A intrincada relação entre a cibersegurança e o reacender do conflito Israel-Palestina

dinheirovivo.pt/opiniao/a-intrincada-relacao-entre-a-ciberseguranca-e-o-reacender-do-conflito-israel-palestina-17305115.html

8 de novembro de 2023

Nos últimos anos, a cibersegurança emergiu como um elemento crítico no contexto do conflito Israel-Palestina, adicionando uma nova dimensão ao já complexo cenário político e militar da região. No artigo deste mês e face à atualidade dos acontecimentos, exploro aqui de forma breve, a intrincada relação entre as questões de cibersegurança e o reacender do conflito, salientando como as ameaças e as ações cibernéticas têm desempenhado um papel fundamental nesse contexto.

A ciberespionagem e as relações entre Israel-Palestina: A cibersegurança está intrinsecamente ligada ao reacender do conflito Israel-Palestina, com ambos os lados envolvidos num intenso clima de ciberespionagem. Israel e vários grupos palestinos têm-se envolvido em atividades de vigilância cibernética para obter informações estratégicas, minar a infraestrutura do adversário e ganhar óbvias vantagens táticas.

Ciberataques e a escalada do conflito: A escalada do conflito na região também sido igualmente influenciada pelo elevado número de ciberataques registados desde o regresso deste conflito. Grupos palestinos, como o Hamas, lançaram ofensivas cibernéticas contra alvos israelitas, enquanto Israel respondeu com ataques cibernéticos a infraestruturas ligadas a grupos extremistas. Essa dinâmica de ataques e contra-ataques cibernéticos tem contribuído para uma escalada de hostilidades.

Proteção de infraestruturas críticas: As infraestruturas críticas, como os sistemas de energia e água, têm sido alvo de uma constante preocupação no que diz respeito a este conflito. Ambos os lados estão cientes de que a cibersegurança é fundamental para a proteção de suas infraestruturas vitais. Os esforços para fortalecer a segurança cibernética desses sistemas tornaram-se uma prioridade, uma vez que, um ataque bem-sucedido poderá ter consequências devastadoras.

Influência das grandes potências regionais e internacionais: A influência das potências regionais e internacionais no conflito Israel-Palestina também se estende ao domínio cibernético. Estados como o Irão e a Rússia têm apoiado grupos palestinianos, fornecendo-lhes capacidades cibernéticas, tecnológicas e humanas mais avançadas. Tal facto aumenta a complexidade da situação e amplia as implicações da cibersegurança no conflito.

A diplomacia cibernética e os atuais desafios para a resolução do conflito: A diplomacia cibernética tornou-se uma componente vital nas tentativas de mediar o conflito, representando outro patamar no âmbito das tradicionais conversações diplomáticas. A

comunidade internacional, nos seus esforços para encontrar uma solução pacífica, precisa considerar não apenas as questões tradicionais, como também as ameaças e as reais oportunidades decorrentes

do ciberespaço. As negociações de cibersegurança podem assim desempenhar um papel crucial na construção da confiança entre as partes envolvidas.

A discrepância de forças pró-palestina/contra-ocidente versus pró-Israel: Pode ser uma surpresa visto que, temos o inverso do lado da Ucrânia/Rússia. A discrepância entre estas forças pode ser surpreendente. Enquanto a Rússia é frequentemente considerada uma superpotência cibernética, com habilidades avançadas em ataques cibernéticos, o conflito Israel-Palestina muitas vezes envolve grupos não-estatais e atores menos convencionais. Isso cria um cenário no qual a cibersegurança desempenha um papel mais equilibrado, com ambos os lados a recorrer a táticas para proteger os seus interesses e espalhar a sua mensagem. Em contraste com o conflito Ucrânia-Rússia, onde os Estados-nação desempenham um papel mais proeminente na guerra cibernética, o conflito Israel-Palestina apresenta uma rede de atores mais diversificada, incluindo grupos militantes, ativistas e hackers independentes, todos desempenhando um papel no cenário cibernético.

A relação de apoio também cibernético de grupos cibercriminosos russos em favor do bloco contra-ocidente: é uma preocupação crescente na arena da cibersegurança global. Esses grupos, frequentemente associados ao governo russo, têm demonstrado um padrão de atividade cibernética agressiva, visando países e organizações que se opõem às políticas do Ocidente. Seja por meio de ataques cibernéticos diretos, desinformação ou campanhas de influência, esses grupos procuram minar a estabilidade e a segurança cibernética em regiões de interesse geopolítico, contribuindo assim para o reacender de conflitos, como o caso Israel-Palestina. Essa relação complexa entre cibercriminosos russos e atores estatais desafia a comunidade internacional a encontrar soluções pacíficas, diplomáticas e eficazes para proteger a segurança digital global e a estabilidade geopolítica.

A influência da guerra cibernética na geração de *fake news* e tentativa de mediatização do conflito: amplificando as tensões existentes e como forma de influência da perceção pública do conflito. A disseminação de desinformação desempenha um papel crucial na moldagem da opinião pública e na manutenção dessas mesmas tensões.

Em suma, a relação entre a cibersegurança e o reacender do conflito Israel-Palestina é intrincada e multifacetada. As ameaças cibernéticas e os ataques desempenham um papel significativo e crescente na escalada do próprio conflito no terreno, enquanto a proteção da infraestrutura crítica e a influência de atores regionais e internacionais no domínio cibernético acentuam cada vez mais a complexidade da situação. A diplomacia cibernética surge por isso, como um novo meio de abordar as questões em jogo, à medida que a comunidade internacional procura, urgentemente, uma resolução pacífica para um dos conflitos mais duradouros e desafiantes do mundo.