa norte-americana no estudo "*Weather as a Force Multiplier: Owning the Weather in 2025*".

Por PEDRO FONSECA

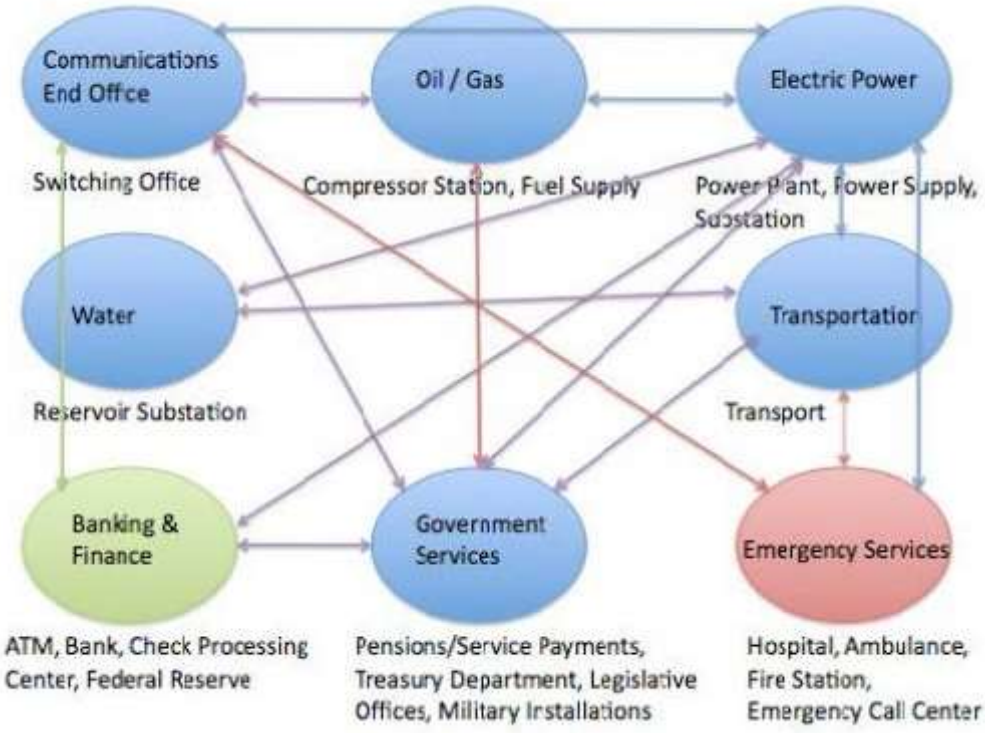
Datado de Junho de 1996, o trabalho pretendia antecipar cenários para as forças aero-espaciais "possuírem" o clima ao capitalizarem em tecnologias emergentes e focarem o desenvolvimento destas tecnologias em aplicações bélicas, escreve-se na introdução do documento.

Estas ferramentas de guerra - nomeadamente através de um sistema militar para uma alteração climática - podiam mudar os cenários de batalha de formas antes impossíveis. Entre outras, nas principais áreas encontravam-se a capacidade computacional, a transmissão e recolha de informação ou uma rede global de sensores.

Nas capacidades operacionais, referia-se a possibilidade de precipitação provocada para afectar os cabos físicos das comunicações, a supressão da água fresca ou outras atitudes para diminuir o conforto pessoal dos adversários.

O documento antecipava que "a modificação meteorológica deverá tornar-se parte da política de segurança nacional" nos EUA.

Antes desta administração ser eleita, a alteração climática era vista como "uma ameaça urgente e crescente à nossa segurança nacional", segundo um memorando do Department of Defense ao Congresso em 2015. A possível obstrução da capacidade militar em cumprir as suas missões foi um dos três eixos então apontados para essa ameaça.



30 anos depois, a situação alterou-se porque a administração daquele país pouco quer ouvir falar de clima. Em meados de Novembro, no jornal The Guardian, Michael Klare (autor de "*All Hell Breaking Loose: The Pentagon's Perspective on Climate Change*") escreveu como os "líderes militares não têm dito muito em público sobre o aquecimento global", derivado da relutância em se envolverem nas disputas partidárias e porque alguns responsáveis governamentais "desencorajaram activamente esse envolvimento".

Já este ano, o U.S. Army War College publicou o documento "*Implications of Climate Change for the U.S. Army*" que, apesar de estar disponível em vários sites civis, não se encontra em nenhum site oficial do Department of Defense, como descobriu a The Red (Team) Analysis Society.

