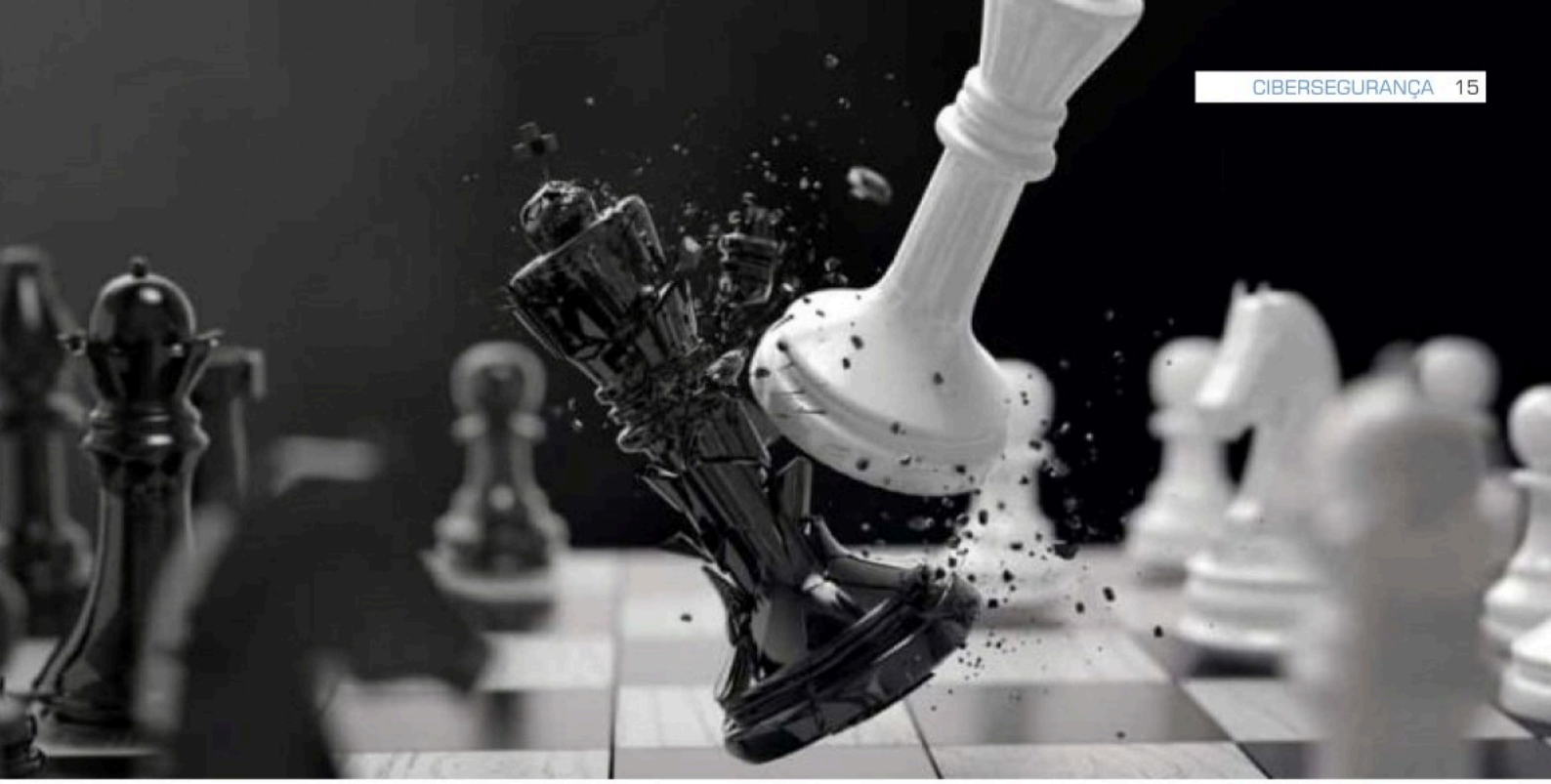

NO XADREZ GEOPOLÍTICO, A CIBERSEGURANÇA FAZ XEQUE-MATE

BRUNO CASTRO
Fundador & CEO da VisionWare
Especialista em Cibersegurança e Investigação Forense

