Ciberterrorismo: a nova tática de guerra do século XXI

dinheirovivo.pt/opiniao/ciberterrorismo-a-nova-tatica-de-guerra-do-seculo-xxi-15310280.html

2 de novembro de 2022

O mês de outubro é assinalado na União Europeia, há dez anos, como o mês da Cibersegurança, contudo, o conceito de ciberterrorismo ganhou destaque muitos anos antes, após o fatídico dia que mudou o mundo e nunca mais nada voltou a ser o que era - o 11 de setembro de 2001. Para além de todo o terror que este dia significou para todo o mundo, expôs também as várias ameaças que estamos todos subjacentes face à cibersegurança neste novo mundo cibernético.

À data de hoje, um dos focos da agenda mediática é justamente, a segurança nacional em todas as vertentes, sendo que várias empresas privadas investiram largamente em especialistas e tecnologia para combaterem os perigos iminentes que este novo paradigma digital nos veio obrigar a saber conviver social e profissionalmente. Mais do que nunca, a comunidade cibercriminosa tem vindo a desenvolver mecanismos cada vez mais sofisticados para aceder a informações pessoais através de, cada vez mais, ataques direcionados a pessoas assente na fragilidade do fator humano. Estando os sistemas financeiros, militares e governativos interligados mais do que nunca, acrescido do facto de termos passado a viver numa "sociedade interconectada em rede" de forma contínua, acredito que o ciberterrorismo se afigura como a principal ameaça da nossa atualidade.

O ciberterrorismo, como a própria denominação indica, é a combinação entre o terrorismo e o ciberespaço. O propósito do ciberterrorismo passa por intimidar um governo, a sociedade civil ou outro tipo de entidades através de ataques dirigidos a redes, sistemas, informação ou pessoas utilizando veículos digitais. Apesar do ciberterrorismo, ao nível da violência física direta, não constituir uma ameaça, é inevitável que cause impactos psicológicos significativos na sociedade e nas populações - principalmente por ser um tipo de terrorismo amplamente desconhecido e no qual há uma grande falta de (des)informação. Ainda assim, e através também de ações de ciberterrorismo, será expectável ataques direcionados a infraestruturas (potencialmente categorizadas como "críticas") que venham a causar violência e impacto físico direto sobre pessoas. Para além da enorme abrangência de potenciais vítimas e impactos, levanta-se a questão primordial deste tipo de ações passarem a constituir uma ameaça enorme, com consequências graves, para as democracias neste novo paradigma (cada vez mais) digital.

Para lidarmos de forma eficaz com o ciberterrorismo, é essencial não só criarmos leis - atuais e modernas - para chamarmos à justiça os responsáveis, assim como implementar procedimentos para que os vários agentes (forças policiais, por exemplo) possam analisar de forma precisa e em tempo útil a (real) ameaça cibernética. É fundamental capacitar as autoridades de ferramentas (e conhecimento) para o constante controlo e monitorização da *deepweb/darkweb* (identificação de *leaks*), análise de riscos de cibersegurança das

infraestruturas críticas, *profiling* de determinados indivíduos através de técnicas de *humint*, deteção e defesa de ciberataques e a monitorização e supervisão contínua de determinados grupos cibercriminosos.

Em Portugal, estamos a caminhar (embora muito devagar) para conseguir dar respostas nesta área. No passado dia 20 de outubro, foi aprovada, em Conselho de Ministros, a Estratégia Nacional de Ciberdefesa, baseada em várias diretrizes, as quais visam "incrementar a nossa resiliência e soberania", como refere Helena Carreiras, Ministra da Defesa Nacional. A estratégia envolve a criação de uma escola de ciberdefesa para promoção da investigação, desenvolvimento e inovação do ciberespaço - algo que considero imprescindível uma vez que é necessário aumentar as qualificações em matéria de cibersegurança e sensibilizar os cidadãos para a importância de nos mantermos (ciber)seguros.

Não obstante, o país ainda não está devidamente preparado para responder de forma positiva e eficaz a uma ameaça cibernética. Devido ao envelhecimento da nossa população existem níveis muito elevados de falta de literacia digital nesta matéria e, portanto, de preparação e prevenção deste problema do século XXI. Numa sociedade democrática, com valores liberais e com respeito pelas liberdades e garantias, temos de assimilar que, atualmente, a guerra já não se faz somente com o armamento convencional. A guerra cibernética é uma das mais perigosas formas de guerra de todos os tempos e devemos fazer tudo o que está ao nosso alcance para sobreviver e tornarmo-nos cada vez mais (ciber)conscientes.