FUTURO
INTERNET DAS COISAS A BORDO

Capitão de Corveta **GEIZON** DE ALMEIDA **GOMES**
Chefe do Departamento de Instrução e Adestramento - CAAML
Aperfeiçoado em Eletrônica

"Chegará o dia em que surgirá o conflito baseado em rede, onde as informações não estarão alojadas em cada plataforma, mas sim disponíveis a todos na rede. Tanto os veículos de combate, como os de apoio logístico e mesmo os Centros de Comando e Controle farão 'downloads' das informações da rede e 'uploads' daquilo que tiver coletado para usufruto das demais unidades. E tudo acontecendo em tempo real. É claro que esta realidade está um pouco distante, uns 10 ou 20 anos a frente talvez, mas ela virá com abrangência global e para uma infinidade de atividades, não apenas militares"

(ZEIDAN, Revista Passadiço, Ed. 22, 2002, p.28-31)

FOTO: US Navy

O texto em destaque pertence a um artigo da edição da Revista Passadiço, expedida há quase duas décadas, no qual seu autor tem uma visão de futuro baseada na Integração de Sistemas (IS) dos diversos meios de guerra em uma única rede de informações. De forma tácita, pode-se perceber nesse texto a conceituação para um dos termos que, atualmente, encontra-se em voga quando o assunto em pauta é tecnologia: a "internet das coisas", também referenciada como IoT, do acrônimo em inglês de *Internet of Things*.

Quando a Internet surgiu, ela poderia ser simplesmente entendida como uma rede de computadores. Porém, com o passar do tempo, outros tipos de dispositivos com a capacidade de se conectar foram sendo criados e essa rede se expandiu. Desse modo, naturalmente, a internet passou a interligar todos os tipos de coisas, nos levando ao conceito da internet das coisas, como o próprio nome sugere.

Dispositivos de IoT, hoje, já são usados para diversas aplicações comerciais, tais como segurança doméstica, dispositivos de saúde, produção em indústrias, rastreamento de cargas, veículos autônomos, etc. Além disso, cada vez mais, surgem aparatos tecnológicos que, sem que percebamos, nos conectam a uma enorme rede de dados por meio de *smartphones* ou de dispositivos "vestíveis" (*wearables*), como *smartwatches* ou *smartbands*.

Como um evidente exemplo de que já nos encontramos imersos na IoT, podemos citar os monitores *fitness* que registram as atividades diárias de um número cada vez maior de pessoas e as auxiliam a atingir suas metas de condicionamento físico, tornando-as mais saudáveis. Outras tecnologias, que prometem tornar as viagens mais seguras e rápidas utilizando carros autônomos e sensores de estrada que detectam e se adaptam às condições das vias em tempo real, já não mais se encontram no campo da abstração e se tornaram realidade.

E a IoT somente se tornou possível graças aos avanços tecnológicos, principalmente nos últimos anos, com destaque para quatro áreas: 1° - a redução dos custos dos sensores e atuadores; 2° - o crescimento das redes sem fio e de "endereços livres" de internet, com a oficialização e popularização do protocolo IPv6; 3° - os ganhos em poder de processamento e armazenamento, como na tecnologia de "computação nas nuvens" (*cloud computing*); e 4° - a criação de novos métodos analíticos avançados, dentre os quais podemos incluir a inteligência artificial (IA).

NOVOS CONCEITOS

A internet das coisas possui uma imensa gama de aplicações militares, podendo conectar navios, aviões, carros de combate, drones, soldados e bases operacionais em uma rede lógica, aumentando a consciência situacional, a avaliação de riscos e o tempo de resposta às possíveis ameaças. Para tanto, outra expressão surge: *Internet of Military Things* (IoMT), que poderia ser definida como a internet das coisas voltadas para as Forças Armadas ou, simplesmente, a IoT de Defesa.

Na indústria naval, "navios inteligentes" (*smart ships*) já são construídos para usufruirem da internet das coisas, nos levando à concepção da Internet dos Navios ou *Internet of Ships* (IoS). De uma maneira geral, a IoS se utiliza de um conjunto de informações compartilhadas e gerenciadas por sistemas preparados para lidar com grandes volumes de dados processados e que incorporam as tendências tecnológicas emergentes que estão sendo adaptadas ao ambiente marítimo.

