Editorial - Novo Ano, Novos Desafios: Ciberataques e Ciberdefesas

General
Gabriel Augusto do Espírito Santo

Novo Ano, Novos Desafios: Ciberataques e Ciberdefesas

Alguns teorizadores das mudanças na guerra têm vindo a desenvolver, a ritmo crescente e com cenários diversificados, as suas preocupações com novas formas de ataques que se concretizam sobre os *outros*, na linguagem da estratégia, agora sem violência nem sangue, que enquadram numa terminologia e em procedimentos que identificam como *ciberguerra*. Ataques que são baratos, muito rápidos, desencadeados anonimamente, que podem atingir alvos críticos em momentos de crise, que já se identificam como *ciberataques* e que tornam o ataque electrónico como uma das formas mais sofisticadas do combate irregular. O denominado *ciberespaço*, onde circulam as ondas electromagnéticas que dão vida à era da informação, tornou-se espaço privilegiado para o confronto de vontades.

Ainda sem uma definição precisa para o que se deve designar por *ciberguerra (*a actividade da guerra propriamente dita, na linguagem do seu teorizador que foi Clausewitz, é o recontro e o recontro pressupõe combate), os *ciberataques* têm sido identificados mais pelos seus alvos e as suas consequências do que pela precisão do conceito. Os alvos mais identificados até agora têm sido sistemas informáticos e as vias (redes) que transportam informação, alterando os caminhos previstos para a sua circulação ou o seu conteúdo e recorrendo a intrusões e alterações nos programas de *software* que os apoiam. Dos dados conhecidos são mencionados com frequência os ataques aos sistemas informáticos da Geórgia e da Estónia (2007), atribuídos à Rússia, a explosão de um gasoduto na Sibéria atribuído a uma interferência da CIA dos EUA (1982) e, recentemente (2009), a interferência no sistema de banda larga do vulgarizado *twitter,* com propaganda contra os EUA originada no Irão. Mostram-se como sistemas preferenciais desses ataques, até agora, os sistemas automáticos de transmissão de dados e fornecedores ou reguladores de serviços (energia, água, tráfego aéreo, comunicações, informação *on-line*) e referenciam-se como muito vulneráveis as transmissões temporárias ponto a ponto para a transmissão de dados (na linguagem das

telecomunicações *peer-to-peer*, já traduzidas na sigla P2P) como aquelas que estão a ser utilizadas para pilotar e comandar veículos aéreos não tripulados (UAV) à distância, como acontece nos meios utilizados em locais distantes como o Iraque ou Afeganistão e comandados dos EUA.

Outra categoria de ataques deste tipo, e menos divulgada, é a que resulta da utilização de *hardware* adulterado, nomeadamente circuitos que utilizam milhares de transístores e de reduzidas dimensões (*chips)* e de quase impossível controlo de qualidade e funcionamento. Utilizados a ritmo crescente, por exemplo, em sensores e sistemas de segurança em aeronaves, crescem os receios sobre a sua fiabilidade e a confiança nas suas origens.

Como sempre aconteceu, perante novas e sofisticadas formas de ataque começam a desenhar-se novas formas de defesa. Uma notícia do Reino Unido dá conta que o MI5, responsável pela segurança interna, contratou recentemente para o serviço cinquenta jovens de países asiáticos, que mostram aptidões especiais para trabalharem com sistemas informáticos e as intrusões que neles se podem provocar. Nos Estados Unidos foi criado, em 1 de Outubro de 2009, o *Cyber Command*. Não tem forças, o seu espaço de actuação é o ciberespaço e a sua missão é proteger as redes militares de transmissão de dados dos EUA e estar pronto para desencadear ciberataques sobre potenciais adversários. A OTAN e a União Europeia estão a considerar nos seus Conceitos Estratégicos a defesa contra este nova ameaça e as operações em redes informáticas. Há cerca de dois meses a Divisão de CIS do Estado-Maior Conjunto das Forças Armadas de Espanha lançou o seu primeiro exercício de Ciberdefesa que mostrou a necessidade de maior cooperação entre Forças Armadas, outros organismos do Estado e sociedade civil para fortalecer conceitos.

As reflexões estratégicas sobre este novo tipo de guerra, se assim se pode designar, apontam para os perigos que ataque e defesa podem conter, tal como aconteceu com a arma nuclear. A imprevisibilidade, rapidez e efeitos devastadores do ataque cibernético podem levar à tentação de ataques preventivos e pré-emptivos, que conduzem à escalada de consequências imprevisíveis. A empresa McAfee, que tem desenvolvido alguns sistemas de segurança informática diz que Israel, EUA, Rússia, China e França encabeçam uma lista de países que estão em verdadeira ciber-guerra-fria.

Esta é uma área nova para a defesa que a Revista Militar gostaria de desenvolver no ano corrente. Em ligação com iniciativas já existentes, como o Núcleo de Ciberguerra, apelamos aos nossos Sócios e leitores para sugestões e ideias no caminho a prosseguir.

_____

* Presidente da Direcção da Revista Militar.