A emergência da cyberware

dinheirovivo.pt/opiniao/a-emergencia-da-cyberware-12683122.html

26 de fevereiro de 2019

No passado dia 10 de fevereiro, o Pew Research Center (Washington), *fact-thank* apartidário cuja missão passa por informar o público sobre os principais desafios, atitudes e tendências do mundo, publicou um estudo realizado com base na perceção de 26 países sobre as principais ameaças globais.

Neste estudo, os ciberataques foram considerados como top 3 das ameaças globais, a par das alterações climáticas e terrorismo islâmico, chegando mesmo a ser considerados a principal ameaça em países como os EUA, o Japão, a Holanda ou a África do Sul.

É, no entanto, importante notar que os ciberataques considerados para efeitos deste estudo tratam-se daqueles perpetrados por outros países numa atitude declaradamente hostil. Este elemento é essencial enquanto indicador da eventual emergência do mais recente conceito de guerra cibernauta nesta nova Era da Informação. Pode ser também identificada como "*cyberwarfare*" ou "*cyberwar*" e representa, cada vez mais, um receio generalizado da comunidade cibernauta mundial.

Os "atores" normalmente envolvidos nas mais recentes *cyberwarfares* - entenda-se aqui, nos mais conhecidos ataques cibernéticos – são, tipicamente, cibercriminosos, normalmente motivados financeiramente, em analogia direta com o conceito de "mercenários". Obviamente, estes não são os únicos intervenientes no "jogo digital" – veja-se, por exemplo, o caso dos *hacktivistas* que se manifestam agressivamente, mas que, essencialmente, são motivados por "causas nobres".

Contudo, o estudo em causa alerta-nos para uma questão distinta e extremamente complexa. Neste novo "território", os Estados são também jogadores.

A emergência de uma *CyberWar* – quase que como se de uma III Guerra Mundial ou de uma Guerra Fria se tratasse – pode parecer tirada de livros e filmes de ficção cientifica mas está, de facto, cada vez mais próxima de se tornar uma realidade. Temos assistido, aliás, a algumas movimentações estratégicas nesse sentido:

- No final do ano passado, foram anunciadas em Bruxelas um conjunto de medidas para combater a "desinformação" nas redes sociais.

- Recentemente, foi aprovado o acordo provisório para o Mercado Digital Único, considerando, entre outros aspetos, investimento em setores digitais tão prementes como: a computação de alta performance, a Inteligência Artificial, a cibersegurança e confiança, as habilidades digitais avançadas e a inserção de tecnologias digitais na economia e sociedade.

- Já este ano, surgiram algumas notícias adiantando que, antes de abril, a Rússia irá, no contexto da sua estratégia de defesa e cibersegurança, testar a desconexão do país inteiro da internet – cenário que remonta, em parte, à postura que tem vindo a ser adotada pela China.

- Além disso, os casos de interferência em eleições, como nas presidenciais dos EUA ou do Brasil, são conhecidos do público e alertam-nos para importantes eleições que decorrerão, um pouco por todo o mundo, este ano.

- Também é conhecido que, no decorrer da Guerra do Iraque, houve um atraso no início dos bombardeamentos aéreos por parte dos Aliados, devido a um ataque cibernauta que estava em curso aos sistemas de informação da Defesa iraquiana, nomeadamente, nas redes e sistemas controlo das baterias antiaérea.

- Por fim, e num conceito lateral ao tradicional termo de *cyberwar*, podemos também referir que os serviços de informação ou inteligência há muito que utilizam o mundo digital e respetivos ataques para angariar informação do inimigo.

Neste jogo de tabuleiro, porém, não são apenas os Estados, numa perspetiva geral, que irão sair lesados. As pessoas – leia-se, civis –, as organizações e empresas, poderão sofrer os danos colaterais deste novo enquadramento geopolítico, devendo, para isso, estar preparados para responder aos desafios de cibersegurança que a Era Digital coloca, de forma quase instantânea. Os Estados irão ser obrigados a desenvolver capacidades de defesa e resposta/ataque cibernauta para além do tradicional armamento convencional. Este conceito militar híbrido, entre o armamento físico e o lógico, é já uma realidade em muitos Estados que foram obrigados a evoluir rapidamente para poder responder às ameaças e ataques já desenvolvidos em ambiente de *cyberwarfare*.

A consciência, a prevenção e, posteriormente, a capacidade de resposta, são essenciais para sobreviver neste cenário que promete, ainda, trazer mudanças significativas à realidade que conhecemos e que já está a mudar drasticamente. Importa reforçar que a *cyberwar*, numa abordagem de ataque militar, irá, provavelmente, ter alvos semelhantes

aos da guerra convencional, nomeadamente, infraestruturas criticas, como a energia, transportes, comunicações, entre outros, capazes de colocar em causa a estabilidade e sustentabilidade de um País.

Bruno Castro é CEO da VisionWare