Rússia vs Ucrânia: guerra que não se vê, mas sente-se

dinheirovivo.pt/opiniao/russia-vs-ucrania-guerra-que-nao-se-ve-mas-sente-se-16329887.html

10 de maio de 2023

Aquando da invasão russa à Ucrânia, as duas nações entraram em guerra aberta. É certo que há muito que Ucrânia e Rússia não tinham uma relação estável - a escalada de tensões entre os dois países começou em 2014, com a anexação russa da Crimeia - e, segundo vários especialistas, este era um fim expectável. Contudo, este conflito estende-se muito além do campo de batalha tradicional, com a utilização da cibersegurança e da ciber inteligência como "novas" armas.

Esta outra guerra, com atores não tão visíveis, ganhou um novo fôlego. E é importante referirmos que "ganhou um novo fôlego", porque não se trata de um começo. A verdade é que, desde então, as duas nações têm usado a ciberguerra como uma ferramenta para tentar obter vantagem estratégica sobre a outra. Por detrás deste conflito "underground", estão militares, mas também ativistas não oficiais, que em prol de uma bandeira, desenvolveu ataques cibernéticos com fins destrutivos, seja isso desativar (mesmo que temporariamente) *websites* de Instituições do Estado, interromper serviços críticos na Banca ou Telcos, ou até, desfigurar mensagens do inimigo.

Falamos de organizações "hacktivistas", algumas já profissionalizadas - veja-se o caso dos Killnet, agora conhecidos como os Wagner do mundo *cyber*. No entanto, tal como é possível ver no conflito bélico, também a nível cibernético esta guerra é desigual. Os russos detêm mais recursos humanos, meios e poder disruptivo - até à data - que os ucranianos. Por isso, e para além do apoio dos serviços de inteligência da NATO (muitos deles suportados em questões cibernéticas, a Ucrânia está a defender-se dos ciberataques com a ajuda de equipas militares ocidentais e de empresas privadas de cibersegurança, financiadas por doações de milhões de dólares. Ofensivamente, e de forma mais ou menos pública, os ucranianos são representados nesta batalha, na sua larga maioria, pela rede voluntária de *hackers* "IT Army of Ukraine".

Não sejamos inocentes: trata-se de uma guerra, portanto, tanto a Rússia e a Ucrânia têm desenvolvido suas capacidades de ciberguerra, criando habilidades para invadir e sabotar redes e sistemas informáticos. A Rússia tem sido acusada de ataques de *ransomware*, de espionagem de alvos estrangeiros e de interferência em redes de computadores governamentais e civis, usando suas redes de computadores para lançar ataques DDoS, na sua maioria a setores críticos da sociedade. Falo-vos de ataques perturbadores - embora temporários - a *websites* de hospitais, tanto na Ucrânia como nos países aliados.

Isto levanta-nos, uma vez mais, a velha questão sobre a falta de uma convenção internacional para a guerra cibernética: uma espécie de extensão da Convenção de Genebra. E também nos coloca uma outra máxima: o facto de os ataques estarem a ser levados a cabo em países da NATO, não poderia desencadear numa contraofensiva

coletiva dos países ocidentais? Estaríamos a considerar um ato de guerra contra países da NATO? Este é o prisma do mundo cibernético e do "hacktivismo". Não conseguimos provar a ligação de um grupo a um Estado... Por outro lado, e na vertente de espionagem de uma guerra também ela cibernética, será que não podemos considerar as ações de angariação de informação da estratégia militar da Rússia, desenvolvida por países da NATO, também poder ser considerado um ato de guerra?

Voltando ao tema em análise, desde o início da invasão em grande escala, a Ucrânia tem-se esforçado por se apresentar como defensora e não como atacante. Ainda assim, e de acordo com relatos, a Ucrânia tem igualmente recorrido a táticas cibernéticas destinadas a desestabilizar a Rússia, incluindo DDoS e fugas de informações confidenciais, nomeadamente, de elementos ligados ao Kremlin e aos serviços secretos.

As disputas entre os dois países também se estendem aos campos da propaganda e da influência digital, utilizando os seus recursos para criar conteúdo com o objetivo de influenciar as opiniões da população e de desenvolver campanhas de desinformação. Mais uma vez, também neste âmbito as forças têm peso desiguais. O objetivo é muito simples: provocar o maior caos possível.

Tal como qualquer guerra, também a guerra cibernética entre estes dois Estados tem tido um impacto significativo nas operações de ambos países. Estes têm causado danos significativos a empresas, governos e indivíduos, resultando em perdas financeiras e partilha de dados confidenciais. Tem custado milhões de dólares às economias dos dois países, e segundo os especialistas, o custo monetário dos ataques cibernéticos tem sido considerável, mas ainda é muito reduzido quando comparado com custo social e político. Além disso, também a reputação internacional tem sido prejudicada, causando preocupação entre os países vizinhos e parceiros comerciais.

Há quem preveja um aumento da gravidade dos ataques por parte da Rússia, à medida que esta se avança no campo físico da batalha. Há quem refira inclusive que os russos estão a coordenar ataques cibernéticos em paralelo com ataques físicos a alvos como as redes de energia. Outros ainda referem que os ucranianos irão impulsionar os seus meios cibernéticos para provocar danos bastante mais disruptivos nos russos, havendo uma combinação de esforços bélicos e cibernéticos na prevista contraofensiva.

Como em todos os aspetos de uma guerra, o nevoeiro é permanente e inconclusivo. E tudo isso ainda se torna mais verdade, no campo do ciberespaço.

Fundador e CEO da VisionWare