“A estratégia de guerra convencional passará também a incluir acções militares de vertente cibernética”

securitymagazine.pt/2022/03/09/a-estrategia-de-guerra-convencional-passara-tambem-a-incluir-accoes-militares-de-vertente-cibernetica

SecurityMagazine 09/03/2022

A actual situação vivida na Ucrânia irá levar à entrada num novo paradigma no que à cibersegurança diz respeito. ´”É inevitável”, avança à Security Magazine Bruno Castro, fundador e CEO da VisionWare e especialista em cibersegurança e investigação forense. O responsável reforça que “muitos dos ataques que virão a ser desenvolvidos daqui em diante, independentemente da motivação, serão realizados à distância, de longa duração e de forma anonimizada. Será um novo conceito de guerra”.

SECURITY MAGAZINE – Do ponto de vista da cibersegurança, como vê a actual situação vivida na Ucrânia, nomeadamente no que toca ao úmero de incidentes reportados, gravidade e principais implicações?

Bruno Castro – Infelizmente, e tal como na guerra bélica, também a vertente cibernética tem estado muito envolvida num conceito claro de warefare, ou seja, falamos também de guerra cibernética, utilizando armas cibernéticas para danificar ou destabilizar sistemas digitais/informáticos que possam colocar em causa a estabilidade do país. Temos assistido a ataque cibernéticos de parte a parte. Inclusive, estamos a ver novamente o reaparecimento de Hackivismo – até num alinhamento de condenação mundial – de um grande número de grupos cibercriminosos (e não só) a desenvolver acções hostis contra a Rússia.

No início desta situação, o próprio governo ucraniano convocou a comunidade de cibersegurança para se juntar no sentido de ajudar o país na sua defesa (e anunciou também a formação de um "IT Cyber Army"). Tanto do lado ucraniano como russo, contabilizam-se mais de 30 grupos que, nos últimos dias, têm reportado diversas iniciativas levadas a cabo, nomeadamente às TVs russas, sites governamentais, farmácias, bancos, empresa envolvida na recepção de dados de satélites, reactores nucleares, a grupos de ransomware pró-Rússia, entre outros. Como devemos olhar para estas iniciativas no ciberespaço?

Tal como se previa, o cenário de guerra inclui também o mundo do ciberespaço, e portanto, daqui em diante, a estratégia de guerra convencional passará também a incluir acções militares de vertente cibernética. Tal como o apoio militar e de apoio humano prestado pela comunidade mundial à Ucrânia, também vários grupos – criminosos ou não – têm vindo a desenvolver acções de guerra cibernética contra a Rússia num conceito de Hackivismo que há muito não se via.

Face a esta situação, é previsível um aumento do número de ciberataques a países da União Europeia nos próximos tempos, que tenham origem/ligação a este conflito?

Sim, completamente. A guerra cibernética tem várias vantagens face a uma guerra convencional bélica. Primeiro, é muito menos dispendiosa e não implica risco humano de quem desenvolve o ciberataque (agressor), e por outro lado, tem a possibilidade de ser "anónima" por parte do agressor face ao agredido.

É provavelmente muito menos visual mediaticamente, o que pode ajudar a controlar a opinião pública, e consegue ter igualmente acções destrutivas de enorme alcance.

Será obviamente mais lenta e com menor abrangência do que uma acção bélica. Portanto, diria que nos próximos anos, a tendência será existir cada vez mais acções de guerra cibernética em países da NATO ou Comissão Europeia face a este novo muro que se avizinha com a Rússia e Bielorrússia. Não nos podemos também esquecer das acções cibernéticas de espionagem que já são há muito uma realidade, mas agora irão certamente acentuar.

Considera que os especialistas em cibersegurança em Portugal deverão estar mais atentos nos próximos tempos e elevar os níveis de alerta e protecção das suas organizações? Embora as preocupações em ciber devam ser transversais a todas as organizações, existem sectores que deverão estar mais "atentos" relativamente a estes temas?

Sim. Aliás, já tem sido um sintoma que temos estado a viver em Portugal desde os últimos 6 meses. O cenário de ciberataques de elevada envergadura e impacto tem vindo a ser uma realidade muito acentuada no panorama nacional.

Agora, com este clima de terror face à guerra pré mundial que estamos a viver, diria que certamente ciberataques a infraestruturas críticas que possam colocar em causa a estabilidade de uma nação, passaram a ser efectivamente um alvo militar.

Adicionalmente, e pela questão das sanções económicas em curso, também diria que acções de fraude (roubo de dinheiro) e espionagem na indústria e governos será (ainda) mais uma forte tendência.

É importante reforçar que muitos dos ataques que virão a ser desenvolvidos daqui em diante, independentemente da motivação, serão realizados à distância, de longa duração e de forma anonimizada. Será um novo conceito de guerra.

Considera que daqui para a frente entraremos num novo paradigma relativamente à temática da cibersegurança?

Sim, é inevitável. Conforme referi anteriormente, já o temos vindo a sentir no último meio ano, mas agora, a cibersegurança – seja na vertente defensiva ou ofensiva – passará a ser uma obrigatoriedade para todos os Estados. Os Governos, Administração Central e Pública e o tecido empresarial terão de se adaptar a este novo paradigma de guerra cibernética. O mundo mudou e nunca mais será o mesmo.