Rússia está a treinar uma nova arma "ultrassecreta" para "uma possível imobilização da Europa"

cnnportugal.iol.pt/guerra/ucrania/russia-esta-a-treinar-uma-nova-arma-ultrassecreta-para-uma-possivel-imobilizacao-da-europa/20240427/6627a287d34e049892200d34

Em menos de um ano, mais de 40 mil voos registaram perturbações no sinal de GPS durante o voo, na região do Báltico, mas os especialistas acreditam o Kremlin que pode não ficar por aqui

Começou devagar, mas tem vindo a intensificar-se. Desde agosto de 2023, milhares de aeronaves civis têm registado diferentes tipos de interferências nos seus sinais de GPS quando operam na região em redor do exclave russo de Kaliningrado. Os especialistas consideram que a estratégia não é nova, mas a sua dimensão sem precedentes pode revelar que a Rússia está “a praticar” uma possível imobilização do continente europeu.

“Nos últimos meses, temos vindo a observar que cada vez mais aviões civis têm sido alvo de interferências eletrónicas, que anulam os seus sistemas de GPS e outros instrumentos de navegação vitais (serviços de posicionamento, navegação e cronometragem)”, afirma Bruno Castro, CEO da empresa de cibersegurança portuguesa VisionWare.

Entre agosto de 2023 e março de 2024, 46 mil voos registaram problemas de interferência em zonas como o Báltico, o Mar Negro e o Mediterrâneo Oriental. O "empastelamento" dos sinais eletrónicos não é novo no mundo da guerra eletrónica. No entanto, os especialistas mostram-se surpreendidos com a escala a que estes ataques estão a acontecer.

Segundo os serviços de informações britânicos, apenas a companhia aérea RyanAir teve 2.300 dos seus voos afetados e a Wizz-Air registou 1.300 ocorrências. Mas estão longe de ser as únicas. Estes ataques têm acontecido diariamente, numa área bastante vasta de território. Atualmente, o número de ataques ronda os 350 por semana.

Em alguns casos, os pilotos ficaram completamente "às escuras" com o sinal de GPS a desaparecer por inteiro. Embora em muitos casos os pilotos tenham recorrido a instrumentos de bordo para navegar o avião, a captura do sinal de GPS pode, em último caso, levar a erros bem mais graves, que podem interferir com a própria aterragem da aeronave.

"Estas interferências afetam os sistemas de comunicação wireless e podem induzir os pilotos a acreditar que o avião se encontra numa localização diferente daquela em que realmente está. No caso dos sistemas de GPS, é muito mais complicado, caso seja necessário aterrar", explica Bruno Castro.

Em janeiro, a Agência Europeia para a Segurança da Aviação alertou para um "aumento acentuado" dos ataques de interferência e falsificação, mas não apontou dedos. No entanto, com base nos locais onde estes aviões têm registado as interferências, os serviços secretos da Estónia de que uma arma eletrónica russa ultrassecreta, alegadamente sediada no exclave de Kaliningrado, tem estado por detrás dos ataques.

A própria Rússia admite que tem unidades militares de guerra eletrónica destacadas na região, embora não assuma a responsabilidade pelas mais recentes disrupções.

Em 2019, o Ministério da Defesa norueguês abordou a questão numa reunião bilateral com funcionários russos, todavia, o Kremlin continua a negar qualquer irregularidade. Em 2020, a Agência Sueca de Investigação em Defesa alertou para o facto de os sistemas de navegação russos conseguirem atacar sistemas de navegação vulneráveis. Os avisos foram aparentemente ignorados.

De acordo com o comandante das forças de Defesa da Estónia, o general Martin Herem, estas armas não afetam apenas os sistemas de GPS da aviação comercial. Estes ataques estão a afetar também os sistemas de GPS dos telemóveis e de sistemas militares. "Eles [os russos] são muito fortes nisto", sublinhou o general em entrevista ao Kyiv Independent.

Uma prova disso mesmo foi um ataque feito a um avião militar inglês, a 13 de março, que transportava o secretário da Defesa britânico Grant Schapps. O sinal do avião foi alvo de uma interferência que durou mais de 30 minutos, quando o avião do ministro regressava da Polónia para o Reino Unido. Downing Street confirmou que o sistema de

GPS do avião foi alvo de um “empastelamento” quando se aproximou de Kaliningrado, mas tentou desvalorizar a ameaça, garantindo que a segurança da aeronave não esteve em causa. No entanto, os especialistas garantem que pode não ser bem assim.

“De recordar que este ataque, realizado a 13 de março deste ano, interferiu com o sistema primário de GPS do avião e com as comunicações via Internet, que se perderam durante meia hora, e também com o sistema de medidas contra um ataque de mísseis. Estamos, como podem perceber, a assistir a algo muito problemático”, recorda Diogo Carapina, subcoordenador do VisionWare Threat Intelligence Center, um centro de monitorização de ameaças cibernéticas.

Mas há muito que a Rússia tem demonstrado uma forte capacidade no campo da guerra eletrónica. No campo de batalha na Ucrânia, a Rússia tem feito sentir o poder destes mecanismos. Relatos de vários comandantes no campo de batalha demonstram que as forças armadas russas possuem capacidade bastante disruptivas, capazes de “cegar” as tropas ucranianas e travar as suas comunicações.

Moscovo nunca teve problemas de demonstrar abertamente as suas sofisticadas capacidades de guerra eletrónica. Em 2015, as forças russas apanharam os próprios Estados Unidos de surpresa com o empastelamento de drones e sistemas de comunicações na Síria. Na mesma altura, Moscovo já utilizava com grande eficácia estas armas na Ucrânia. O general norte-americano, então comandante das forças americanas na Europa, descrevia as capacidades russas como capazes de “levar lágrimas aos olhos”.

“Esta estratégia não é nova e há relatos de manobras semelhantes - o mesmo género de ataques eletrónicos - que têm sido também alegadamente utilizadas no Donbass, no leste da Ucrânia, desde 2015”, recorda Bruno Castro.

Mas o cenário agora é diferente e a Rússia demonstra estar disposta a utilizar esta arma fora dos territórios onde as suas forças armadas estão a combater. Para o especialista do RUSI Jack Watling, apesar de a Rússia utilizar há muito “a interferência do GPS como instrumento de perseguição", agora "está a projetá-la para além das fronteiras da NATO".

Um dos especialistas da Chatham House, Keir Giles, afirma que, caso a Rússia consiga afetar os serviços de GPS não só de aviões, mas também dos transportes terrestres, o caos estaria instalado e a Europa ficaria imobilizada.

Os ataques dos últimos meses podem ser vistos, por um lado, como a Rússia a praticar uma possível imobilização da Europa e, por outro lado, como uma demonstração do seu poder cibernético.

“Os ataques destes últimos meses podem ser vistos, por um lado, como a Rússia a praticar uma possível imobilização da Europa (e “cegueira” do seu espaço aéreo) e, por outro lado, como uma demonstração do seu poder eletrónico – com forte pendor cibernético”, garante Diogo Carapinha.