



Comando Naval de Operações Especiais



Defesa Cibernética: uma visão naval

CA (FN) Eduardo – 20 de julho de 2022



Objetivo



Fomentar o interesse e provocar a discussão sobre o tema “Ameaças Cibernéticas”; e apresentar ações em curso na Marinha do Brasil.



Roteiro



- Introdução
- Espaço Cibernético e suas Ameaças
- Estrutura Cibernética na MB
- Sistema Dreadnought
- Operações Cibernéticas na MB
- Projetos e Desafios
- Considerações Finais



Introdução



16SET2019

**Ativação do
CoNavOpEsp**



Missão



**Comandar ou
Compor**

- FT OpEsp e FT GCiber
- Singular, Combinada ou Conjunta

Planejar e Coordenar

- Participação da MB
- Operações, adestramentos e exercícios conjuntos de OpEsp, OpInfo, AGE, AGA e AGCiber

Assessorar

- CON e os setores da MB
- Aspectos de OpEsp, OpInfo, AGE, AGA, AGCiber e Ameaças Híbridas

Conduzir

- AGCiber no âmbito da MB

**A fim de contribuir
para**

- Aprestamento e emprego de Forças Navais, Aeronavais e de Fuzileiros Navais



Roteiro



- Introdução
- Espaço Cibernético e suas Ameaças
- Estrutura Cibernética na MB
- Sistema Dreadnought
- Operações Cibernéticas na MB
- Projetos e Desafios
- Considerações Finais



