



Projeto Sementes de Futuro em Defesa

TIC Internet das Coisas – Vol. 3, N° 9



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.

Coordenação

Dr. Bernardo Salgado Rodrigues (LSC/EGN)

Conselho Editorial e Científico

Dr. Bernardo Salgado Rodrigues (LSC/EGN)

Dr. Claudio Rodrigues Corrêa (LSC/EGN)

Doutoranda Valdenize Pereira Oliveira (PPGEM/EGN)

MSc. José Ribeiro Sampaio de Menezes (FND/UFRJ)

Gestão de Tecnologia da Informação e Infraestrutura de Rede

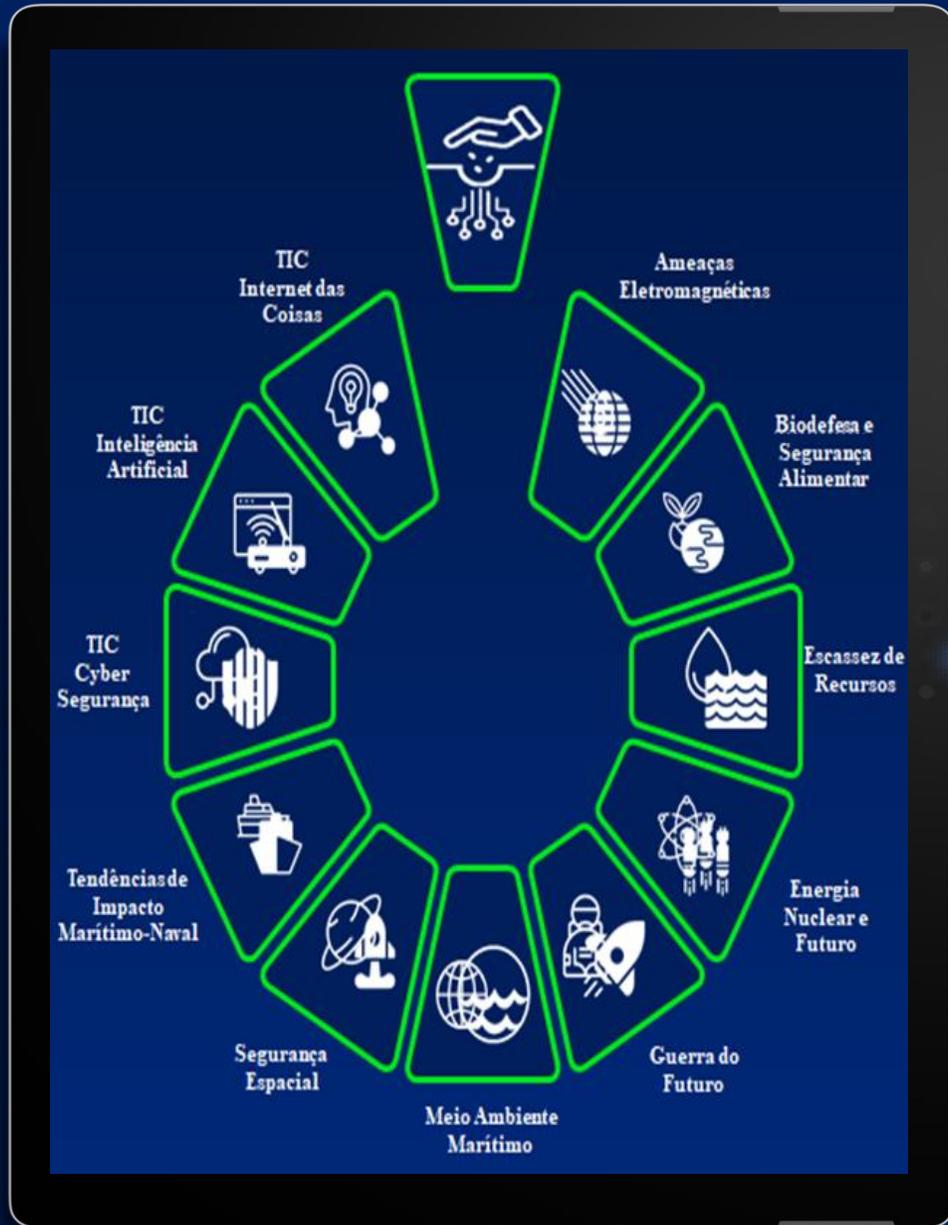
Esther Cesar Augusto da Silva (LSC/EGN)

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





Linhas de Pesquisa

Sementes de Futuro em Defesa



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

Legendas

TIC Internet das Coisas

Incertezas, fragilidades e consequências da implantação da Internet das Coisas (IoT) e seus impactos na Segurança e Defesa, assim como as implicações dessa tecnologia para a sociedade como um todo, considerando as particularidades do ambiente cibernético.



