Laboratório de Segurança Cibernética de Sistemas Ciberfísicos do IME - LaSC/IME

Workshop on Trustworthy Artificial Intelligence and Cyber-Physical Systems

"O emprego da Inteligência Artificial na Cibersegurança"

12 AGO 2024

Laboratório de Segurança Cibernética de Sistemas Ciberfísicos do IME - LaSC/IME

Inteligência Artificial e Cibersegurança de Infraestruturas Críticas no Laboratório de Segurança Cibernética de Sistemas Ciberfísicos do IME (LaSC/IME)

Sumário

- O que é Cibersegurança?
- O que é Inteligência Artificial?
- O que são Infraestruturas Críticas?
- O Laboratório de Segurança Cibernética de Sistemas Ciberfísicos do IME - LaSC/IME
  - Infraestrutura
  - Pesquisas e Projetos
- Conclusão

O que é Cibersegurança?

- Cibersegurança é o conjunto de práticas, tecnologias, procedimentos e políticas projetados para proteger sistemas, redes, dispositivos e dados contra ataques cibernéticos. Esses ataques podem visar a comprometer a confidencialidade, integridade e disponibilidade das informações, representando uma ameaça para organizações, governos e indivíduos.

O que é Inteligência Artificial?

- Inteligência Artificial (IA) refere-se à capacidade das máquinas de imitar e realizar tarefas que normalmente exigiriam inteligência humana. Essas máquinas são programadas para aprender com dados, reconhecer padrões, fazer inferências e tomar decisões com base nesses dados, de forma semelhante ao raciocínio humano.

O que são Infraestruturas Críticas?

- Infraestruturas Críticas referem-se a sistemas, instalações e serviços essenciais para o funcionamento seguro, eficiente e contínuo de uma sociedade ou economia. Essas infraestruturas desempenham um papel fundamental no suporte às necessidades básicas e ao bem-estar das pessoas, bem como no funcionamento de outras organizações e setores.
  - Energia
  - Água e Saneamento
  - Transporte
  - Comunicações
  - Saúde

O Laboratório de Segurança Cibernética de Sistemas Ciberfísicos do IME - LaSC/IME

Cibersegurança + Infraestruturas Críticas + Supercomputação + Inteligência Artificial

Workshop on Trustworthy Artificial Intelligence and Cyber-Physical Systems

Antecedentes

1ª Reunião DCT-ITAIPU-PTI

Parcerias Potenciais Levantadas

Junto à ITAIPU:

- estágios de curta duração para alunos do IME na ITAIPU
- cooperação no processo de atualização tecnológica dos equipamentos e sistemas da Usina
- pesquisa em geração de hidrogênio
- pesquisa em sistemas elétricos de propulsão
- pesquisas em fontes alternativas de energia

Junto ao PTI-BR

- instalação de Escritório do DCT
- intercâmbio acadêmico de professores e estudantes: Segurança de Barragens
- pesquisas em fontes alternativas de energia
- desenvolvimento em tecnologia da informação com base em SW livre
- intercâmbio na área de segurança da informação e de informações geográficas
- acompanhamento da situação geopolítica na tríplice fronteira

2006

Antecedentes

Acordo de cooperação em P&D – FPTI - EB/DCT

DOU Nº 144, de 29 de julho de 2008

NOTIME — 25 de julho de 2008

O DCT ASSINA PROTOCOLO DE INTENÇÕES COM A FUNDAÇÃO PARQUE TECNOLÓGICO ITAIPU

No dia 25 de julho, uma comitiva do Departamento de Ciência e Tecnologia, chefiada pelo Vice-Chefe, Gen Div Renato Joaquim Ferrarezi, e integrada também pelo Comandante do IME e representantes da Assessoria 3 do DCT, deslocou-se para a cidade de Foz do Iguaçu – PR com a finalidade de participar do evento de assinatura do protocolo de intenções com a Fundação Parque Tecnológico Itaipu – FPTI. A cerimônia contou com a presença do Sr. Juan Carlos Sotuyo, Diretor Superintendente da FPTI, e do Prof Alcibíades Luiz Orlando, Reitor da Universidade Estadual do Oeste do Paraná (UNIOESTE), além de outros integrantes daquela Fundação.

