A volatilidade geopolítica e a fragilidade digital do Ocidente

A volatilidade geopolítica deixou de ser um ruído de fundo para se tornar num fator estrutural nas operações de cibersegurança e, em 2026, seria até algo ingénuo falar de cibersegurança como um domínio técnico separado da atual política internacional. Cada conflito regional, cada sanção económica e cada realinhamento estratégico tem hoje uma tradução direta no risco cibernético das organizações.

A realidade mostra-nos que a infraestrutura digital é cada vez mais um campo de disputa entre Estados: datacenters, cabos submarinos, satélites e plataformas cloud são ativos estratégicos, sujeitos a pressões diplomáticas, restrições legais súbitas e, em alguns casos, a sabotagem e ciberataques. A geopolítica não entra nos sistemas pela porta da frente, infiltra-se através de dependências invisíveis.

Um exemplo evidente é o caso recente da operação militar dos Estados Unidos para capturar o presidente venezuelano Nicolás Maduro. Um dos elementos mais notórios é a admissão de que capacidades cyber foram usadas para desligar ou interferir no sistema de energia e de comunicações em Caracas, facilitando assim a inserção das forças e confundir as defesas locais.

Isto confirma que operações cyber já estão a ser integradas em operações geopolíticas de alto impacto, incluindo ações com efeitos físicos no terreno. Não se trata apenas de ataques informáticos isolados ou de espionagem, mas antes de ciber operações coordenadas com meios militares convencionais para atingir objetivos estratégicos.

Assim, a escalada de conflitos híbridos, tensões entre blocos económicos e disputas estratégicas refletem-se hoje em ciber operações persistentes: espionagem, sabotagem, campanhas de desinformação e ataques a infraestruturas críticas deixam de ser exceções para se tornarem instrumentos normalizados de pressão política. Em consequência, organizações civis e empresas privadas passam a ocupar um papel desconfortável: não são alvos estratégicos por si mesmos, mas tornam-se antes, danos colaterais previsíveis. Em contextos de tensão geopolítica, a distinção entre ator estatal, grupo criminoso e proxy patrocinado por um Estado torna-se deliberadamente ambígua, sendo essa mesma ambiguidade uma arma poderosa.

Esta realidade expõe uma fragilidade fundamental das operações no ciberespaço: a dependência de cadeias globais. Software desenvolvido num país, mantido noutro, alojado num terceiro e operado a partir de um quarto país, deixa de ser apenas uma escolha económica passando a ser uma decisão com implicações geopolíticas. Em cenários de sanções, conflitos ou ruturas diplomáticas, estas cadeias podem quebrar-se de forma abrupta, deixando organizações expostas. Assim, a questão já não é apenas se, uma organização está protegida contra ciberataques, mas se, estará preparada para operar em ambientes de confiança degradada, onde parceiros de ontem podem tornar-se os riscos de amanhã.

Este contexto deveria servir de alerta inequívoco para a Europa investir seriamente em capacidades de ciberdefesa, não apenas em tecnologia, mas muito mais em talento, know-how, inteligência partilhada e capacidade operacional real. Sem isso, a dependência de terceiros e a fragmentação entre Estados-Membros continuarão a transformar o espaço digital europeu num terreno vulnerável, onde a dissuasão é fraca e a resposta é lenta.

Em 2026, operar no ciberespaço implica escolher dependências, alianças tecnológicas e, implicitamente, posicionamentos geopolíticos. Ignorar esta realidade não reduz o risco, apenas o desloca para zonas menos visíveis e mais difíceis de controlar.

Num mundo marcado por instabilidade e rivalidades crescentes, as operações no ciberespaço precisam de abandonar a ilusão de isolamento técnico. A cibersegurança deixou de ser somente uma questão de firewalls, antivírus e resposta a incidentes. É, cada vez mais, uma questão de leitura geopolítica, de estratégia e de coragem para reconhecer que o risco digital é, hoje, uma extensão direta do risco global.

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