A IoS também é apresentada como uma solução comercial capaz de detectar quando um componente de um navio está se aproximando de sua vida útil e deve ser substituído ou quando a corrosão de uma chapa atingiu um certo limite, por exemplo. E todas essas informações podem ser apresentadas facilmente em um aplicativo de *smartphone*, com a antecedência suficiente para evitar manutenções imprevistas ou riscos desnecessários à segurança das tripulações.

POSSIBILIDADES

A tecnologia pode estar presente praticamente em todas as tarefas realizadas pela Marinha, desde a manutenção de equipamentos à melhoria da precisão dos armamentos. Portanto, a incorporação de dispositivos e sensores de IoT pode ter diversos efeitos positivos, aumentando a eficiência e reduzindo os custos. Os dispositivos e serviços da IoT podem coletar dados cada vez mais complexos e analisá-los mais rapidamente; fazer maior uso de automação; reduzir o erro humano; fornecer capacidades militares mais precisas e eficientes e reduzir custos de pessoal.

FOTO: U.S. Air Force - J.M. Eddins Jr.

A tecnologia empregada em carros autônomos pode ser adaptada para ser utilizada, a título de exemplo, para o auxílio à navegação e atracação dos navios. Um sensível aumento da segurança no tráfego marítimo pode ser obtido a partir de sistemas mais precisos que monitorem o fluxo e possam evitar abalroamentos ou, no caso de colisões inevitáveis, alertem as tripulações dos meios envolvidos de modo a permitir o início das ações com a maior antecedência possível.

Outra aplicação pode ser verificada nas Marinhas dos EUA, da Rússia e da República Popular da China que já desenvolvem navios não-tripulados – *Unmanned Surface Vessels* (USV) –, verdadeiros "drones navais" com a tecnologia IoT embarcada e que possuem capacidade de cumprir tanto tarefas antiaéreas, como antissubmarino.

A IoT pode se traduzir, também, numa inovação nos processos de auxílio à tomada de decisão dos Comandantes, não somente no nível tático, mas também nos níveis operacionais e estratégico. Por exemplo, ter dispositivos de internet das coisas distribuídos pelos meios de um Grupo Tarefa (GT), produzindo imensas quantidades de dados que poderão ser convertidos em informações por um sistema de IA, poderão se tornar diferenciais na capacidade analítica de uma situação pelos decisores.

OBSTÁCULOS E DESAFIOS

Alguns pontos merecem atenção quando há a intenção de se adotar a tecnologia de internet das coisas para um ambiente militar. Problemas de padronização, segurança e privacidade persistem como verdadeiros obstáculos a serem transpostos e requerem o desenvolvimento de soluções. Além disso, a conexão de dispositivos inteligentes deverá, em última instância, sempre ser controlada por pessoas, limitando o nível de autonomia de tais sistemas a bordo.

Para que a IoT possa ser amplamente adotada, diversas questões técnicas importantes precisam ser levadas em consideração, tais como infraestrutura necessária e custos envolvidos. Outro desafio é a necessidade de elaborar padrões comuns, principalmente se houver a intenção de uma futura integração entre a IoT das três Forças Armadas, a fim de utilizar a referida tecnologia em uma atuação conjunta e/ou combinada. Atualmente, vários padrões estão sendo desenvolvidos pelas empresas, mas a padronização e a interoperabilidade no meio militar devem ser tratadas com a devida importância, pois uma das maiores vantagens da tecnologia IoT para as Forças Armadas estaria na possibilidade de conectar muitos dispositivos diferentes e usar o *Big Data* por eles gerado em prol da missão.

Embora as tecnologias de IoT ofereçam economias a longo prazo, os grandes custos iniciais de aquisição são um considerável empecilho. Além disso, os processos de obtenção de produtos destinados à área militar são normalmente caracterizados pela inegável necessidade da manutenção do sigilo reservado dos projetos no decorrer de sua elaboração, algo que vai de encontro à cultura do setor privado. Empresas de tecnologia privadas também estão menos dispostas a trabalhar com artefatos de defesa em razão da limitação dos direitos de propriedade intelectual e dos rígidos controles habitualmente impostos sobre os equipamentos.