O instrumento firmado tem por objeto a cooperação e a execução de atividades de interesse comum nas áreas técnica, científica e acadêmica, bem como o compartilhamento de infra-estrutura de laboratórios e outras

instalações físicas e equipamentos. Identificados vários temas como de interesse comum, o IME e a FPTI já deram início a projetos nas áreas de Segurança de Barragens, *Data Mining*, Robótica, Automação e Simulação de Sistemas Elétricos, Estabilidade de Sistemas Elétricos de Potência, Veículo Elétrico, Comando e Controle, Intercâmbio de Alunos e Pesquisadores e Incubadora de Empresas. Nesta fase inicial de definição, os projetos estão sendo coordenados por meio de reuniões por videoconferência.

Trata-se, sem dúvida, de mais uma parceria que fortalece o ensino e a pesquisa no IME, ao ampliar o intercâmbio e os instrumentos de geração de novos conhecimentos para o Exército e o País.

Antecedentes

Acordo de cooperação em P&D – FPTI - EB/DCT

Desenvolvimento de novo método de ensaio de campo para avaliar a efetividade de Estabilizadores de Sistemas de Potência (PSSs)

- Avaliação da efetividade de PSSs: ensaio em malha fechada inferência sobre a malha aberta;
- Ensaio aplicado à malha de tensão de 2 geradores inferência sobre o comportamento dinâmico do conjunto de geradores: modos de oscilação eletromecânicos (agregado e intraplanta) da usina.
- Aprimoramento do método de ensaio pela aplicação de sinais de sondagem do tipo multissenos para levantamento da resposta em frequência;
- Redução do tempo de duração dos ensaios e melhores resultados decorrentes da pouca alteração nas condições operativas durante a sua realização.

1º Ensaio – Itaipu 60Hz – 13/09/2008

2º Ensaio – Itaipu 50Hz – 26/09/2010

3º Ensaio – Itaipu 60Hz – 07/05/2011

4º Ensaio – Itaipu 50Hz – 19/05/2019

- Avaliação do comportamento em malha aberta dos modos intraplanta;
- Validação, em decorrência dos resultados do primeiro teste, do banco de dados do Sistema Interligado Nacional e dos *software* de análise e simulação do CEPEL.
- Consolidação do método de ensaio da malha de tensão de usinas de grande porte com múltiplos geradores utilizando sinais de sondagem multissenos;
- Levantamento de dados mais atuais para futuro ajuste de PSS com nova estrutura e maior grau de liberdade.

Antecedentes

IECFOZ 2013
1º Seminário sobre Proteção de Infraestruturas Críticas

2006 **2008** **2013**

ITAIPU propõe Ceape[2]

ITAIPU BINACIONAL

Publicado em *ITAIPU BINACIONAL* (http://www.itaipu.gov.br)

Início > Itaipu propõe centro de proteção de estruturas estratégicas

Itaipu propõe centro de proteção de estruturas estratégicas

Por *romeu*
Criado em *29/08/2013 - 17:13*
Data:
29/08/2013 (All day)
Hora:
16:12

Foz do Iguaçu, no Paraná, poderá abrigar o primeiro Centro de Estudos Avançados em Proteção de Infraestruturas Críticas da região Sul do País. A ideia é que o centro ofereça serviços que envolvam inteligência, desenvolvimento de metodologias e certificações, além de um laboratório de segurança eletrônica, de comunicações e cibernética.

A proposta foi apresentada nesta quinta-feira (29), no Parque Tecnológico Itaipu (PTI), pelo assessor de Informações da Diretoria Geral Brasileira da Itaipu Binacional, coronel Carlos Roberto Sucha, durante o 1º Seminário sobre Proteção e Infraestruturas Críticas (IEC Foz 2013).

Um protocolo de intenções para a criação do centro foi assinado pelo diretor-geral brasileiro de Itaipu, Jorge Samek; pelo diretor do Departamento de Segurança de Informações e Comunicações do Gabinete de Segurança Institucional da Presidência da República, Raphael Mandarino Jr.; pelo comandante do Centro de Defesa Cibernética do Exército, José Carlos dos Santos; e pelo gerente do Sistema Integrado de Proteção de Estruturas Estratégicas Terrestres (Proteger), José Fernando Iasbech – entre outras autoridades.

