Três anos de guerra na Ucrânia e a ameaça silenciosa à cibersegurança

itsecurity.pt/news/analysis/tres-anos-de-guerra-na-ucrania-e-a-ameaca-silenciosa-a-ciberseguranca

As armas são agora computadores, as balas transformam-se em linhas de código e os campos minados dão lugar a redes ocultas. No lado obscuro do digital, a guerra deixa de ser travada apenas no campo de batalha e expande-se para o ciberespaço. Esta segunda-feira, 24 de fevereiro de 2025, assinalam-se três anos desde o início da guerra na Ucrânia – um conflito que ultrapassa as fronteiras físicas e ganha novas dimensões no domínio digital.

Nos últimos três anos, a cibersegurança deixou de ser apenas uma preocupação técnica para se tornar um pilar estratégico na defesa de Estados e empresas. O conflito na Ucrânia acelerou essa transformação ao demonstrar que ataques informáticos podem ser tão disruptivos quanto confrontos no terreno. Infraestruturas críticas, sistemas governamentais e cadeias de abastecimento tornaram-se alvos preferenciais, enquanto a ciberguerra evolui com o uso crescente de inteligência artificial, deepfakes e novas formas de engenharia social. Assim, torna-se essencial analisar as mudanças que marcaram este período e antecipar os desafios que vão definir o futuro da cibersegurança e da geopolítica digital.

Ciberguerra: um novo paradigma nos conflitos modernos

Nos últimos três anos, assistiu-se a um aumento expressivo de ciberataques direcionados a infraestruturas críticas, como redes elétricas, sistemas de telecomunicações e instituições governamentais, o que para Bruno Castro, Fundador e CEO da VisionWare, *"foi o primeiro grande alerta - proteger as infraestruturas vitais da sociedade contra ciberataques destrutivos"*. Um dos exemplos mais notáveis foi a atuação do grupo pró-Rússia NoName057(16), que, desde março de 2022, tem realizado ataques DDoS contra organizações na Ucrânia e em países da NATO. Em 2024, verificou-se ainda uma mudança tática dos cibercriminosos russos, que passaram a focar-se na inteligência digital, operando de forma silenciosa para permanecer indetetáveis pelo maior tempo possível. *"Este foi outro grande alerta para todos os Estados"*, diz, *"isto é, os ataques silenciosos, a ciberespionagem e as campanhas de desinformação"*.

Os tipos de ciberataques também evoluíram significativamente, segundo o especialista, *"os ataques wipers tornaram-se uma das principais armas de guerra no ciberespaço, sendo bastante utilizados para destruir dados e comprometer redes inteiras"*. Paralelamente, ataques DDoS massivos ganharam escala e complexidade e visam *"perturbar e sobrecarregar websites de órgãos governamentais e instituições financeiras"*. Bruno Castro destaca ainda o aumento dos ciberataques direcionados a infraestruturas críticas e cadeias de abastecimento, cujo objetivo é causar disrupção em toda a sociedade.

A guerra influenciou o ecossistema do cibercrime, estreitando a relação entre grupos de ransomware e interesses estatais. De acordo com o CEO da VisionWare, *"o grupo Conti, por exemplo, declarou apoio à Rússia, enquanto outros grupos adotaram uma postura mais nacionalista, direcionando ciberataques para alvos considerados hostis*

ao seu país de origem". Simultaneamente, campanhas de desinformação tornaram-se mais sofisticadas, utilizando redes sociais, bots e deepfakes para disseminar narrativas falsas e influenciar a perceção pública do conflito.

Engenharia social, deepfakes e inteligência artificial nos ciberataques

A engenharia social e a Inteligência Artificial (IA) têm desempenhado um papel crucial nestes ataques, e a sua combinação tem tornado as ameaças mais sofisticadas e difíceis de detetar. Se antes a engenharia social se focava essencialmente na extorsão financeira, atualmente é usada de forma estratégica para comprometer redes e aceder a dados críticos. Como explica Bruno Castro, *"neste contexto, muitos grupos criminosos utilizaram essas técnicas para fins de disrupção, direcionados a alvos específicos como membros do governo e militares, de forma a roubar credenciais e assim obter acesso a redes e dados críticos"*.