20 anos VisionWare since 2006

A instabilidade geopolítica deixou de ser um simples pano de fundo e passou a assumir um papel estrutural na forma como as organizações encaram a cibersegurança. Em 2026, já não faz sentido tratar a segurança digital como um domínio puramente técnico, desligado da política internacional e das dinâmicas de poder globais. A infraestrutura tecnológica global – centros de dados, cabos submarinos, satélites, redes de telecomunicações – transformou-se num ativo estratégico de disputa entre Estados, sujeito a pressões diplomáticas, mudanças regulatórias inesperadas e, em casos extremos, a sabotagem e a operações de ataque. A geopolítica não entra nos sistemas de forma explícita, mas infiltra-se através das dependências tecnológicas, das cadeias de fornecimento globais e das relações de confiança entre parceiros.

Um dos sinais mais recentes desta crescente politização da cibersegurança foi a decisão dos Estados Unidos de abandonar o Global Forum on Cyber Expertise (GFCE) e o European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), duas estruturas internacionais dedicadas à cooperação e fortalecimento das capacidades em matéria de cibersegurança e de resposta a ameaças híbridas. Esta saída faz parte de uma ordem executiva que determina a retirada dos EUA de dezenas de organizações internacionais que, na avaliação da administração norte-americana, já não estariam alinhadas com os seus "interesses nacionais", incluindo plataformas

GFCE Global Forum on Cyber Expertise

Hybrid CoE

de cooperação que reúnem governos, empresas, universidades e equipas de resposta a incidentes. A decisão pode enfraquecer a coordenação global em resposta a ciberataques transnacionais, reduzir a partilha de inteligência e fragmentar ainda mais o ecossistema internacional de resiliência digital, justamente num momento em que a colaboração é apontada como um dos pilares essenciais para enfrentar ameaças complexas.

Também os exemplos recentes confirmam que as capacidades cibernéticas são cada vez mais utilizadas como parte integrante de operações geopolíticas de elevado impacto, com efeitos concretos no terreno. Um caso ilustrativo foi a intervenção militar recente dos Estados Unidos para capturar o presidente venezuelano Nicolás Maduro, onde capacidades cibernéticas foram utilizadas para interromper sistemas de energia e comunicações em Caracas, facilitando a operação no terreno. Isto comprova que as operações cibernéticas já são integradas em campanhas geopolíticas de elevada intensidade, com efeitos físicos tangíveis e não apenas através de ciberataques isolados.

Neste contexto, organizações civis e empresas privadas tornam-se frequentemente vítimas colaterais previsíveis, mesmo não sendo alvos estratégicos diretos. A fronteira entre atores estatais, grupos criminosos e entidades patrocinadas por Estados é cada vez mais difusa e deliberadamente ambígua, o que dificulta a atribuição de responsabilidades e a resposta coordenada.

A FRAGMENTAÇÃO REGULATÓRIA E A DEPENDÊNCIA EXCESSIVA DE TERCEIROS CONTINUAM A TORNAR O ESPAÇO DIGITAL EUROPEU MAIS VULNERÁVEL, COM FRACA CAPACIDADE DE DISSUASÃO E RESPOSTAS LENTAS FACE À VELOCIDADE DAS AMEAÇAS.

Este contexto deveria servir como um sinal de alerta claro para a Europa reforçar de forma consistente as suas capacidades de ciberdefesa, não apenas ao nível da tecnologia, mas sobretudo no investimento em talento, formação, inteligência partilhada, cooperação entre Estados-Membros e capacidade operacional efetiva.

A fragmentação regulatória e a dependência excessiva de terceiros continuam a tornar o espaço digital europeu mais vulnerável, com fraca capacidade de dissuasão e respostas lentas face à velocidade das ameaças. Em 2026, operar no ciberespaço implica, inevitavelmente, escolher alianças estratégicas e posicionamentos implícitos no tabuleiro geopolítico. Ignorar esta realidade não reduz o risco, apenas o transfere para áreas menos visíveis e mais difíceis de controlar. Num mundo marcado por instabilidade, rivalidades e aceleração tecnológica, a cibersegurança pode fazer a diferença no derradeiro xeque-mate.