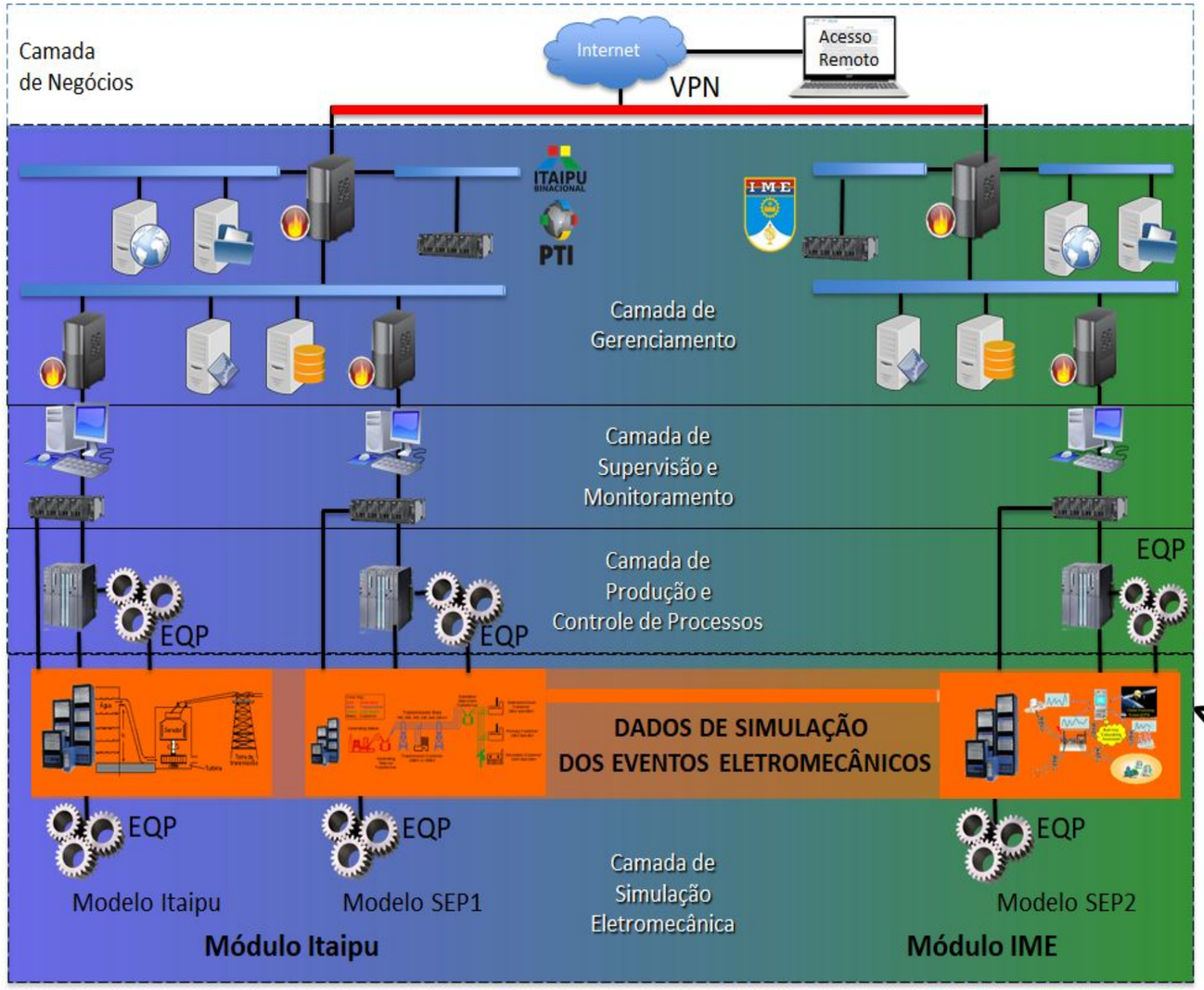
Workshop on Trustworthy Artificial Intelligence and Cyber-Physical Systems

Simulação *Hardware-In-The-Loop* em tempo real de Sistemas Ciberfísicos

Infraestrutura corporativa e interface com rede de TA virtualizada

Equipamentos de automação

RTDS - Simulação de sistemas elétricos em tempo real



Simula ciber ataques

Testa a proteção das redes

Treina Administradores dos Sistemas

Analisa o comportamento de equipamentos e aplicativos (PLC, IoT, SCADA etc.)

