O desafio da governança da defesa cibernética

Tarcísio Takashi Muta

Crédito da imagem: Fundação Ezute

Em um cenário global caracterizado por ameaças externas difusas e assimétricas, baseadas em tecnologias com ciclos de vida muito rápidos, sem controle do Estado e sem vínculos nacionais, a Defesa Cibernética tornou-se o dispositivo fundamental para atender à preservação dos objetivos e interesses dos países. No Brasil, a Estratégia Nacional de Defesa (END) identifica e estabelece parâmetros para essa atividade, juntamente com a Defesa Nuclear e a Espacial, e a coloca sob a coordenação do Exército Brasileiro, em uma concepção sistêmica, e que requer métodos, procedimentos e características que lhe são peculiares.

O espaço cibernético é um ambiente em permanente mudança, que tem a tecnologia como base, formado por uma complexa rede de agentes, equipamentos e locais, cujo aumento significativo de sistemas e redes de informação e comunicação é estimulado a partir de facilidades crescentes de acesso à Internet. Com isso, proliferam também as ameaças e as vulnerabilidades, justificando a urgência do fortalecimento de uma cultura de segurança cibernética e de uma atuação estratégica que considere as suas diversas dimensões, tanto em termos das tecnologias utilizadas, quanto os aspectos sociais e seu inter-relacionamento. Em suma, é fundamental a visão sistêmica.

Do ponto de vista da defesa, esse novo teatro de operações e de conflitos vem se somar às zonas terrestres, marítimas e aeroespaciais, mas seu conjunto de ações é transversal a todos esses domínios, no que se refere à proteção segura dos sistemas de informação e de transmissão de dados para produção de conhecimento de inteligência. Atualmente, são inúmeros e variados os meios e as ferramentas que compõem o espaço cibernético, envolvendo redes de comunicação, aplicativos, tecnologias de informação, inteligência artificial e a chamada internet das coisas, que abrange de celulares a relógios, óculos, e muitos dispositivos que ainda iremos conhecer. A própria automação da indústria 4.0 e num contexto mais amplo o desenvolvimento das cidades inteligentes, se dá com base na utilização desses meios.

São notórias as dificuldades para tomadas de decisões relacionadas ao gerenciamento da segurança cibernética, especialmente pelos grandes volumes de dados envolvidos. Isso exige a implantação de controles, a atualização sistemática das práticas e procedimentos adotados para os sistemas de informação, desde o estabelecimento de requisitos direcionadores até uma gestão de segurança que permita avaliar riscos e capacidade de resposta diante de eventuais incidentes. A palavra chave para o êxito do enfrentamento dessas ameaças é resiliência. Não basta apenas estar apto a se defender, mas sim poder principalmente antecipar, e também prover uma rápida reação, com capacidade de mudança e adaptação à nova realidade no caso de um ataque. Nesse novo teatro de operações é preciso otimizar ao máximo a capacidade de manter as infraestruturas críticas operando sob condições de ataque, ou de restabelecê-las após uma ação adversa, sem chances de quebra. As fronteiras nesse novo ambiente não são tão claras quanto as dos domínios clássicos. O ambiente cibernético oferece mais condições para que um indivíduo, não necessariamente vinculado a um Estado, possa ameaçar ou provocar danos, em termos nacionais ou mesmo globais, impedindo a disponibilidade, integridade, confidencialidade e autenticidade de dados e informações, e afetando sistemas vitais para o funcionamento das sociedades.

É um novo ambiente, totalmente assimétrico, não é mais uma questão de país contra país. Nesse novo espaço cibernético, como não há mais fronteiras, os controles ficam fragilizados, o que exige outro paradigma, outra forma de se defender. A inteligência artificial

permite que os dispositivos estejam vinculados à internet e rapidamente se reconfigurem, obrigando quem tem a responsabilidade pela defesa cibernética a desenvolver a capacidade de aprender e reaprender rapidamente com as situações.

O soldado cibernético, por sua vez, necessitará formação complementar específica e com visão sistêmica. Será um profissional altamente especializado, que terá como desafio monitorar essas novas fronteiras assimétricas em constante mutação, identificar ameaças e configurar respostas que possam impedir a sua concretização, neutraliza-las e se necessário contra-atacar.

Para tanto serão necessárias mudanças de comportamento e até alterações culturais, para definir mais prontamente o tipo de capacitação e conhecimento mais adequados para permitir que esse novo soldado possa atuar na plenitude da sua eficiência e eficácia. Será importante também definir qual será a sua missão e pensar na estrutura estratégica necessária para otimizar sua atuação nesse novo contexto.

O desafio, portanto, é estratégico, tático e operacional. Será fundamental harmonizar as condições de compartilhamento de informações com a proteção, segurança, confidencialidade e privacidade, e contextualizar esse novo teatro de operações como um domínio da defesa no qual os agentes públicos e privados se organizam para oferecer respostas rápidas. E, na visão dos especialistas, serão mais bem sucedidas em dar respostas a esse novo tipo de desafio as sociedades que puderem se organizar através de uma modelagem institucional da sua atuação em termos da governança da defesa cibernética.

Como ressalta a doutrina de defesa cibernética do Ministério da Defesa, esse novo cenário estratégico exige a atuação integrada de vários órgãos, sejam civis ou militares, cada um com atribuições específicas, mas com um modelo de atuação em um ambiente interagências. Nesse sentido, no âmbito da responsabilidade e sob a coordenação conferida pela END ao Exército Brasileiro, seria recomendável o estabelecimento de uma estrutura de alto nível na administração pública, que seja responsável por interagir de forma mais livre e direta com todos os interessados.

Um organismo que funcione como um grande facilitador em um ambiente colaborativo, com procedimentos pré-estabelecidos e informações que estejam disponíveis para todos os entes envolvidos, sejam governamentais, sejam organismos da sociedade, comprometidos há mais tempo com as novas tecnologias que balizam esse domínio e, portanto, capacitados a atuar no sentido de impedir que sistemas estratégicos vitais sejam afetados por uma ameaça ou um ataque direcionado a um ou mais desses agentes. E que em sua configuração propague, também, informações para a sociedade, permitindo que o maior número possível de cidadãos tenha informações sobre as questões que envolvem a segurança do sistema a partir de práticas seguras na circulação de dados pessoais na Internet. T&D

N. da R.: Tarcísio Takashi Muta é presidente do Conselho de Administração da Fundação Ezute.