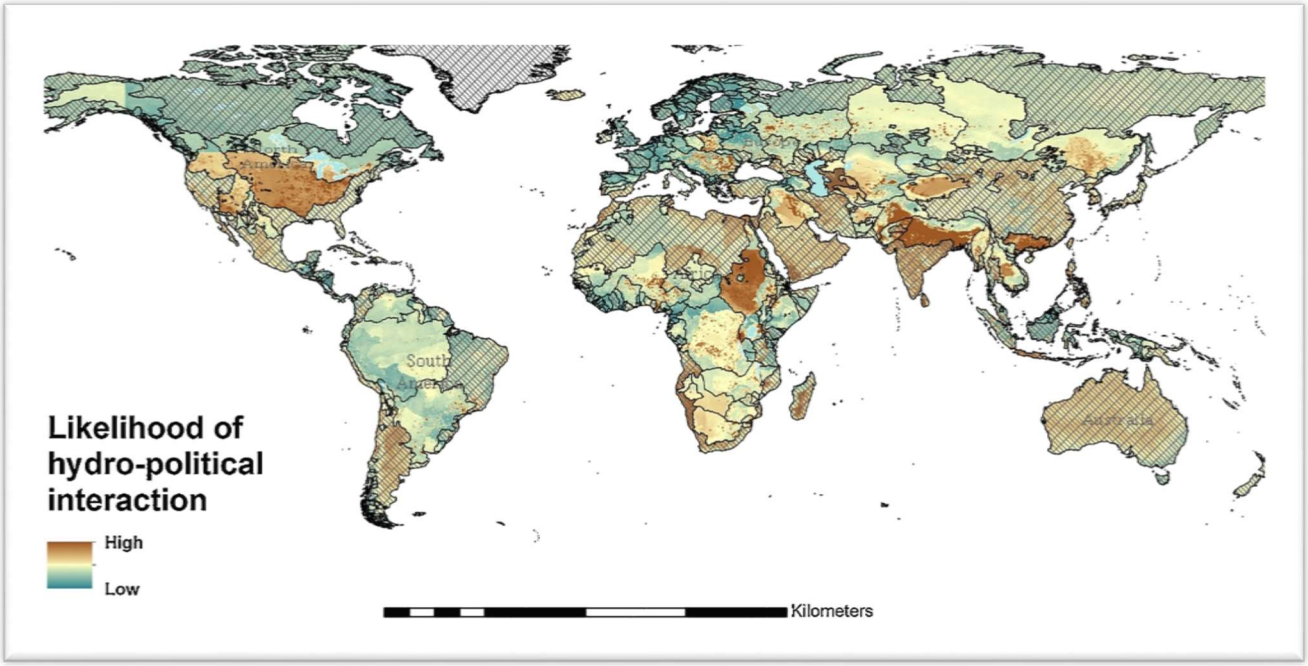
O estudo aponta um futuro entre 20 a 50 anos perigoso para a segurança nacional pelas consequências das alterações climáticas, como a emergência de doenças, escassez de água potável, fome e guerras.

No seu sumário executivo, o documento nota

como algumas alterações já ocorreram mas tendem a agravar-se nos próximos anos. O aumento do nível do mar, a insegurança no fornecimento de água e comida ou eventos meteorológicos mais extremos podem levar à migração das populações, a adoecer mais ou a uma instabilidade duradoura, principalmente em regiões com um fraco poder governamental - num conjunto de situações que tendem para o crescimento na procura da assistência humanitária militar.

Quanto ao total de 926 conflitos registados na Water Conflict Chronology, passou-se de 15 há uma década para 54 em 2015, 62 no ano seguinte, 87 em 2017, 73 no ano passado e três dezenas até 20 de Novembro.

Esta disputa pela água é um foco de tensão internacional e pode ocorrer quando a água é usada como arma (inundações provocadas, por exemplo), como "gatilho" em eventos que depois escalam para a violência ou quando são usados como alvos militares.



Conflitos ambientais estão a acontecer

Um outro estudo publicado em Outubro de 2018 por autores do Joint Research Centre (JRC) europeu revelou como as alterações climáticas vão acelerar as tensões relativamente a recursos escassos mas necessários para o ser humano, como a água. As denominadas "questões hidro-políticas" terão um impacto em cinco regiões vulneráveis, em redor dos rios Nilo, Ganges-Brahmaputra, Indus, Tigre-Eufrates e Colorado.

Assim, como refere o documento do U.S. Army War College, existe a necessidade de os militares anteciparem cenários para estes ambientes em constante mutação.

Uma das pricipais linhas de atenção da segurança nos EUA passa pela tecnologia, nomeadamente no forte investimento na inteligência artificial (IA). No início de Novembro, a National Security Commission for Artificial Intelligence dos EUA

divulgou um "*Interim report*" onde considera desafios urgentes da IA poder servir de ameaça por potências estrangeiras ou como pode ela melhorar as capacidade de defesa do país e da segurança nacional também do ponto de vista da competitividade económica.

Além da tecnologia, os efeitos geoestratégicos relacionados com o clima nem sempre são óbvios e a antecipação de cenários é essencial. De forma sintética, o elevado grau tecnológico de algumas nações pode colocá-las sob uma pressão analógica que já não sabem gerir.

Em Fevereiro passado, o European Union Institute for Security Studies (EUISS) publicou um documento de antecipação de cenários para 2021, sendo um deles a possibilidade de o Sol ser o ponto de partida para uma ciberguerra.