PTI
Parque Tecnológico Itaipu

ITAIPU BINACIONAL

R$ 3,5 milhões

R$ 0,9 milhões

DCT

I-M-E

Workshop on Trustworthy Artificial Intelligence and Cyber-Physical Systems

Lab Computação Alto Desempenho Def Ciber – IA – LaSC – MecatrIME

Simulações
Dados e informações realistas – *big data*

INTELIGÊNCIA ARTIFICIAL

- INTELIGÊNCIA ARTIFICIAL
- ANÁLISE DE DADOS
- CLOUD COMPUTING
- TOMADA DE DECISÃO
- BIG DATA
- HPC

2022 – 2024

DEFESA CIBERNÉTICA

LABORATÓRIO DE ALTO DESEMPENHO

SUPERCOMPUTADOR

CRAY

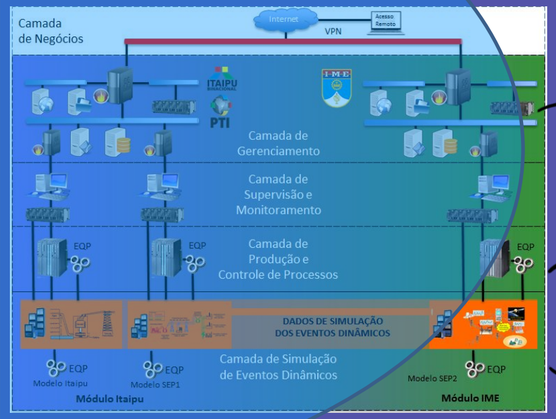
2013 - 2024

INTEGRAÇÃO

SEGURANÇA CIBERNÉTICA DE SISTEMAS CIBERFÍSICOS

INFRAESTRUTURAS CRÍTICAS – SEP

RTDS



2022 - 2026

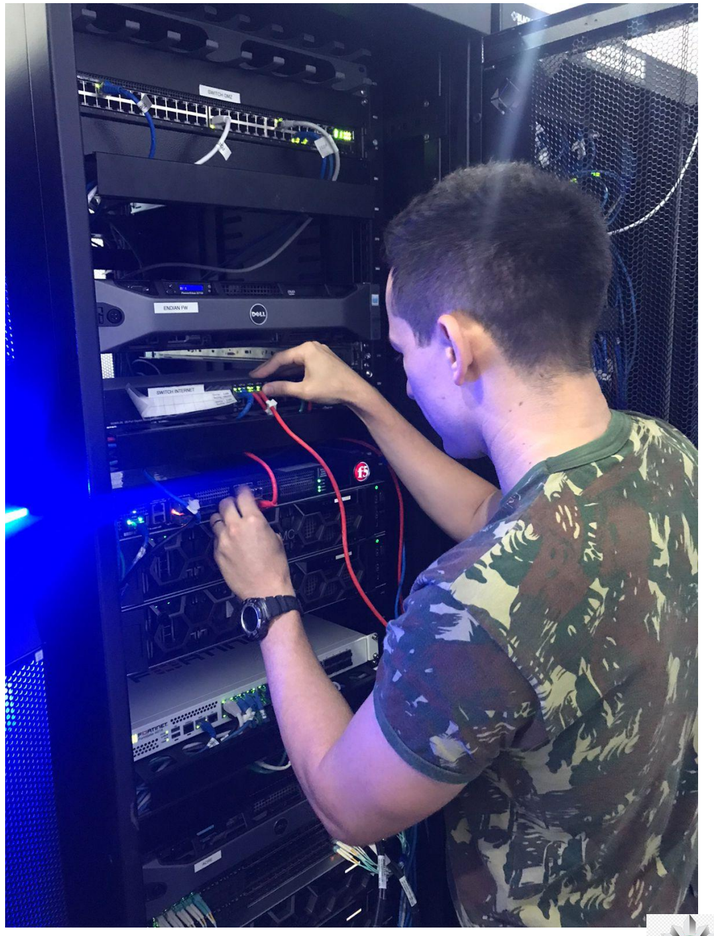

Testa a proteção das redes


Treina Administradores dos Sistemas


Analisa o comportamento de equipamentos e aplicativos (PLC, IoT, SCADA etc.)