PROJETO DE IOT REFORÇA INTERESSE EM DESENVOLVIMENTO DE TECNOLOGIA PRÓPRIA PELOS ESTADOS EUROPEUS



09/03/2023 – Press Release Capgemini



Florence Lievre



A IoT (Internet das Coisas) foi identificada pela Comissão Europeia como uma das tecnologias que está na vanguarda da transformação econômica e que pode gerar impactos tanto em pessoas quanto em instituições. Por meio do Programa de Investigação e Inovação chamado European Union's 2023 – Projeto IoT-NGIN, que reúne indústrias e institutos de pesquisa científica, o programa contará com o investimento de 8 milhões de euros até setembro de 2023. O objetivo da União Europeia (UE) com este projeto é alavancar tecnologias e empresas que apoiem soluções e inovações na indústria, assim como os “valores europeus”, a fim de criar uma base de IoT interoperável a nível europeu para garantir a segurança de dados de objetos conectados.



O debate sobre IoT e Inteligência Artificial (IA) envolvem o questionamento entre as práticas e a ausência de regulamentações no desenvolvimento e aplicação da tecnologia, seja no meio civil ou militar. Os avanços em IoT e IA, bem como a “corrida” para o desenvolvimento de softwares e hardwares próprios, tem alertado para o alargamento do “gap” tecnológico entre os Estados, bem como a preocupação com a cyberssegurança de seus cidadãos e cidades conectadas. Investimentos em projetos de grande porte, como este da União Europeia, pode ser um sinal de reajustes no desenvolvimento das capacidades e implementações de soluções de engenharia de dados para além do espaço unicamente empresarial, inclusive no Brasil.



Principais Atores e suas Estratégias



IoT; cyberssegurança; política; União Europeia.



https://prod.ucwe.capgemini.com/wp-content/uploads/2023/04/2023_04_05_Capgemini_IoT-next-generation_European-Commission_near-final.pdf



Monah M P Carneiro – Mestre em Estudos Marítimos (PPGEM/EGN) e Analyst Relations na Stefanini Group

IOT APRESENTA POTENCIAL PARA EFICIÊNCIA ENERGÉTICA EM GESTÃO DE RECURSOS MILITARES



26/04/2023 – Defesa em Foco



Redação



A implementação de tecnologias da Internet das Coisas (IoT) nas instalações militares vem apresentando potencial para aumentar a eficiência energética e melhorar a gestão de recursos. A IoT possibilita o monitoramento em tempo real do consumo de energia, gerenciamento de recursos hídricos, manutenção preditiva e aprimoramento da segurança e vigilância. Algoritmos de aprendizado de máquina e sensores inteligentes permitem otimizar o uso de energia, identificar vazamentos, prever manutenção e monitorar atividades, contribuindo para operações militares mais sustentáveis e eficientes.



A adoção de tecnologias IoT no setor de defesa promoverá maior sustentabilidade, redução de custos e melhoria na segurança. A eficiência energética e a gestão de recursos aprimoradas permitirão operações militares mais eficazes e resilientes que podem ser incorporadas no contexto brasileiro. A manutenção preditiva e a vigilância aprimorada garantirão a prontidão operacional e a prevenção de falhas inesperadas, proporcionando vantagens estratégicas e táticas no cenário de defesa global.



Tendência de Peso



IoT; ESG; eficiência energética; gestão de recursos.



<https://www.defesaemfoco.com.br/aumento-da-eficiencia-energetica-em-instalacoes-militares-com-iot/>



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





METAVERSO PODE APOIAR A EVOLUÇÃO DE TREINAMENTOS DE OPERAÇÕES MILITARES E DE OPERAÇÕES DE PAZ



30/04/2023 – Exército Brasileiro



Redação



A III Conferência de Chefes de Polícia das Nações Unidas (UNCOPS), realizada de agosto a setembro de 2022, e que contou com a participação do Exército Brasileiro através do Comando de Operações Terrestres (COTER), deu destaque ao emprego de novas tecnologias para a preparação da Polícia das Nações Unidas (UNPOL). Uma delas é a construção de cenários virtuais para treinamento através do metaverso, além das capacidades e mentalidades requeridas para superar os gargalos do emprego policial nas missões de campo. A Conferência teve por finalidades avaliar o emprego da UNPOL em Missões de Paz, os resultados obtidos através das ações Action for Peacekeeping (A4P) e Action for Peacekeeping Plus (A4P+), assim como apresentar metas futuras para o incremento da participação policial.



