Ciberguerra: A ascensão da nova frente de batalha do século XXI

SOL sol.sapo.pt/2023/10/26/ciberguerra-a-ascensao-da-nova-frente-de-batalha-do-seculo-xxi

26 de outubro de 2023

A frente cibernética é hoje determinante para o desenrolar, e até para o próprio desfecho, dos conflitos, aparecendo para complementar as manobras militares no terreno.

Os Estados investem cada vez mais em unidades que operam no ciberespaço. No entanto, mesmo as superpotências podem apresentar algumas vulnerabilidades face a ciberataques, porque uma vez tendo o processo de virtualização e digitalização de informação mais consolidado, são criadas fragilidades. Os estudos levados a cabo pelo VisionWare Threat Intelligence Centre (VWTIC), centro de estudos de *Intelligence* da empresa de cibersegurança portuguesa, são uma valiosa ferramenta para a análise destas problemáticas.

O Nascer do SOL conversou com Bruno Castro, CEO do VisionWare, e com Diogo Carapinha, consultor e subcoordenador do VWTIC, de modo a obter informações mais profundas sobre a atividade cibernética e os seus impactos na ordem internacional.

Bruno Castro explica a importância deste trabalho. **«No VisionWare Threat Intelligence Centre ressalvamos a importância da vigilância, recolha e análise atenta destes fenómenos no ciberespaço para permitir a consciencialização, estudo e prevenção dos efeitos nefastos que a ciberguerra acarreta. A ciberguerra tem efeitos que duram por muito tempo, ao contrário dos conflitos convencionais.»**. Quanto à questão do Direito, o CEO sublinha a dificuldade de enquadramento dos atores: **«Havendo uma clara dificuldade em classificar legalmente estes atores, a criação de um quadro legal torna-se uma tarefa complexa. A solução que se apresenta é a promoção de um esforço cooperativo entre os Estados, e até mesmo entre o setor privado e público.»**.

A ciberguerra e a geopolítica

Diogo Carapinha, formado em Relações Internacionais, abordou os impactos geopolíticos causados por ataques desta natureza: **«A ciberguerra é uma área em constante mudança que influencia a geopolítica, a segurança nacional e as relações internacionais. Trata-se de uma guerra diferente, uma que permite que nações e grupos de indivíduos isolados lutem sem armas.»**.

O conflito israelo-palestiniano é um exemplo disto, e o subdiretor do VWTI faz referência à influência de agentes não estatais: **«Para além dos intervenientes patrocinados pelo Estado – que já intensificam os seus esforços cibernéticos nos bastidores – existem também grupos de *hacktivistas* patriotas que apoiam um dos lados do conflito e que**

têm vindo a intensificar os seus ciberataques. Torna-se bastante claro que os *hacktivistas* estão a trabalhar para fazer do conflito Israel-Hamas a próxima frente de guerra cibernética.». No que à complementaridade deste tipo de guerra com a convencional diz respeito, Diogo Carapinha conclui que **«este é o novo campo de batalha, onde grupos de *hackers* de várias nações lutam, medindo forças com os Estados.»**.

Mas estes atores não atuam num vazio, estabelecendo relações, ainda que não formais, com os Estados e organizações do sistema internacional: **«embora não existam laços diretos entre estes grupos e os governos – ou, pelo menos, provas concretas dessa ligação – os grupos *hacktivistas* tendem a conduzir ataques informáticos que beneficiam os países que lhes dão abrigo.»**. Diogo Carapinha dá um exemplo: **«Grupos de piratas informáticos com ligações a países como o Irão e a Rússia, lançaram uma série de ciberataques e campanhas online contra Israel, alguns dos quais poderão ter ocorrido durante o período que antecedeu o ataque do Hamas a sete de outubro. De momento não há material que permita confirmar que existe uma coordenação entre os ataques no terreno com os do ciberespaço (…) [mas] uma certeza que temos é que as campanhas online reforçam os ataques físicos com uma ofensiva digital potencialmente replicando a forma como a Rússia e *hacktivistas* simpatizantes atacaram a Ucrânia informaticamente nos primeiros dias da guerra.»**.