FINANCIAMENTO:

Apoio direto do IME aos projetos do Programa Estratégico do Exército Defesa Cibernética

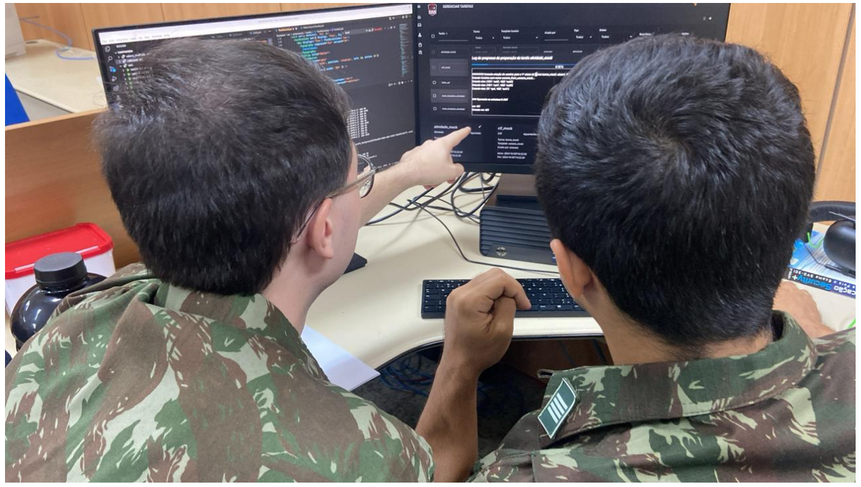
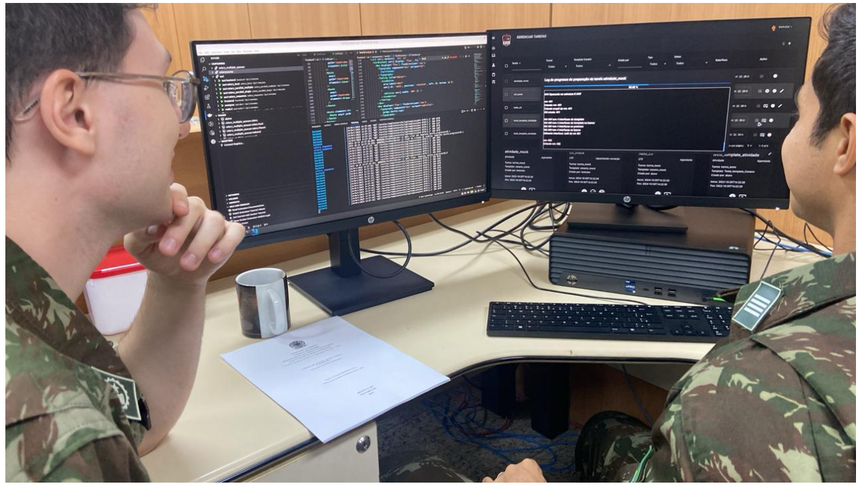


Apoio direto do IME aos projetos do Programa Estratégico do Exército Defesa Cibernética

Apoio direto do IME aos projetos do Programa Estratégico do Exército
Defesa Cibernética

Apoio direto do IME aos projetos do Programa Estratégico do Exército Defesa Cibernética



Workshop on Trustworthy Artificial Intelligence and Cyber-Physical Systems

Pesquisas e Projetos

- ✔ **Apoio direto aos projetos do Programa Estratégico do Exército Defesa Cibernética**
- ✔ **Participação no Exercício Guardião Cibernético**
- ✔ **Pesquisas em andamento:**
  - **Desenvolvimento de Cyber Range multipropósito para infraestruturas críticas múltiplas: plantas elétricas, sistemas rádio (rádios militares, 5G)**
  - **IA aplicada à Cybersecurity:**
    - **Intrusion Detection System e Firewall (IDS-MPC)**
    - **Gerador Sintético de Tráfego de Rede (tráfego de fundo e tráfego malicioso)**

Visão de futuro do LaSC

- ✔ **Se tornar um centro de referência em Cibersegurança para Infraestruturas Críticas a nível internacional**

Workshop on Trustworthy Artificial Intelligence and Cyber-Physical Systems

OLHAR DIGITAL NOTÍCIAS VÍDEOS FICHAS TÉCNICAS DICAS E TUTORIAIS EDITORIAS OF

Olhar Digital > Veículos e Tecnologia > Como os drones com IA podem mudar (ainda mais) as guerras?

