Internet das Coisas

Projeto Sementes de Futuro em Defesa

Vol. 2 Nº 19

EXPEDIENTE

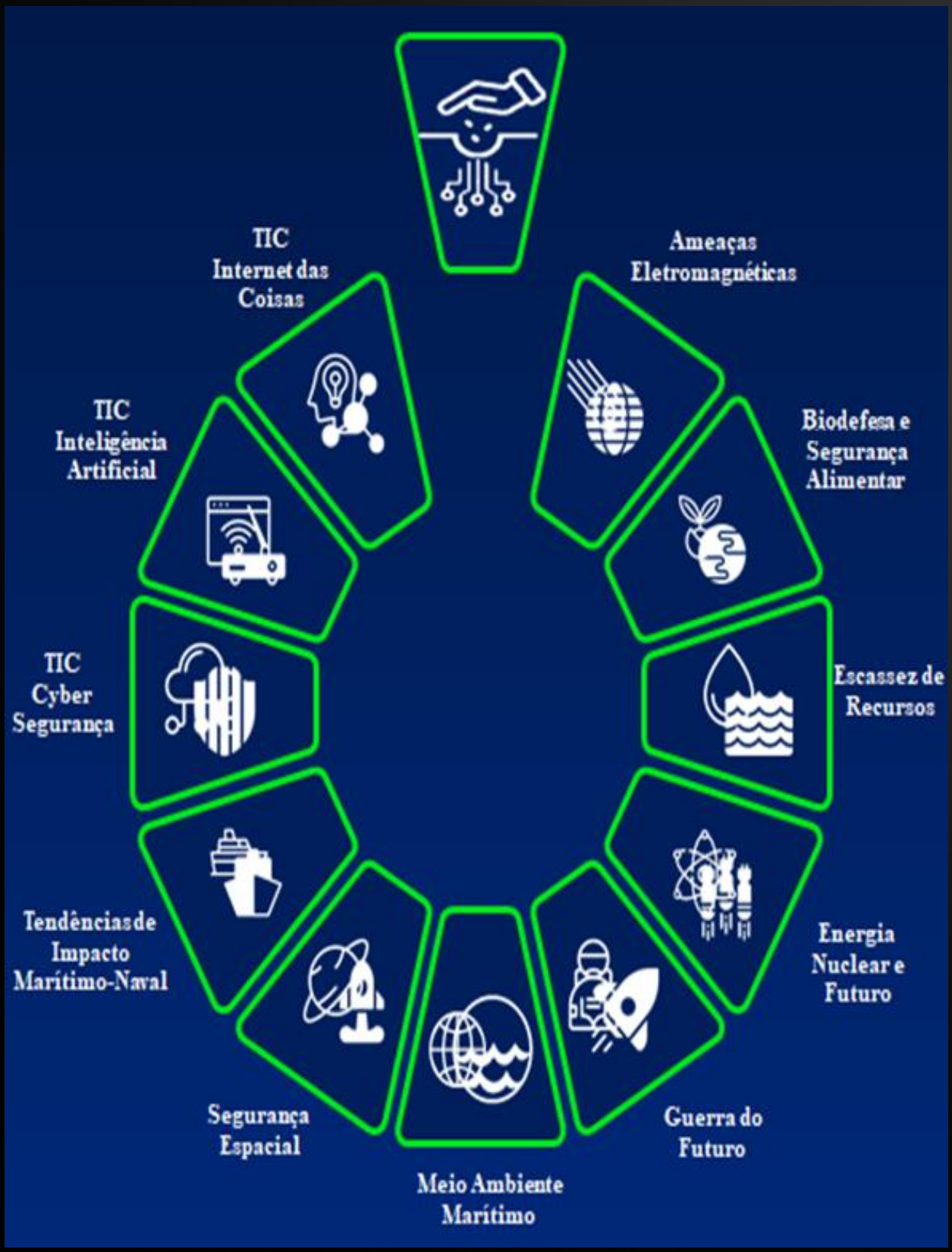
O Projeto Sementes de Futuro em Defesa faz parte do Programa de Cooperação Acadêmica em Defesa Nacional (PROCAD-DEFESA) “Prospectiva para Segurança e Defesa”, projeto da CAPES e do Ministério da Defesa (MD) liderado pela Escola de Guerra Naval (EGN) com 10 outras IES, Instituições e Empresas, para formar uma rede colaborativa de pesquisa e monitoramento de sementes do ambiente futuro, apoiada em plataforma computacional, análise multicritério, com abrangência nacional, participação social pública e privada, civil e militar para acompanhamento dos cenários prospectivos do Ministério da Defesa e uso dual.