Segundo os estudos deste centro do VisionWare, disponibilizados ao Nascer do SOL, compreende-se que existem semelhanças entre os dois grandes conflitos em curso, que pautam a agenda mediática: houve um aumento de ciberataques e campanhas de desinformação observado quase imediatamente após o ataque do Hamas e a subsequente resposta de Israel, como também aconteceu após a invasão da Rússia à Ucrânia; a maioria dos ataques são ataques distribuídos de negação de serviço (DDOS) e desfiguração de *websites*, mas também roubo de dados confidenciais para a sua distribuição gratuita, tentando causar disrupção política, securitária e social; além dos ataques aos países que estão diretamente envolvidos nos conflitos, os relatórios demonstram que outros Estados – nomeadamente países ocidentais que apoiam tanto Israel como a Ucrânia – têm sido um alvo preferencial para os atacantes.

A guerra da desinformação

Os conflitos atuais também se desenrolam na frente da comunicação e redes sociais, onde se tenta – e muitas vezes consegue – disseminar a propaganda ideológica através da descontextualização e informação seletiva. De acordo com os relatórios disponibilizados pelo VWTIC, tem havido uma rápida e extensa disseminação de desinformação através das redes sociais, nomeadamente através da criação de contas falsas no *X* (antigo Twitter). **«A desinformação tem sido espalhada propositadamente por indivíduos e grupos que procuram reforçar uma determinada narrativa (…) as redes sociais têm sido utilizadas para espalhar o medo e transmitir atos de guerra. Para termos uma ilustração real,**

uma cidadã israelita descobriu que um familiar tinha sido morto por um militante do Hamas depois de uma transmissão em direto no Facebook.», afirma Diogo Carapinha, subcoordenador deste centro de estudos.

O CEO do VisionWare confirma, constatando que **«Este conflito [Israel-Hamas] é, também, uma guerra de desinformação. (…) com a Inteligência Artificial é possível manipular imagens e áudios: criar todo este conteúdo rapidamente e de forma acessível permite a sua disseminação e viralização antes que se consiga apurar a sua veracidade. A desinformação, ao tornar-se viral nas redes e nos média, estimula opiniões que promovem a guerra, sendo inquestionável que esta tem sido uma dimensão vastamente explorada no conflito. Ambos os lados estão a utilizar esta tática (…) e sem dúvida é uma arma poderosa.»**.

A rede *X* já recebeu uma advertência por parte da Comissão Europeia, sendo acusada de difundir **«conteúdos ilegais e desinformação»**, violando a Lei dos Serviços Digitais da União Europeia

Capacidade e impacto dos ataques

«É importante ressalvar que estes ataques têm uma capacidade dupla», avança Bruno Castro, que acrescenta ainda que «Num sentido mais direto, causam um impacto imediato, provocando instantaneamente o caos e a disrupção. Por outro lado, indiretamente, acabam por funcionar como manobras de ilusionismo, não só chamando atenção para os próprios grupos *hacktivistas* – servindo-lhes de publicidade – mas também criando falhas de segurança noutros domínios. São inúmeros os danos colaterais que os ciberataques podem causar. (…) Uma operação cibernética (…) pode inadvertidamente afetar hospitais ou outras infraestruturas críticas, causando danos a indivíduos inocentes.». Quanto ao controlo, o diretor executivo da empresa reconheceu a dificuldade, assumindo que **«o verdadeiro impacto de um ataque é difícil de controlar devido à complexidade do mundo digital. Os impactos financeiros desta guerra [Israel-Hamas] são evidentes, mas – mais do que isso – já existem exemplos de que ciberataques podem criar disrupção numa dimensão física e em infraestruturas vitais para os Estados soberanos. O *malware Stuxnet*, por exemplo, irá ficar para a história como um episódio marcante de danos físicos que os ciberataques podem causar.»**.

Tal como na vertente cinética da guerra, também ao nível cibernético os grupos não estatais têm ganho preponderância. Segundo Bruno Castro, **«é preocupante existirem já organizações não estatais – com ou sem apoio de nações soberanas – com capacidades para medir forças com os Estados.»**.

No contexto geopolítico atual, que se caracteriza pela sua volatilidade, as ações no ciberespaço podem revelar-se um fator capital para desenhar os contornos dos conflitos e da ordem internacional *per se*, e não podem, de maneira alguma, ser desvalorizadas.