VEÍCULOS E TECNOLOGIA

Como os drones com IA podem mudar (ainda mais) as guerras?

Os drones já estão sendo utilizados nas guerras, mas o avanço da inteligência artificial pode tornar essas armas ainda mais eficazes

Por **Alessandro Di Lorenzo**, editado por **Bruno Capozzi** | 15/03/2024 12h28

THE NEW YORK TIMES • TECNOLOGIA • RÚSSIA

Inteligência artificial e Guerra da Ucrânia iniciam era dos robôs assassinos; veja vídeo

Guerra da Ucrânia acelera busca por tecnologia mais mortífera enquanto país vira Vale do Silício para armas

F DÊ UM CONTEÚDO

Workshop on Trustworthy Artificial Intelligence and Cyber-Physical Systems

Workshop on Trustworthy Artificial Intelligence and Cyber-Physical Systems

'Robôs assassinos': Ucrânia aposta em armas movidas por inteligência artificial para ganhar vantagem na guerra contra a Rússia

Pressão para superar o inimigo, juntamente com grandes fluxos de investimento, doações e contratos governamentais, transformou o país em um Vale do Silício para drones autônomos e outras armamentos

Por Paul Mozur e Adam Satariano, Em The New York Times — Kiev

03/07/2024 04h30 · Atualizado há uma semana

Workshop on Trustworthy Artificial Intelligence and Cyber-Physical Systems

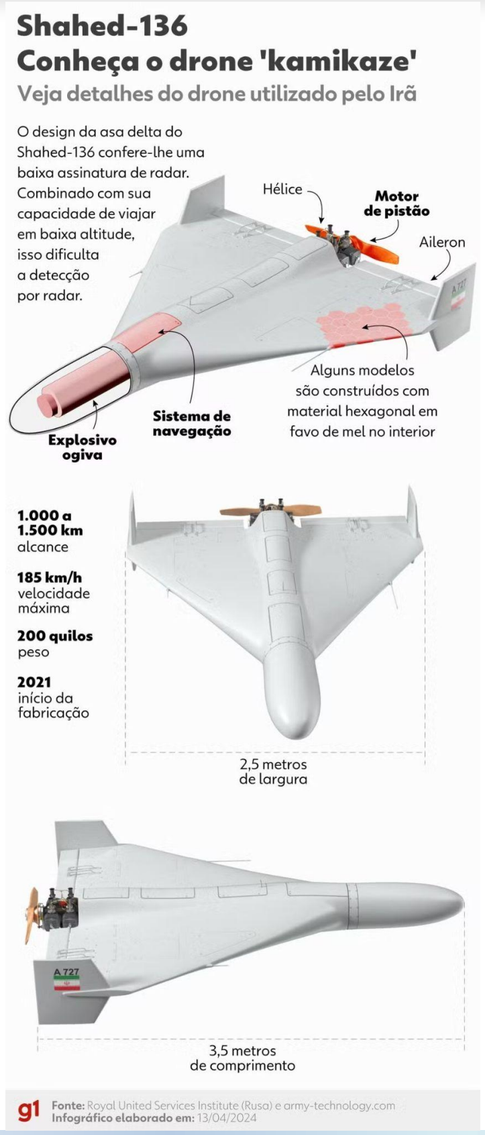
Workshop on Trustworthy Artificial Intelligence and Cyber-Physical Systems

Oleksandr Yabchanka, à esquerda, comandante dos Lobos da Vinci, um batalhão conhecido por sua inovação em armamentos, em um estande de tiros perto de Kiev; Yabchanka postou um pedido aberto no Facebook para uma metralhadora informatizada e controlada remotamente SASHA MASLOV/NYT