O Sementes de Futuro em Defesa é um produto digital e semanal desenvolvido pelos pesquisadores das Linhas de Pesquisa Cenários Prospectivos de Segurança e Defesa do Laboratório de Simulações e Cenários (LSC) da EGN, cuja divulgação visa estimular e disseminar sementes de futuro para temas estratégicos sobre defesa e segurança, subsidiando análises prospectivas altamente qualificadas para auxiliar as Forças Armadas brasileiras no desenvolvimento de estratégias de longo prazo. As matérias deste informativo não representam o posicionamento institucional de qualquer setor das Forças Armadas.

Acompanhe-nos nas Redes Sociais

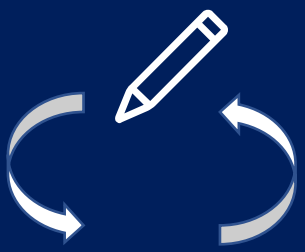
Laboratório de Simulações e Cenários
Linha de Pesquisa Cenários Prospectivos para Segurança e Defesa
Avenida Pasteur, 480 – Urca, Rio de Janeiro – RJ – Brasil – CEP: 22290-240

PROCAD DEFESA
PROSPECTIVA
PDPROSPECTIVA


TIC
Internet das
Coisas
Ameaças
Eletromagnéticas
TIC
Inteligência
Artificial
Biodefesa e
Segurança
Alimentar
TIC
Cyber
Segurança
Escassez de
Recursos
Tendências de
Impacto
Marítimo-Naval
Energia
Nuclear e
Futuro
Segurança
Espacial
Guerra do
Futuro
Meio Ambiente
Marítimo

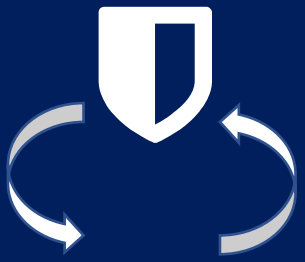
TENDÊNCIA DE PESO	**São eventos cuja direção e sentido são suficientemente consolidados para que se possa admitir sua continuidade no futuro; retratam processos cujo rompimento requer um esforço hercúleo e improvável de apresentar resultados. (LIMA; CURADO, 2017, pp. 16-17)**
FATO PRÉ-DETERMINADO	**São eventos já conhecidos, cuja ocorrência é praticamente certa. No geral, as indicações resultantes não se efetivaram ainda, mas se sabe que o evento irá ocorrer no futuro. (LIMA; CURADO, 2017, p. 17)**
FATO PORTADOR DE FUTURO	**São sinais existentes no ambiente, ínfimos por sua dimensão presente, mas imensos por suas consequências e potencialidades futuras. (MARCIAL, GRUMBACH, 2014, p. 240)**
INCERTEZA CRÍTICA	**São eventos mais incertos e de maior importância à cenarização; tratam-se das variáveis que determinarão a lógica e a ideia-força dos cenários, portanto, suas mudanças críticas possibilitam múltiplos futuros possíveis. (LIMA; CURADO, 2017, p. 17)**
SURPRESA INEVITÁVEL	**São forças previsíveis, pois têm suas raízes em forças que já estão em operação neste momento; entretanto, não se sabe quando irão se configurar, quais suas consequências previsíveis e como afetarão. (MARCIAL, GRUMBACH, 2014, p. 244)**
CORINGAS (WILD CARDS)	**Referem-se a grandes surpresas possuidoras de baixa probabilidade de ocorrência e extremamente difíceis de serem antecipadas; se consolidadas, possuem grande impacto e se materializam rapidamente. (LIMA; CURADO, 2017, p. 18)**
PRINCIPAIS ATORES E SUAS ESTRATÉGIAS	**Indivíduos, grupos ou organizações que influenciam ou recebem influência significativa do sistema; o ator desempenha importante papel, influenciando o comportamento das variáveis com objetivo de viabilizar seus projetos. (MARCIAL, GRUMBACH, 2014, p. 238)**

