The real Grinch: ciberataques com motivações geopolíticas

dinheirovivo.dn.pt/opiniao/the-real-grinch-ciberataques-com-motivações-geopolíticas

Os ciberataques podem ter várias e distintas motivações. As mais comuns, ou pelo menos, aquelas a que estamos mais habituados, são as motivações financeiras. Contudo, perante o atual contexto político e securitário, ao nível global, os ciberataques motivados por interesses geopolíticos continuarão a ser uma tendência crescente em 2025, desempenhando um papel central na rivalidade entre Estados e em disputas globais. Tal dinâmica reflete a crescente dependência da infraestrutura digital para operações económicas e militares, tornando o ciberespaço num campo estratégico para conflitos e influência política.

Os ciberataques são menos dispendiosos e menos arriscados do que conflitos militares convencionais, com a vantagem para os agentes de ameaças que podem igualmente causar um impacto devastador no inimigo – desde, paralisar infraestruturas críticas, roubar informações sensíveis ou desestabilizar economias – tudo isso sem mobilizar tropas ou equipamentos militares.

Com as habituais disputas entre grandes potências, como os Estados Unidos, China e Rússia, que continuam a intensificar-se, a ambição pelo controlo de tecnologias emergentes e a soberania aumenta, e o ciberespaço é frequentemente utilizado como uma extensão dessas tensões, com ciberataques destinados a demonstrar força ou influenciar políticas internas e externas.

A manipulação de informações através de campanhas de desinformação e ciberataques a processos eleitorais foi algo já sentido em 2024 e certamente, continuará a ganhar força. Os meios digitais concretizam-se como meios viáveis para levar a cabo estratégias para influenciar decisões políticas noutros países e exemplos recentes de interferências em eleições, mostram que esse método é eficaz para enfraquecer a confiança nas instituições e nos próprios processos democráticos.

Os ciberataques são ainda frequentemente utilizados para fins de ciberespionagem, principalmente, para roubar segredos industriais, propriedade intelectual e informações confidenciais de governos e empresas. Em 2025, a ciberespionagem poderá tornar-se ainda mais sofisticada sobretudo devido ao recurso à inteligência artificial para identificar e explorar vulnerabilidades.

As infraestruturas críticas continuam a ser um dos alvos favoritos dos atacantes; não há melhor forma de perturbar uma sociedade e os agentes de ameaças estão bem cientes deste facto. Como tal, existem setores particularmente mais vulneráveis a ciberataques com este tipo de motivações, nomeadamente, o setor da energia, saúde, financeiro e ainda, telecomunicações. Estes são, indubitavelmente, alvos estratégicos de

ciberataques motivados por interesses geopolíticos e que podem causar interrupções significativas, ao afetar a sociedade civil e assim exercer pressão política ou económica sobre os Estados atacados.

Neste contexto, as preocupações para 2025 são algumas. Por um lado, as rivalidades entre grandes potencias podem intensificar ciberataques mútuos relacionados com a competição por hegemonia tecnológica e influência global. Os próprios países já em conflito, como por exemplo, a Rússia e a Ucrânia, deverão continuar a utilizar ciberataques para destabilizar os seus oponentes e influenciar cenários geopolíticos mais amplos. E, existem ainda os grupos de hacktivistas apoiados por Estados que continuam cada vez mais a desempenhar papéis críticos em operações no ciberespaço, cada vez mais imprevisíveis e disruptivas.

A intensificação de ciberataques geopolíticos exigirá maior cooperação internacional para regulamentar o ciberespaço. À medida que os atacantes evoluem continuamente as suas estratégias, a comunidade de cibersegurança em geral deverá procurar ter capacidade de resposta. A procura de cooperações globais, a criação de parcerias público-privadas e o desenvolvimento de estruturas para combater ameaças são vitais para aumentar a resiliência coletiva. No entanto, as diferenças ideológicas e os interesses distintos entre os Estados dificultam o consenso na criação de normas globais eficazes. A tendência aponta para um cenário de conflito constante no ciberespaço, onde a capacidade de adaptação e inovação será essencial para evitar danos e proteger interesses estratégicos.

Bruno Castro, Fundador & CEO da VisionWare. Especialista em Cibersegurança e Investigação Forense