Na situação fictícia mas baseada num evento real ocorrido no Canadá em 1989, os efeitos geomagnéticos do Sol sobrecarregam as centrais de energia eléctrica. Essa forte tempestade solar provoca a libertação de partículas e afecta o campo magnético da Terra, dá início a uma falha no sistema de controlo ferroviário, gera um grave acidente e, com o difícil acesso às comunicações, é dificultada a gestão da crise humana e tecnológica.

A escala do evento leva um hipotético Cyber Defence Group a concluir tratar-se de um enorme "*Denial of Service Attack*" (DDoS) lançado pelo país vizinho, tendo retaliado de forma desproporcionada.

A situação é preocupante pelos contornos pouco futuristas que apresenta, principalmente numa situação semelhante pela falta de comunicações.

Como muitos equipamentos estão interligados, tudo pode sofrer um ataque de "hacking", adverte Laura Brandimarte no artigo "*What Would It Take to Shut Down the Entire Internet*?", publicado na revista Gizmodo no final de Outubro. A professora de gestão de sistemas de informação na University of Arizona nota como a infra-estrutura física dos cabos submarinos ou de fibra óptica usados para as comunicações podem ser alvo de ataque.

Embora no caso da Internet, por ser uma rede distribuída e redundante, esse efeito pernicioso possa ser atenuado, já o mesmo seria possível nas redes de gás ou de electricidade - com enormes danos humanos no Inverno, por exemplo -, ou na distribuição de água.

Impacto militar e guerra algorítmica

Todas estas redes de distribuição são interessantes para provocar perturbações e a necessidade de intervenção militar, a par de serem "atractivas" para o cibercrime, nota a consultora McKinsey em "*Critical infrastructure companies and the global cybersecurity threat*" (Abril de 2019).

Devido ao avultado investimento necessário, muitas organizações que as gerem estão "insuficientemente preparadas" mas elas estão sob crescente ameaça e são um dos factores a ter em conta nas tensões geopolíticas em que se lançam ataques a infra-estruturas críticas.

Tudo isto chamou a atenção de líderes políticos e militares. Em Abril passado, o EUISS voltou a antecipar cenários em "Global Trends To 2030 – Challenges and Choices for Europe", alertando sobre como um aumento de 1,5 graus na temperatura global pode gerar danos económicos e ambientais.

A situação pode ser agravada quando o ambiente geopolítico passa de um sistema unipolar para

"nós de influência", ocorre uma escassez de água e de comida, e quando a "inteligência da máquina começar a rivalizar com a humana".

É neste cenário que algumas chefias militares apostam: sistemas de sensores ou robôs capazes de tomarem decisões autónomas em terreno inimigo, usando a IA para a rápida análise de enormes bases de dados e até assumirem capacidades de decisão autónoma.

"Estamos a desenvolver uma camada de IA sobre como reunimos os sensores, a camada de computação e a analítica para gerir os dados", disse Doug Matty, director da Army AI Task Force Deputy Director, à revista The National Interest no início de Novembro.

A IA pode antecipar o comportamento inimigo ou as vulnerabilidades no fornecimento de bens, e também pode existir como sensor de reconhecimento de ameaças - uma tecnologia cujo protótipo deverá ser concluído em Janeiro próximo nos EUA.

São pequenos passos para uma guerra em mais larga escala que irá opor "algoritmo contra algoritmo", antecipa o director do Joint AI Center, Jack Shanahan. "Se tentarmos fazer isto com humanos contra máquinas, e o outro lado tem as máquinas e os algoritmos e nós não, corremos um risco inaceitavelmente alto de perder esse conflito".

Shanahan alerta para a necessidade de garantir que a IA não "ganha vida própria", derivado do seu cargo também envolver o "desenvolvimento de políticas apropriadas éticas, legais e outras", cujo resultado foi conhecido este mês no documento "*AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense*".

Mas nem só de conflitos vive a IA no sector da defesa. Em Abril passado, a ministra francesa das Armadas, Florence Parly, revelou a IA como "uma prioridade estratégica da defesa nacional" e apresentou o projecto "*BlueForce for soldiers*", que passa pelo desenvolvimento de um sistema de geolocalização para peões dentro de edifícios.

Trata-se de um desafio "crítico" localizar e socorrer pessoas sem necessidade de instalar sistemas complicados para essa detecção ou atrasar a intervenção médica, explicou o responsável do projecto.

A defesa norte-americana enfrentou uma situação semelhante num caso que não foi de simulação. Em Março passado, inundações severas do rio Missouri afectaram instalações militares - incluindo um comando estratégico da Força Aérea -, que levou à evacuação de pessoal, equipamento sensível ou munições. David Norton, responsável da base, declarou à Associated Press que "a rapidez com que [essas inundações] chegaram foi avassaladora".

Também a rapidez com que o mundo evoluiu, no âmbito climático e tecnológico, está patente nas declarações do senador Jay Rockefeller que, em Outubro de 2009, apontava como a questão da cibersegurança era algo "constantemente iminente" enquanto, a curto prazo, as alterações climáticas não o eram. Mas, "a longo prazo, se não resolvemos a alteração climática, então nada do resto fará diferença", transcrevia a publicação GovInfoSecurity.