A inovação é o motor para a produção de uma nova geração de sistemas de defesa

Delfim Ossamu Miyamaru

O aparelhamento do Poder Militar tem sido impulsionado pelos avanços tecnológicos em diferentes setores de pesquisa e desenvolvimento. Vivenciamos o surgimento de diversas tecnologias e inovações de uso pessoal e corporativo, cujas pesquisas foram originadas no meio militar.

Ao final da Segunda Guerra Mundial verificamos o advento do computador e, ao longo do tempo, chegamos à criação da Internet. Com sua natureza descentralizada e sua resiliência pudemos entrar na era da informação. Esses são exemplos claros do transbordamento tecnológico que não só aumentam as capacidades do setor de defesa mas que trazem também, de forma até exponencial, benefícios para a sociedade civil.

Mediante esse contexto várias tecnologias ficaram em evidência na atualidade. A primeira que podemos citar é o "Big Data".

Essa tecnologia vem se tornando crucial, principalmente no contexto de guerras assimétricas, pois fornece um recurso de inteligência situacional, por meio do processamento e análise de uma quantidade massiva de dados provenientes de sensores e dispositivos, muitos deles atuando em cenários da vida do cotidiano e não em teatros sofisticados de conflitos ou em operações militares. Isso graças à ascensão da IoT ("Internet of Things").

A capacidade de criar correlações e de quantificar aspectos do mundo que nunca foram considerados permite o combate, por exemplo, ao terrorismo e fornece mecanismos que enriquecem os elementos táticos operacionais que apoiam a tomada de decisão estratégica.

Toda essa informação e a forma como ela é coletada ao longo da exploração de dados, leva ao questionamento sobre a segurança cibernética, outro arcabouço de conhecimentos e tecnologias hoje em evidência. A chamada cyber-segurança, faz uso da tecnologia para o combate aos crimes cibernéticos para a proteção dos sistemas sigilosos e críticos considerados primordiais pela segurança nacional.

O Brasil e os Estados Unidos, por exemplo, criaram estruturas de comando para planejar e implementar políticas de defesa cibernética. O Comando de Defesa Cibernética do Exército (ComDCiber) e o Comando Cibernético (USCYBERCOM), respectivamente, são claras demonstrações da importância que estes países dão ao uso do conjunto de tecnologias e conhecimentos associados ao tema, onde novos paradigmas de segurança estão sendo desenvolvidos. Um deles é conhecido por "zero trust" (confiança zero).

No modelo tradicional de segurança de Tecnologia de Informação, a arquitetura se baseia na ideia de que uma organização possui barreiras que limitam o acesso de qualquer sistema externo à sua rede. Entretanto, qualquer um já dentro da organização tem acesso livre a qualquer conteúdo interno, o que inclui possíveis invasores que burlaram algum sistema de autenticação.

No "zero trust", ao contrário do modelo tradicional, a arquitetura de segurança parte da ideia de que, por padrão, as organizações nunca devem confiar em qualquer entidade interna ou externa que entre em seu perímetro, ou seja, "nunca confie, sempre verifique". Nesse modelo, pressupõe-se que pode haver invasores dentro e fora da rede e, portanto, nenhum usuário ou dispositivo deve ser confiável.

Os Estados Unidos passaram a concentrar esforços para implementar "zero trust" nas suas organizações internas. No seu programa "Comply to Connect", esse conceito já está sendo utilizado para verificações de laptops e celulares antes de se conectarem à rede.

A robótica e a inteligência artificial (IA) também estão no palco do atual cenário militar. Ambos se tornaram populares com o advento dos drones.

A partir dos atentados terroristas de 2001, sistemas robóticos aparecem como sendo um dos principais recursos utilizados, consumindo assim, uma parcela importante de seus investimentos militares.

Na Rússia, o Exército está trabalhando no desenvolvimento de uma unidade militar armada com tanques robôs, equipados com um canhão automático de 30mm, lança chamas e mísseis antitanques.

Em recente entrevista, a área de defesa do Reino Unido, confirmou que o número de máquinas autônomas ou controladas remotamente pode crescer nas Forças Armadas do país, com a estimativa de que, em 2030, o Exército Britânico poderá contar com 30 mil soldados robôs.

Além da IA aplicada nos drones e em outros dispositivos robóticos, uma das subáreas que merece destaque é o "Deep Learning". Essa tecnologia pode desempenhar várias funções importantes em

uma estratégia de segurança cibernética. Um dos casos de uso inclui a detecção automática de intrusão com uma taxa de descoberta excepcional.

Outras das tecnologias que ganharam grande apelo nos dias atuais são a Realidade Virtual e a Realidade Aumentada. A Realidade Virtual (VR – Virtual Reality) se preocupa com a criação de um ambiente simulado do mundo físico com o auxílio de tecnologia computacional, enquanto a Realidade Aumentada (AR – Augmented Reality) conecta um ambiente virtual ao ambiente físico por meio de objetos virtuais criados por computador.

Na Suécia, simulações em Realidade Virtual estão sendo utilizadas para auxiliar militares a lidar da melhor maneira com civis em locais de conflito. Dessa forma, os soldados podem se adaptar melhor às diferentes realidades em que são expostos quando liderados por órgãos internacionais, como a Organização das Nações Unidas (ONU).

No Brasil, o Primeiro Grupo de Artilharia Antiaérea de Autodefesa (1.º GAAAD) utiliza Realidade Aumentada no treinamento de militares que defendem pontos sensíveis. O ambiente de treinamento conta com um lançador de mísseis, que o atirador que está sendo treinado posiciona sobre o ombro, e com uma tela, onde se pode observar o céu à procura de aeronaves ou mísseis inimigos. O cenário ainda conta com efeitos sonoros aos quais o atirador tem que ficar atento.

Até a "Blockchain", um livro-razão compartilhado e imutável usado para registrar transações ordenadas no tempo em um sistema distribuído e sem confiança nos nós da rede, ganhou seu lugar no cenário de tecnologias emergentes que vêm sendo utilizadas nos meios militares, para autenticação na manipulação de dados sensíveis distribuídos.

Diante de todas essas novas tecnologias e de outras que irão ainda surgir, é necessário lembrar que os vários sistemas que as utilizam possuem um ciclo de vida, no qual a inovação é o motor para a produção de nova geração de sistemas de defesa.

Nesse contexto, se fazem cada vez mais importantes a adoção do conceito da hélice da inovação, com a articulação da sociedade, empresa, academia e governo para incentivar e fortalecer o processo colaborativo da inovação que é dinâmico e, devido a seu ineditismo, apresenta risco de não obter os resultados almejados de forma imediata.

O Governo Brasileiro tem estabelecido mecanismo de Encomenda Tecnológica (ETEC) contido no Decreto 9.283/2018, para fomentar a geração da economia do conhecimento, a partir de aquisição de soluções onde existem riscos tecnológicos dos resultados. As ETEC são, portanto, uma ferramenta importante para que os investimentos em pesquisa e desenvolvimento sejam direcionados com maior segurança jurídica, o que certamente contribuirá para a obtenção de mais capacidade de atualização tecnológica em contexto, civil e militar, no qual a demanda por inovações cresce de forma nunca vista em nossa história. T&D

N. da R.: Delfim Ossamu Miyamaru é diretor-presidente da Fundação Ezute.