Os sistemas de treinamento virtuais e simuladores, amplamente utilizados pelas forças militares ao redor do mundo, deverão ser impactados positivamente com a implementação de metaverso e mundos virtuais cada vez mais realistas. A aposta está na utilização de meios ultrarrealistas seguros para incremento da capacidade de resposta em campo e tomada de decisões mais assertivas. A adoção de tecnologias imersivas pelas Forças Armadas e Forças de Paz pode aumentar consideravelmente os resultados esperados nos treinamentos para combate.



Tendência de Peso



IoT; metaverso; treinamento, ONU.



<http://www.coter.eb.mil.br/index.php/noticias-do-coter/2505-coter-participa-da-3-uncops>



Gabriella Nichols – Mestre em Estudos Marítimos (PPGEM/EGN)



IOT APRESENTA DESAFIOS ÉTICOS E LEGAIS EM OPERAÇÕES MILITARES E DE INTELIGÊNCIA



25/04/2023 – DCiber.org



Redação



A crescente adoção de tecnologias da Internet das Coisas (IoT) em operações militares e de inteligência traz consigo preocupações éticas e implicações legais. Questões relacionadas à privacidade, autonomia, responsabilidade, segurança cibernética e conformidade com o Direito Internacional Humanitário devem ser abordadas. É fundamental estabelecer controle, regulamentação e diretrizes claras para o uso responsável da IoT nessas operações, envolvendo legisladores, especialistas em ética e tecnologia, e outros interessados.



Ao enfrentar proativamente os desafios éticos e legais da IoT, as Forças Armadas e agências de inteligência podem garantir a segurança e o bem-estar dos cidadãos e adaptar-se às mudanças tecnológicas. Políticas e regulamentações sólidas permitirão o aproveitamento do potencial da IoT para melhorar a eficiência e eficácia das operações, ao mesmo tempo em que se promove a cooperação internacional e o compartilhamento de informações para estabelecer normas globais e melhores práticas.



Principais Atores e suas Estratégias



IoT; privacidade; autonomia; segurança cibernética; ética.



<https://dciber.org/desafios-eticos-e-legais-do-uso-de-iot-em-operacoes-militares-e-de-inteligencia/>



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





“GEMÊOS DIGITAIS” SÃO UTILIZADOS PARA TESTAR PLANOS DE BATALHAS



31/08/2022 – InnovationAus.com



Justin Hendry



O Departamento de Defesa australiano está construindo um “Gemêo Digital – Digital Twin” para permitir que os comandantes testem rapidamente planos de batalha para elevar o comando e controle do ADF (Command and Control (C2) of the Australian Defense Force). Por meio do desenvolvimento de uma série de sub-sistemas de integração para aprimorar os recursos de planejamento e execução, denominado de Phoebe, o projeto conta com a liderança do Grupo de Ciência e Tecnologia de Defesa da Austrália (DSTG) que utilizará os recursos para integrar “jogos de guerra, modelagem, simulação e arquitetura ágil”. O intuito é para que os planejadores usem o Phoebe para planejar digitalmente um pacote de ataque envolvendo guerra eletrônica e os efeitos desta envolvendo mortes em massa, assim como possibilitar que os tomadores de decisão possam verificar se os planos logísticos e operacionais são eficazes em futuras operações.



O uso da tecnologia “Gemêo Digital – Digital Twin” combina IoT (Internet das Coisas) e IA (Inteligência Artificial) para representar um ou mais objetos físicos no formato digital com a finalidade de apoiar processos e tomadas de decisão por meio da antecipação dos acontecimentos. O desenvolvimento e avanço da tecnologia pode acrescentar uma ferramenta a mais às Escolas Militares para capacitar seu corpo militar. Testar com segurança e em maior número estratégias e táticas em ambientes virtuais contribui com a redução de custos e implementações de planos com maior eficácia.



Surpresa Inevitável



IoT; cibersegurança; inovação; digital twin; Departamento de Defesa da Austrália.



<https://www.innovationaus.com/defence-prototypes-digital-twin-to-test-battle-plans/>



Monah M P Carneiro. – Mestre em Estudos Marítimos (PPGEM/EGN) e Analyst Relations na Stefanini Group.



Sementes de Futuro em Defesa

Sinalizar o futuro para defender o presente



 facebook.com/people/Sementes-de-Futuro-em-Defesa/100076353903885/

 instagram.com/sementesdefuturoemdefesa

 linkedin.com/company/sementes-de-futuro-em-defesa/about/