DATA E FONTE

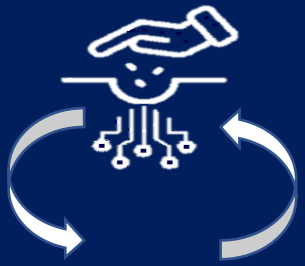


AUTOR

DESCRIÇÃO



IMPACTOS FUTUROS
EM DEFESA



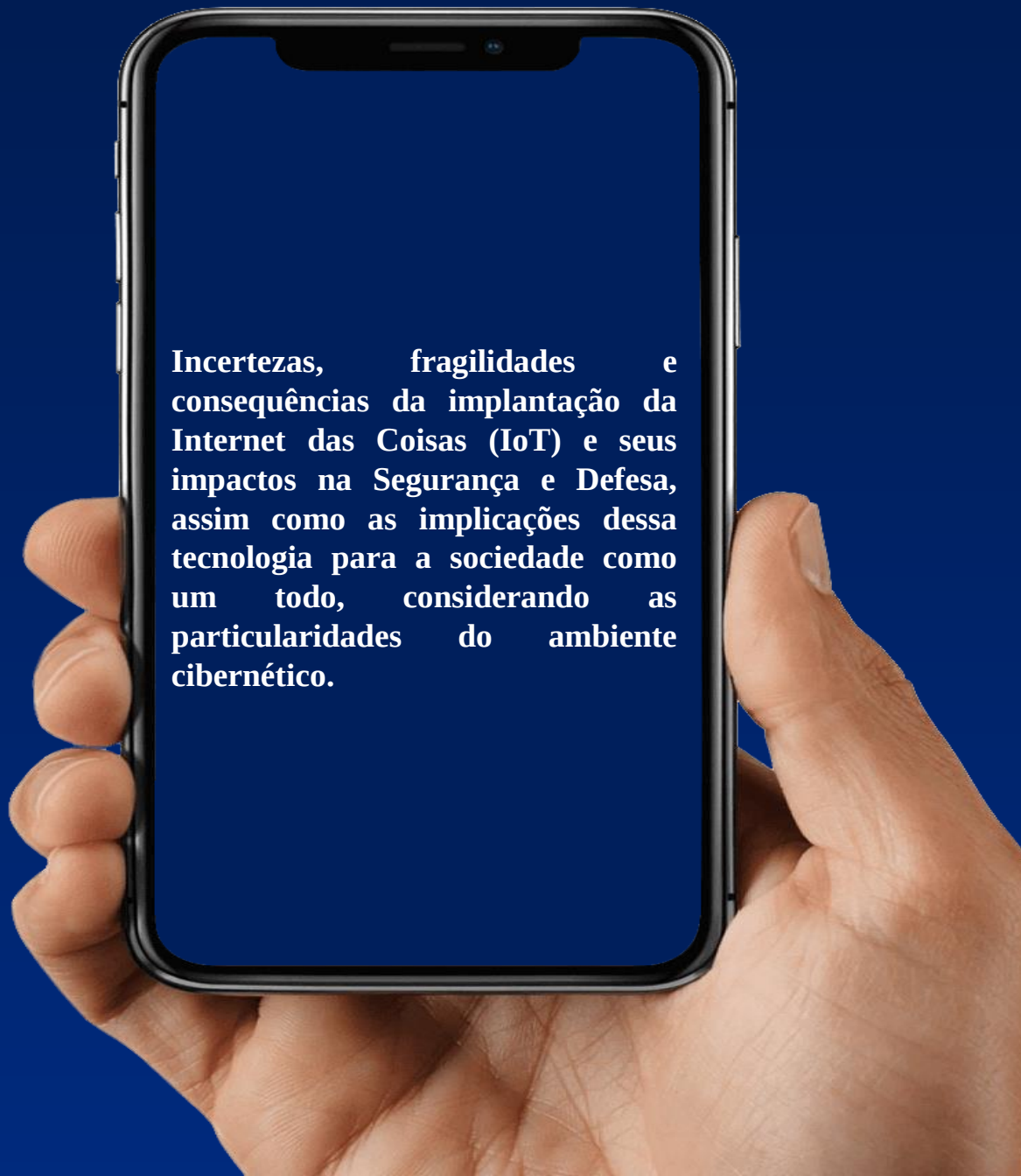
SEMENTES DE FUTURO
EM DEFESA

PALAVRAS-CHAVE

LINK DE ACESSO

PESQUISADOR DO LSC

TIC Internet das Coisas



CONECTIVIDADE VIA SATÉLITE AIS SE DESENVOLVE COM A INCLUSÃO DA IOT NO SISTEMA

22/03/2017 – The Maritime Executive

Redação

A evolução da tecnologia de monitoramento e rastreamento de embarcações tem aproveitado a conectividade via satélite *AIS* (Sistema de Identificação Automática), *IoT* (Internet das Coisas) e *Big Data* para permitir níveis sem precedentes de visibilidade e controle no futuro do comércio e cadeias de fornecimento oceânicos globais inteligentes. Inicialmente, o *AIS* foi previsto como um sistema de curto alcance e identificação de alta intensidade para evitar colisões entre embarcações e controle no rastreamento. Com a evolução do sistema, a vigilância e segurança dos navios começaram a ser monitoradas via satélites, onde entidades comerciais e governos tem acesso a dados no combate à pirataria, monitoramento ambiental e fiscalização da pesca.

