A face da batalha que não se vê, mas que se sente

visao.pt/opiniao/2025-02-20-a-face-da-batalha-que-nao-se-ve-mas-que-se-sente

Diogo Alexandre Carapinha 20 de fevereiro de 2025

Os ciberataques deixaram de ser uma questão meramente tecnológica e passaram a impactar diretamente eleições, economias e a própria estrutura das sociedades, sobretudo das que se encontram a lutar pela sua existência

Os números não mentem: em 2024, foram identificadas mais de 40 mil vulnerabilidades de segurança a nível global. Cada uma delas representa uma porta aberta para ciberataques. Mas não se trata apenas de estatísticas; são alertas de que os agentes maliciosos dispõem de mais oportunidades do que nunca.

Os acontecimentos de 2024 demonstraram a gravidade do problema. Nos Estados Unidos, hackers infiltraram empresas de telecomunicações. Na Roménia, a primeira volta das eleições presidenciais teve de ser anulada devido a uma interferência cibernética. Na Ucrânia, todos os dias acontecem novos incidentes. Os ciberataques deixaram de ser uma questão meramente tecnológica e passaram a impactar diretamente eleições, economias e a própria estrutura das sociedades, sobretudo das que se encontram a lutar pela sua existência.

A invasão russa à Ucrânia, iniciada há três anos, não se tem desenrolado apenas no campo de batalha tradicional, como o leitor saberá. Desde os primeiros momentos do conflito, que remontam à invasão da Crimeia, o ciberespaço revelou-se um domínio fundamental para ambas as partes, com ataques informáticos a infraestruturas críticas, campanhas de desinformação e a mobilização de atores estatais e não estatais.

A preponderância do ciberespaço na guerra foi evidente antes mesmo da invasão terrestre, no dia 21. Nos meses que a antecederam, a Ucrânia foi alvo de uma série de ciberataques coordenados, muitos dos quais atribuídos a grupos ligados ao Kremlin. Estes ataques visavam desestabilizar o país, comprometendo redes governamentais, bancos e serviços essenciais. Recordemo-nos, por exemplo, do uso do malware WhisperGate, projetado para destruir dados e inviabilizar sistemas ucranianos.

Durante a invasão, o ciberespaço tornou-se um campo de batalha paralelo. A infraestruturas energéticas, transportes e comunicações foram alvos de ciberataques, numa tentativa de minar a resiliência do país. No entanto, a Ucrânia conseguiu resistir graças a um reforço significativo das suas capacidades digitais, apoiada por aliados ocidentais e empresas tecnológicas privadas. A migração de dados críticos para servidores no estrangeiro foi uma das estratégias mais bem empregues para proteger informações sensíveis.

Os ataques contra os setores de segurança e defesa aumentaram significativamente. O grupo APT44, ligado aos serviços de inteligência militar russos, tem-se especializado na espionagem digital, explorando dispositivos capturados de soldados ucranianos para

extrair informações valiosas sobre movimentações militares e cadeias logísticas.

A utilização de malware através de aplicações de comunicação também se intensificou, comprometendo tanto militares como civis. Por isso, o governo ucraniano proibiu o uso do Telegram em dispositivos oficiais, temendo que a plataforma servisse como canal de espionagem. No entanto, apesar das restrições, o Telegram continua a ser amplamente utilizado no país.

Novos recursos, sofisticação das ameaças

A inteligência artificial tem sido utilizada para sofisticar ataques cibernéticos, como a geração de e-mails de phishing mais convincentes ou interações mais realistas entre hackers e vítimas. Em 2024, assistimos a uma mudança tática dos hackers russos: em vez de ataques destrutivos altamente divulgados, passaram a focar-se na inteligência cibernética, operando silenciosamente para permanecer indetectáveis pelo maior tempo possível.

O grupo APT44 foi responsável por um ataque massivo em dezembro de 2024, que comprometeu cerca de 60 bases de dados nacionais da Ucrânia. O incidente interrompeu serviços essenciais, incluindo o registo de nascimentos, casamentos, transações imobiliárias e outros processos legais. Embora algumas funções tenham sido restauradas rapidamente, a dependência digital da sociedade moderna foi exposta como um ponto frágil.

Para além dos ataques diretos, o ciberespaço tem sido palco de uma intensa guerra de informação. A Rússia usa as redes sociais e meios de comunicação controlados pelo Estado para disseminar narrativas que justificassem a invasão e minem o apoio interno e internacional ao governo de Kiev. Em contrapartida, a Ucrânia tem utilizado estratégias digitais para expor as atrocidades cometidas pelos invasores, mobilizar apoio global e manter a moral da sua população e das suas tropas.

Outro elemento inédito foi a participação de grupos de hackers independentes. O coletivo Anonymous declarou “guerra” contra a Rússia, conduzindo ataques DDoS a websites governamentais e revelando informações sensíveis. Grupos ligados ao governo russo, como o Killnet, respondem com ataques contra alvos ocidentais em retaliação às sanções impostas contra Moscovo.

Os próximos tempos

É certo que 2024 diz-nos que o número de incidentes críticos e de grande impacto diminuiu, mas o número total de incidentes e ataques contra instituições governamentais e autoridades locais aumentou.

Os ciberataques contra os setores da segurança e da defesa aumentaram em relação ao ano anterior e a Rússia intensificou os esforços para recolher informações através dos dispositivos dos militares ucranianos, como foi mencionado ao longo deste texto. Estas atividades não vão parar.

Uma tendência notável que comprova a utilização cada vez mais sistemática de ciberataques para apoiar objetivos militares.

A cibercriminalidade com fins lucrativos, os grupos ligados ao Estado que visam as infraestruturas críticas e as atividades encobertas dos serviços secretos, essas prosseguirão sem interrupção.

A guerra na Ucrânia demonstra-nos exatamente que o ciberespaço não é apenas um complemento das operações militares convencionais, mas um domínio essencial dos conflitos modernos. O equilíbrio de poder nos próximos conflitos será cada vez mais determinado pela capacidade dos Estados de defenderem as suas infraestruturas digitais e de utilizarem a informação como uma arma estratégica.

Ao assinar está a ajudar no combate pela verdade e pela construção de uma sociedade aberta e informada.