Workshop on Trustworthy Artificial Intelligence and Cyber-Physical Systems

F-35 Lighting II (Lockheed Martin, F-35 Joint Strike Fighter)

- Custo planejado do desenvolvimento: US$ 59 Bi
- Custo atual do desenvolvimento, construção e mnt: US$ 400 Bi
- Custo unitário de produção: US$ 100 Mi
- Tempo entre concepção e primeiro vôo: 10 anos



Shahed-136 (Irã)

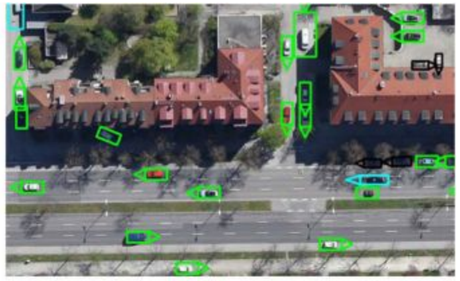
- Custo unitário de produção: US$ 20 Mil
- Tempo entre concepção e primeiro vôo: 2 anos

Novas Capacidades de Atuação do IME

Inteligência Artificial Aplicada a Enxame de Drones e Robótica Móvel

robolME

(a)



(b)


GUERRA CIBERNÉTICA QUÂNTICA
APLICAÇÕES DE COMPUTAÇÃO QUÂNTICA
COMUNICAÇÃO QUÂNTICA
RADAR QUÂNTICO
COMPUTADOR QUÂNTICO
INTERNET QUÂNTICA
DETECÇÃO DE MAGNETOMETRIA QUÂNTICA
GUERRA QUÂNTICA
NAVEGAÇÃO INERCIAL QUÂNTICA
MAPEAMENTO SUBTERRÂNEO QUÂNTICO
DETECÇÕES QUÍMICAS QUÂNTICAS
GUERRA ELETRÔNICA QUÂNTICA
GUERRA SUBAQUÁTICA QUÂNTICA
RADAR QUÂNTICO
NAVEGAÇÃO INERCIAL QUÂNTICA
MAPEAMENTO SUBAQUÁTICO QUÂNTICO
COMUNICAÇÃO QUÂNTICA


APLICAÇÕES CIVIS
SEGURANÇA
INTELIGÊNCIA ARTIFICIAL QUÂNTICA
LOGÍSTICA PARA EMERGÊNCIAS
OTIMIZAÇÃO DE SISTEMAS FINANCEIROS
ESTUDO DE SISTEMAS COMPLEXOS
DESENVOLVIMENTO DE MODELOS CLIMÁTICOS
MEDICINA PERSONALIZADA E BIOMEDICINA
OBTENÇÃO DE NOVOS FÁRMACOS

Outras Áreas de Atuação do IME

Tecnologias QUÂNTICAS

Mecânica Quântica

- Proposta por Max Planck em 1900
- Propriedades físicas de partículas atômicas e subatômicas
- Incerteza, Emaranhamento e Superposição

Emprego em hardware

- Ressonância magnética
- Fibra óptica
- Transistor

Inovações no século XX

- Exames médicos além da radiografia
- Comunicação em grandes distâncias com alta velocidade e banda de transmissão
- Microcomputação

Novas Capacidades de Atuação do IME

Tecnologias QUÂNTICAS

Tecnologias quânticas no séc. XXI	
COMPUTAÇÃO QUÂNTICA	• Quebra do algoritmo RSA • Algoritmos pós-quânticos (*Quantum Resistant*)
COMUNICAÇÃO QUÂNTICA	• QKD (*Quantum Key Distribution*) • Criptografia Quântica - detecção de intrusão
SENSORES QUÂNTICOS	• Ressonância magnética • Detecção de objetos • Relógios atômicos (GPS de satélites)

Novas Capacidades de Atuação do IME

Tecnologias QUÂNTICAS

Pesquisas no IME

- **Criptografia** - Algoritmos resistentes à quântica
- **Computação Quântica** - Algoritmos de otimização e busca
- **Computador Quântico** - *hardware*

- **Comunicações Quânticas** - compartilhamento de fótons emaranhados; troca de chaves quântica (QKD), criptografia quântica

PROJETO REDE HERMES QUÂNTICA

- **Sensoriamento Quântico** - Detecção de elementos Químicos Biológicos e Radiológicos no ambiente

Parceria IDQBRN

Novas Capacidades de Atuação do IME

Tecnologias QUÂNTICAS

Em que podemos contribuir?