A aplicação de *Data Analytics* e *IoT* no comércio marítimo internacional possibilita que empresas e órgãos fiscalizadores possuam acesso a dados complexos para monitoramento de contêineres, commodities e outros bens em transporte marítimo em tempo real. Tal fato eleva a previsibilidade logística das cadeias de fornecimento. O impacto dessa tendência permitirá a redução de atividades suspeitas no transporte marítimo, bem como a construção de planos de ação a partir da análise dos dados coletados. Com a análise dos dados possibilitados pelo *AIS*, *IoT* e *Big Data*, é possível identificar recorrências e reduzir o tempo de detecção das ameaças, prevendo um melhor preparo de fiscalização e ação protetiva dos órgãos responsáveis no Brasil.

Fato Pré-Determinado

Sistema de Identificação Automática; sistema de curto alcance; monitoramento; fiscalização.

https://www.maritime-executive.com/editorials/ais-meets-iot

Marcelo Andrade de Barros – Pós-graduado em Gestão da Tecnologia da Informação e Comunicação (UCAM)
Monah Marins – Mestre em Estudos Marítimos (PPGEM/EGN)

NAVIOS DE CARGA REMOTAMENTE CONTROLADOS EVOLUEM COM IOT

23/06/2017 – Linkedin

Maximilian Immo Orm Gorissen

Entre as várias vertentes e áreas de aplicação da *IoT* (Internet das Coisas), a navegação autônoma de navios de carga é uma área com diversos testes pelo mundo. Ao se referir a um navio autônomo compreende-se um navio "remotamente" comandado por uma equipe em terra. Entretanto, há diversos desafios e questões na legislação que precisam avançar visto que, pelo navio não ser tripulado, não há cumprimento de regramentos tais como as regras da tripulação a bordo, como tratamento de esgoto, banheiros, cabines, comida, médicos, salva-vidas, entre outros. Outro ponto é a incapacidade de oferecer assistência de emergência a náufragos e a possibilidade de ingresso de passageiros clandestinos. Para o navio se tornar realmente autônomo muitos avanços terão que ser cumpridos.

Os avanços tecnológicos aplicados nas embarcações oferecem potencialidades e controversas, principalmente por envolver questões de responsabilidade civil que o Direito do Mar (1982) e outras Convenções não previam em seus artigos. A possibilidade de falhas de navegação, riscos de acidentes e incidentes envolvendo embarcações, bem como o descumprimento das normas internacionais e/ou ataques cibernéticos aos sensores de direcionamento são algumas das questões que limitam a aplicabilidade destas embarcações em larga escala. Esta é uma tendência de um novo momento na indústria marítima e, além do debate e a aplicação de uma jurisdição ser necessária, o investimento em novas tecnologias não pode ser tratado como um desafio para o Brasil.

Tendência de Peso

Navios autônomos; IoT; empregos do futuro.

https://www.linkedin.com/pulse/iot-os-navios-de-carga-aut%C3%B4nomos-sua-evolu%C3%A7%C3%A3o-e-gorissen/?trk=related_artice_IoT%20%E2%80%93%20Os%20Navios%20de%20carga%20aut%C3%B4nomos%2C%20sua%20evolu%C3%A7%C3%A3o%20e%20consequ%C3%AAncias._article-card_title

Marcelo Andrade de Barros – Pós-graduado em Gestão da Tecnologia da Informação e Comunicação (UCAM)
Monah Marins – Mestre em Estudos Marítimos (PPGEM/EGN)

APLICAÇÕES DE IA E IOT APRESENTAM DUALIDADE PARA A SEGURANÇA DOS ESTADOS

21/06/2022 – Wired

Alexa O’Brien

A comunidade de inteligência dos EUA lançou iniciativas para debater e conceituar o uso e aplicação da IA (Inteligência Artificial) e de *IOT* (Internet das Coisas) sobre como a tecnologia tem sido desfragmentada e utilizada estrategicamente por Estados rivais, como a China. O pedido para criação de um “ecossistema digital de IA” na Lei de Autorização de Inteligência de 2022 (*Intelligence Authorization Act*) aponta o receio da comunidade de inteligência norte americana com a evolução do “*machine learning*” aplicado a coleta e consolidação em massa de dados dos dados de tráfego global da WEB.