Além disso, à medida que nos tornamos mais dependentes desses dispositivos conectados, garantir sua disponibilidade também pode ser crítico. Redes sensíveis e que venham a controlar sistemas vitais, não poderão falhar nem por um segundo. E se o fizerem, deverão ser capazes de se autorrecuperar rapidamente. Assim sendo, indispensavelmente, redes alternativas e sistemas distribuídos serão compulsórios para a obtenção de um nível ideal de confiança em tais ferramentas.

RISCOS

As novas funcionalidades e recursos que a IoT concederá também poderão trazer uma série de novos riscos na área da segurança cibernética. A possibilidade de *hackers* invadirem e passarem a controlar um sistema de armas de um navio de superfície seria algo inimaginável até há pouco tempo, porém, no presente, é um ponto que deve ser revestido de seriedade ao tratarmos de riscos inerentes à tecnologia IoT.

Dispositivos de IoT, quando aplicados no âmbito da Defesa, podem constituir riscos significativos de segurança, especialmente no que tange às guerras eletrônica e cibernética. Conforme os dispositivos são implantados e aplicativos de IoT são utilizados, o número de pontos de vulnerabilidade para os invasores virtuais aumenta. Ameaças internas e erros dos usuários também passam a ser motivos de preocupação. Podemos, ainda, somar o fato de que a maioria das tecnologias IoT dependem da comunicação sem fio via rádio frequências e que, portanto, bloqueios de sinal ou indiscrições poderão ocorrer.

Não se pode, ainda, subestimar o risco de que invasores possam disseminar desinformações nas redes utilizadas ou interromper processos e operações dos componentes de IoT por meio de ataques cibernéticos. Por isso, é realmente importante que os dados gerados e divulgados pelos sistemas de IoT possuam elevada proteção contra acesso não autorizado.

Além de algoritmos de criptografia próprios da Força, a utilização de camadas de permissões de acesso se farão necessárias a fim de permiti-lo apenas aos militares que possuam a necessidade de conhecer.

CONCLUSÃO

A despeito dos problemas e dificuldades listados, se a tecnologia IoT atingir a sua maturidade e corresponder a todo o seu potencial, ela transformará todos os aspectos de nossas vidas diárias.

Como um dos principais componentes da Indústria 4.0 – como está sendo chamada a Quarta Revolução Industrial –, a Internet das Coisas enfrenta oportunidades históricas em seu desenvolvimento e na sua aplicação na Indústria de Defesa. O emprego da IoT no campo militar já se mostra como um requisito inevitável para que Forças Armadas atinjam o "estado da arte".

Para tanto, procedimentos aceitáveis de mitigação dos riscos envolvidos na utilização da tecnologia deverão ser implementados e aprovados. Do mesmo modo, um conjunto de padrões e práticas deverão ser definidos, não somente no âmbito de nossa Marinha, mas, também, em parceria com as demais Forças coirmãs, a fim de que os dispositivos de IoT possam ser utilizados, mantendo-se um elevado nível de segurança da estrutura do sistema e de proteção dos dados gerados.

Em última análise, as possibilidades de aplicação dos serviços de IoT a bordo estão limitadas apenas pela imaginação humana e, decisivamente, a vantagem nos conflitos tenderá para as instituições que melhor souberem explorar as suas capacidades e garantirem a sua segurança.

Referências:

BREEDEN II, J. **The Army and Navy are still mapping how to bring more internet of things devices into combat domains**. 2018. Disponível em: <https://www.nextgov.com/ideas/2018/05/internet-things-role-battlefields-and-sea/147877/>. Acesso em: 17 abr. 2019.

NIST, D. D. *"Cybersecuring" the internet of things*. 2017. Disponível em: <https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=9147>. Acesso em: 20 fev. 2019.

SULLIVAN, S. **Naval Internet of Things (IoT) effectiveness and efficiency**. 2018. Disponível em: <https://www.navysbir.com/n18_A/N18A-T027.htm>. Acesso em: 12 fev. 2019.

WORTH, D. **Royal Navy to use AI and IoT during major cyber warfare exercise**. 2017. Disponível em: <https://www.theinquirer.net/inquirer/news/3004766/royal-navy-to-use-ai-and-iot-during-major-cyber-warfare-exercise-next-month>. Acesso em: 07 mar. 2019.

_____. **The Internet of Ships**: a new design for smart ships. 2017. Disponível em: <https://www.rina.org.uk/The_Internet_of_Ships_a_new_design_for_Smart_Ships.html>. Acesso em: 17 abr. 2019.