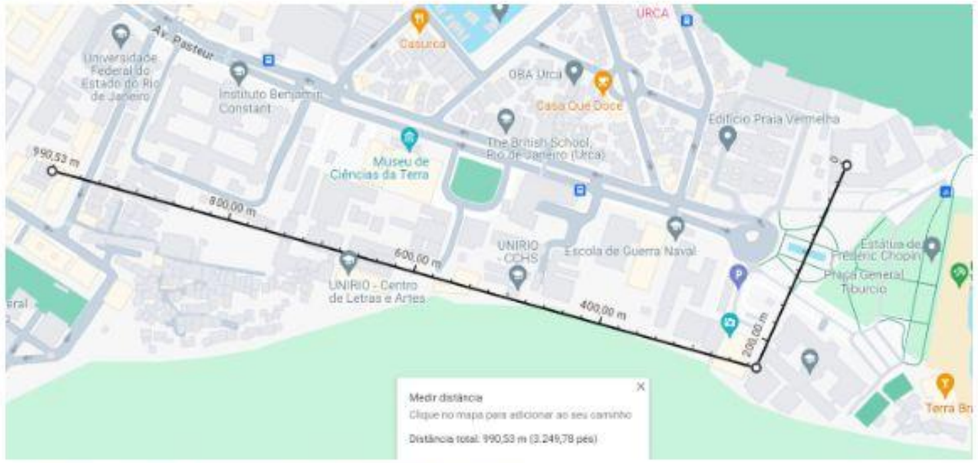
1. **Segurança cibernética:**
   - Migração para Criptografia QR
2. **Segurança cibernética:**
   - Comunicações seguras com estruturas *offsite*
3. **Problemas de otimização:**
   - Nas áreas de manutenção, operação e engenharia

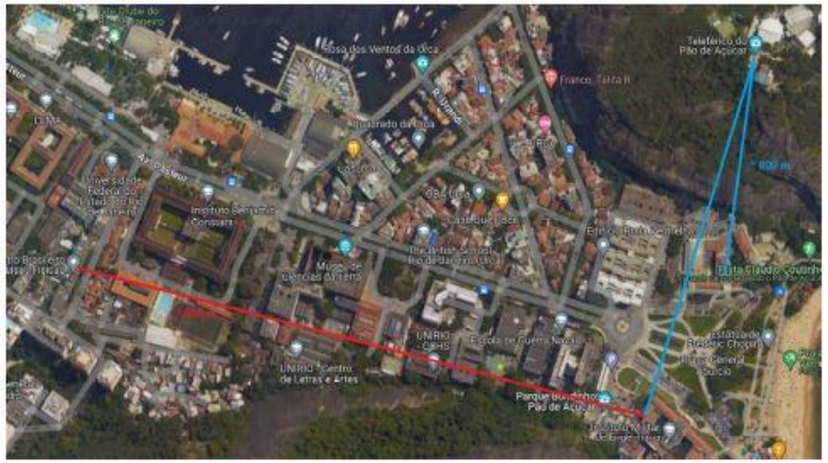
Projeto Rede Hermes Quântica

Estruturado em três fases







President Biden Limits Key Technology Exports, including Quantum Computing

"[...] The order, issued by President Biden, identifies China, Hong Kong, and Macau as countries of concern. It proposes a **new program to protect technologies critical to military innovation, including semiconductors, quantum information technologies, and artificial intelligence**. The Treasury is inviting public input to help shape the program, which will not change the U.S.'s open investment climate but will **target investments in highly sensitive technologies**.

"The Biden Administration is committed to keeping America safe and defending America's national security through appropriately protecting technologies that are critical to the next generation of military innovation."

Obrigado e estamos abertos para perguntas

- ✔ Cel QEM Clayton Escouper das Chagas - Eng. Comp. e Eng. Tele. - Professor do IME
- ✔ escouper@ime.eb.br
- ✔ Arquiteto e *Tech Lead* do LaSC