Um dos desafios do uso de IA e *IoT* no contexto governamental pode ser a cobertura de alvos de coleta e a subsequente identificação destes como ameaças. Com a IA, por meio da *IoT*, é possível realizar análises complexas sobre *Big Data* ou mesmo produzir raciocínios complexos e argumentos lógicos sobre determinada situação e área avaliada. Em termos de segurança nacional, a capacidade de monitoramento de áreas nacionais, possibilitadas pelo código aberto, chama atenção para as atividades e os usos de IA e de como os Estados podem intervir – ou não – na interpretação destes dados em seus territórios.

Principais Atores e suas Estratégias

IoT; cybersegurança; machine learning; Estados nacionais; segurança.

https://www.wired.com/story/ai-machine-learning-us-intelligence-community/

Monah Marins P. Carneiro – Mestre em Estudos Marítimos (PPGEM/EGN)

EMPRESA MARÍTIMA UTILIZA SENSORES IOT NOS MOTORES PARA MANUTENÇÃO PREVENTIVA

22/06/2022 – DCiber

Redação

A empresa Caterpillar Marine está instalando diversos sensores *IoT* (Internet das Coisas) nos motores dos navios para receber preventivamente informações sobre defeitos que podem prejudicar o funcionamento das embarcações. Todos os dados coletados pelos mais de 5 mil sensores passam por uma análise do sistema *OSIsoft* e, caso seja identificado um problema, os sensores propõem uma possível solução. Com essa ação a manutenção pode ser feita sem parar o navio, economizando recursos financeiros e beneficiando o trânsito marítimo.

Com a utilização de sensores para manutenção preventiva, as embarcações podem reduzir os riscos e incertezas de problemas técnicos em alto-mar ou portos, além de reduzir os custos financeiros da embarcação inativa. De acordo com o *ICC International Maritime Bureau* (IMB), que monitora atividades de pirataria ao redor do mundo, mais de 195 incidentes envolvendo atos de pirataria foram reportados por embarcações em 2020. Com o uso de sensores *IoT* nos motores das embarcações, estratégias de percursos e rotas – mesmo em espaços marítimos instáveis – reduzem as incertezas do trânsito marítimo e possibilitam uma comunicação ágil entre embarcações, portos e IMB.

Tendência de Peso

IoT; sensores; segurança marítima.

https://dciber.org/iot-caterpillar-marine-evita-que-motores-de-navios-precisem-parar-para-manutencao/

Marcelo Andrade de Barros – Pós-graduado em Gestão da Tecnologia da Informação e Comunicação (UCAM)

EUA INTERROMPEM BOTNET RUSSA QUE HACKEOU MILHÕES DE DISPOSITIVOS

20/06/2022 – Zdnet

Liam Tung

Em maio de 2022, o Departamento de Justiça dos EUA (*DoJ*) desmantelou a infraestrutura de uma *botnet* russa que consistia em milhões de dispositivos hackeados de *IoT* (Internet das Coisas). A *Botnet* oferecia dispositivos de IP invadidos no lugar de endereços de IP legítimos, com isso, realizava ataques de credenciais em páginas da *web* de *login*, como e-mails coorporativos, entre outros acessos. Segundo o *DoJ*, as vítimas foram universidades, indivíduos e empresas. Há uma tendência na aplicação de *IoT* em diversos setores, sendo o uso da nuvem uma das mudanças estratégicas para impulsionar o crescimento de plataformas de nuvem *IoT*. Com o aumento desse mercado, a segurança dos usuários finais tem sido um debate crescente na aplicação e desenvolvimento de *IoT*.

Com a utilização e inclusão da *IoT* em diversas áreas da vida humana, a utilização de sistemas seguros e confiáveis torna-se essencial para que usuários finais – civis e militares – possam compartilhar dados com proteção de ponta-a-ponta. Compreender a infraestrutura conectada e como ela se reflete na área de trabalho (*workplace*) é um compromisso que usuários e instituições brasileiras precisam garantir para a segurança cibernética, uma vez que sistemas e ambientes de Tecnologia da Inofrmação (TI) podem aumentar o escopo de crimes.

Tendência de Peso

IoT; Cybersegurança; serviços de nuvem; Estados Unidos; Rússia.

https://www.zdnet.com/article/us-disrupts-russian-botnet-that-hacked-millions-of-devices/

Monah Marins P. Carneiro – Mestre em Estudos Marítimos (PPGEM/EGN)
Gabriella Nichols – Mestre em Estudos Marítimos (PPGEM/EGN)

SEMENTES DE FUTURO EM DEFESA

Sinalizar o futuro para defender o presente