A inteligência artificial tem também impulsionado campanhas de phishing altamente personalizadas, tornando-as mais convincentes e difíceis de detetar. Segundo o especialista, os *"modelos generativos estão a ser utilizados insistentemente para criar e-mails, mensagens e até vozes falsas em ataques de engenharia social"*. Além disso, chatbots maliciosos são usados para manipular debates online e amplificar a desinformação, levando a um risco crescente. *"O maior risco desta tendência"*, alerta Bruno Castro, *"é sobretudo a escalada da eficácia dos ataques, tornando cada vez mais difícil, ou mesmo quase missão impossível, conseguir efetivamente distinguir o que é real do que é digitalmente manipulado"*.

Deepfakes têm sido usados para criar vídeos falsos de líderes políticos, distorcendo declarações e manipulando a opinião pública. De acordo com Bruno Castro, *"campanhas de desinformação, amplificadas por bots e deepfakes, espalham narrativas fabricadas para semear desconfiança, evangelizar falsas doutrinas e políticas, acabando por dividir populações"*. Estas campanhas são frequentemente coordenadas com outras formas de poder, permitindo moldar atitudes e comportamentos em larga escala. *"O objetivo"*, acrescenta, *"será o de obter vantagens sobre o adversário e manipular a opinião pública, numa escala anteriormente inimaginável"*.

A resposta dos serviços de inteligência

Face a esta realidade, os serviços de inteligência dos Estados têm vindo a adaptar-se através de investimentos *"na monitorização de ciberameaças em tempo real"*, além disso, recorrem também a IA para *"monitorizar grupos criminosos, identificar padrões suspeitos e, assim, tentar antecipar riscos de ciberataques"*.

Paralelamente, a cooperação entre agências internacionais tem registado avanços significativos, *"resultando em partilhas mais céleres de informações sobre ataques e grupos criminosos"*. Além disso, algumas nações têm apostado no recrutamento e formação de equipas especializadas em operações de ciberguerra, tanto ofensivas como defensivas, o que fortalece a capacidade de resposta a ameaças globais.

O futuro dos ciberataques e a nova corrida às armas

No futuro, os ciberataques continuarão a ser uma extensão dos conflitos tradicionais, combinando operações físicas e digitais para maximizar o impacto. A proliferação de IA nestes ataques também deverá acelerar, tornando as defesas tradicionais menos eficazes. Além disso, a tecnologia já é amplamente utilizada em autonomous lethal weapons, robótica e sistemas de reconhecimento de alvos. No caso da Rússia, por exemplo, *"é notório o desenvolvimento de drones militares autónomos"*.

O avanço de ciberarmas sofisticadas pode intensificar as tensões diplomáticas e desencadear uma corrida armamentista digital, enquanto a ciberespionagem afirma-se como uma ameaça silenciosa e cada vez mais presente. O especialista garante que *"esta é uma tendência em ascensão – uma ameaça silenciosa que muitos atores utilizam para obter vantagens, de forma menos visível, mas igualmente, disruptiva"*.

Para enfrentar este novo paradigma, as empresas e instituições devem adotar uma abordagem proativa, reforçando a cibersegurança em todas as áreas. *"As organizações devem adotar estratégias de defesa mais proativas, incluindo treino intensivo em cibersegurança para colaboradores, implementar um Security Operations Center, algo que constitui sempre uma grande mais-valia, investir no uso de inteligência artificial para detetar comportamentos anómalos, e, claro, investir ainda em serviços de Strategic Intelligence para uma tomada de decisão estratégica, antecipada, consciente e bem informada"*, sublinha o CEO e Fundador da VisionWare. Além disso, a cooperação entre o setor público e privado será determinante para fortalecer a ciber-resiliência global e mitigar as ameaças emergentes.