A guerra na Ucrânia vai ser decidida pela inteligência artificial?

sabado.pt/mundo/detalhe/a-guerra-na-ucrania-vai-ser-decidida-pela-inteligencia-artificial

Diogo Alexandre Carapinha, subcoordenador do VisionWare Threat Intelligence Center, explica à SÁBADO como os ciberataques se alteraram desde o início da invasão russa e como são agora centrais para o conflito.

A invasão russa à Ucrânia começou há três anos, a 24 de fevereiro de 2022, mas não parece ter fim à vista. Enquanto no meio diplomático o primeiro mês de Donald Trump agitou as tradicionais alianças e iniciou conversações para "parar com as milhões de mortes" provocadas pela guerra, sem incluir a Ucrânia nem a UE, no terreno as posições parecem estar estagnadas.

No entanto, há muito que ficou provado que as guerras modernas não são travadas apenas no campo de batalha, mas também no espaço cibernético, onde os ataques podem ser menos visíveis, mas igualmente destruidores. Diogo Alexandre Carapinha, subcoordenador do VisionWare Threat Intelligence Center, considera que "a inteligência artificial utilizada para aperfeiçoar os ataques de ciberespionagem e melhorar os combates é o que vai decidir a guerra".

O especialista deste centro de análise de ameaças cibernéticas explica à **SÁBADO** que os russos "têm oscilado na sua estratégia". Se "no início assistíamos a ataques muito destrutivos, a empresas de setores chave, como telecomunicações ou centrais energéticas, acompanhadas de muitas fugas de informação e desinformação espalhada através das redes sociais, em 2024 a Rússia adotou uma estratégia mais *low key* evitando o ruído e focando-se nas operações de ciberespionagem em setores relacionados com a economia de guerra e política", segurança e defesa.

A inteligência artificial "já está a ser utilizada em ciberataques, por exemplo, para gerar mensagens de correio eletrónico de *phishing* em ucraniano ou para facilitar as interações entre *hackers* e vítimas através de aplicações de mensagens ou correio eletrónico".

Isto significa que "o ciberespaço tem por si só um conflito latente" e tem assumido o papel fundamental nos combates "sendo utilizado para conseguir informações que possam ser utilizadas na frente de combate" como "ter acesso à localização das tropas", refere Diogo Alexandre Carapinha.

Exemplo disso foi "a tentativa do grupo SANDWORM de perturbar as operações de cerca de vinte empresas de água e aquecimento comprometendo as suas cadeias de abastecimento, ao mesmo tempo que atacava infraestruturas essenciais na primavera de 2024". Desta forma, é claro que "os ataques cibernéticos podem ser utilizados para

potencializar os ataques físicos", no entanto, neste caso não foi obtido sucesso porque "medidas operacionais ucranianas conseguiram detectar as ameaças e o ataque falhou", refere Diogo Alexandre Carapinha.

Com a chegada dos soldados norte-coreanos à guerra na Ucrânia, "as autoridades ucranianas receavam que o apoio se espalhasse para o campo dos ataques cibernéticos". Porém, até agora não há indícios de que tenha acontecido: "Pelo menos não existem provas". Ainda assim, o subcoordenador do VisionWare Threat Intelligence Center refere que os *hackers* e as agências norte-coreanas "têm muito boas ciberqualificações, nomeadamente através do grupo LAZARUS, relacionado com o governo".

Apesar da inteligência russa e norte-coreana ser muito forte no que toca à ciberespionagem, Diogo Alexandre Carapinha ressalva que "os ucranianos têm uma grande capacidade de resposta a este nível, foram-se preparando ao longo dos anos tendo em conta a ameaça russa". Desde o início da invasão, Kiev "conta com muitos apoios ocidentais".

O poder das *deepfakes*

Diogo Alexandre Carapinha alerta que "a Rússia está cada vez a utilizar mais a inteligência artificial, sobretudo para criar *deep fakes* que tenham influência naquilo que é a política interna ucraniana".

Esta é uma questão especialmente importante tendo em conta que nos últimos dias, a tensão entre Zelensky e Donald Trump aumentou, chegando o líder norte-americano a considerar que Zelensky é um "ditador sem eleições", uma vez que, devido à lei marcial, as eleições na Ucrânia estão suspensas. Agora é esperado que as *deepfakes* se concentrem neste tema, com o objetivo de "tentar alterar a opinião pública e diminuir a credibilidade do governo de Zelensky".

Este é um campo onde tem existido especial desenvolvimento. Agora, "um bom *deepfake* é muito fácil de fazer e cada vez mais difícil de detectar", considera o especialista. É também por isso que "o Conselho Nacional de Segurança e Defesa da Ucrânia decidiu, em setembro, proibir a utilização do Telegram em dispositivos utilizados por agências governamentais, pelo sector da defesa e por funcionários de infraestruturas críticas".