Espaço Cibernético



Sem limite físico



Alcance global



Difícil identificação



Incerteza da segurança



Facilidade de acesso



Ameaças Cibernéticas



Crime



Guerra Cibernética



Espionagem



Hacktivism



Terrorismo

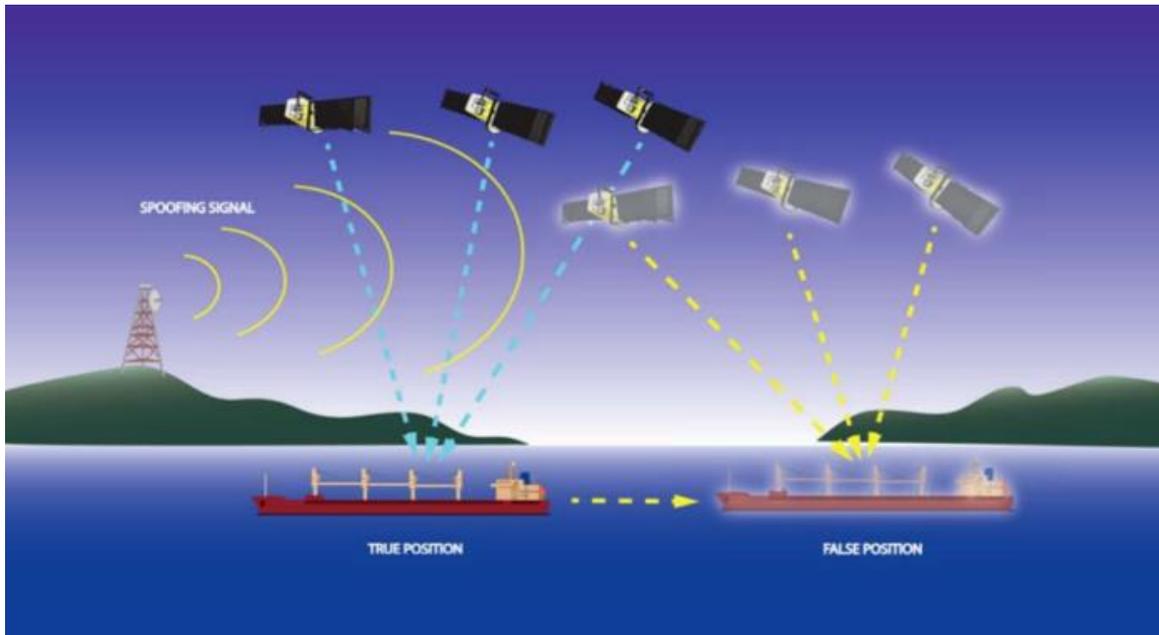


Exemplos de Ameaças Cibernéticas





GPS Spoofing



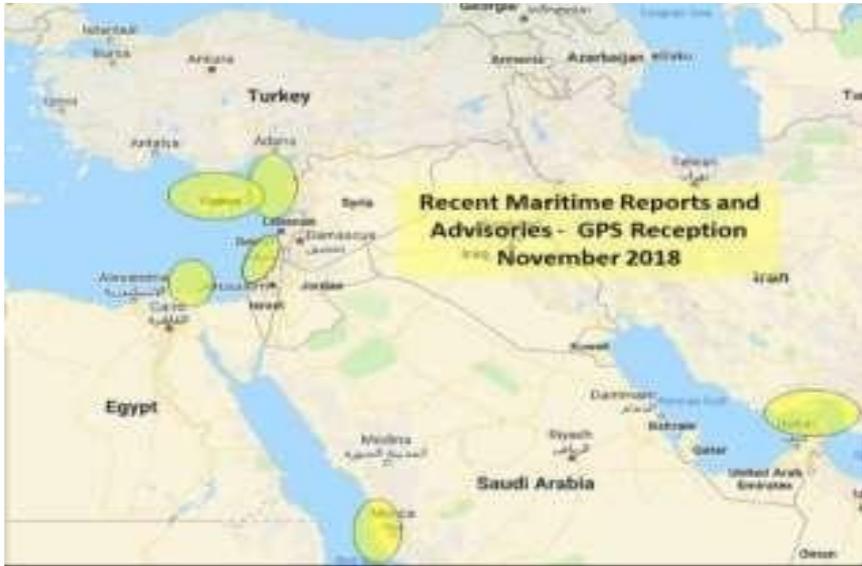
Um ataque de GPS Spoofing tenta enganar um receptor GPS transmitindo sinais falsos, estruturados para se assemelhar a um conjunto de sinais GPS normais, ou retransmitindo sinais genuínos capturados em lugar ou momento diferente.



GPS Spoofing



Várias ocorrências de interferência significativa no GPS foram relatadas por embarcações e aeronaves que operam no Mar Mediterrâneo Oriental (e também no Pacífico)





Maersk – 2017



Ataque cibernético com o vírus NotPetya



Problemas no processamento de pedidos



“Políticas” e “Administração de TI hábil” estabelecidas falharam em impedir o ataque e suas consequências





Colonial Pipeline 2021



G1

ECONOMIA

TECNOLOGIA

O ataque de hackers a maior oleoduto dos EUA que fez governo declarar estado de emergência

Um grupo de hackers desconectou completamente um oleoduto e roubou mais de 100 GB de informações.



Por BBC

10/05/2021 10h51 - Atualizado há 5 dias

Pipeline spans more than 5,500 miles

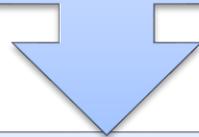




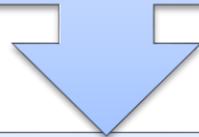
Colonial Pipeline 2021



Hackers desconectaram a rede e roubaram mais de 100 GB de informações do oleoduto da empresa Colonial



Oleoduto transporta mais de 2,5 milhões de barris de óleo por dia, correspondendo a 45% do abastecimento de diesel, gasolina e querosene de aviação da costa leste dos EUA



Estimativa de aumento dos combustíveis entre 2 e 3% por dia enquanto durasse a crise



Jawaharlal Nehru Port



Logistics

Suspected cyber attack cripples box terminal run by Jawaharlal Nehru Port Authority

P. Manoj | Mumbai, February 22 | Updated On: Feb 22, 2022



JNPCT is not accepting vessels alongside due to outage of the system and has diverted one vessel

A suspected cyber-attack of the management information system (MIS) has crippled the container terminal run by the state-owned port authority at Jawaharlal Nehru Port from Monday, forcing the Jawaharlal Nehru Container Terminal (JNPCT) to divert one container

ship to other terminals at the port located near Mumbai.

- porto de contêineres mais movimentado da Índia
- sofreu um ataque de ransomware em fevereiro 22



Expeditors International Washington



US logistics giant Expeditors International goes down in major cyberattack

Likely further impacting strained supply chains

February 25, 2022 By: Sebastian Moss [Comment](#)



Logistics giant Expeditors International of Washington has shut down most of its systems due to a cyberattack, disclosed on Sunday, February 20.

The company said that it had "limited ability" to conduct operations, such as arranging freight shipments, customs, and distribution. The company employs around 18,000 people and manages freight movements in more than 300 locations.

The outage comes as global supply chains struggle with the pandemic, and limited US port capacity.

In its quarterly report, the company warned that the cyberattack would impact its financial results.

The type of attack, and whether it was ransomware, was not disclosed. The perpetrator of the attack was also not disclosed.

Also this week, US chip designer [Nvidia was hit by what appears to be a ransomware attack](#).



- Thinkstock / Prasit Rodphan_1

- paralisou seus sistemas por cerca de três semanas
- levou a despesas de US\$ 60 milhões



OTAN terá programa para resposta rápida a ciberataques



29 de junho de 2022



Otan terá programa para resposta rápida a ciberataques

Os países membros da OTAN concordaram em criar um novo programa para responder rapidamente a ataques cibernéticos

- capacidade virtual de resposta rápida para se contrapor a atividades cibernéticas maliciosas significativas
- OTAN reafirmou um compromisso de 2021 de que um ataque cibernético poderia (mas não automaticamente) desencadear o Artigo 5 do Tratado do Atlântico Norte, o que o tornaria um ataque contra a aliança como um todo



ROTEIRO



- Introdução
- Espaço Cibernético e suas Ameaças
- **Estrutura Cibernética na MB**
- Sistema Dreadnought
- Operações Cibernéticas na MB
- Projetos e Desafios
- Considerações Finais



Estrutura Cibernética na MB



Vários Atores

- Ações Transversais
- Níveis Decisórios

SegCiber

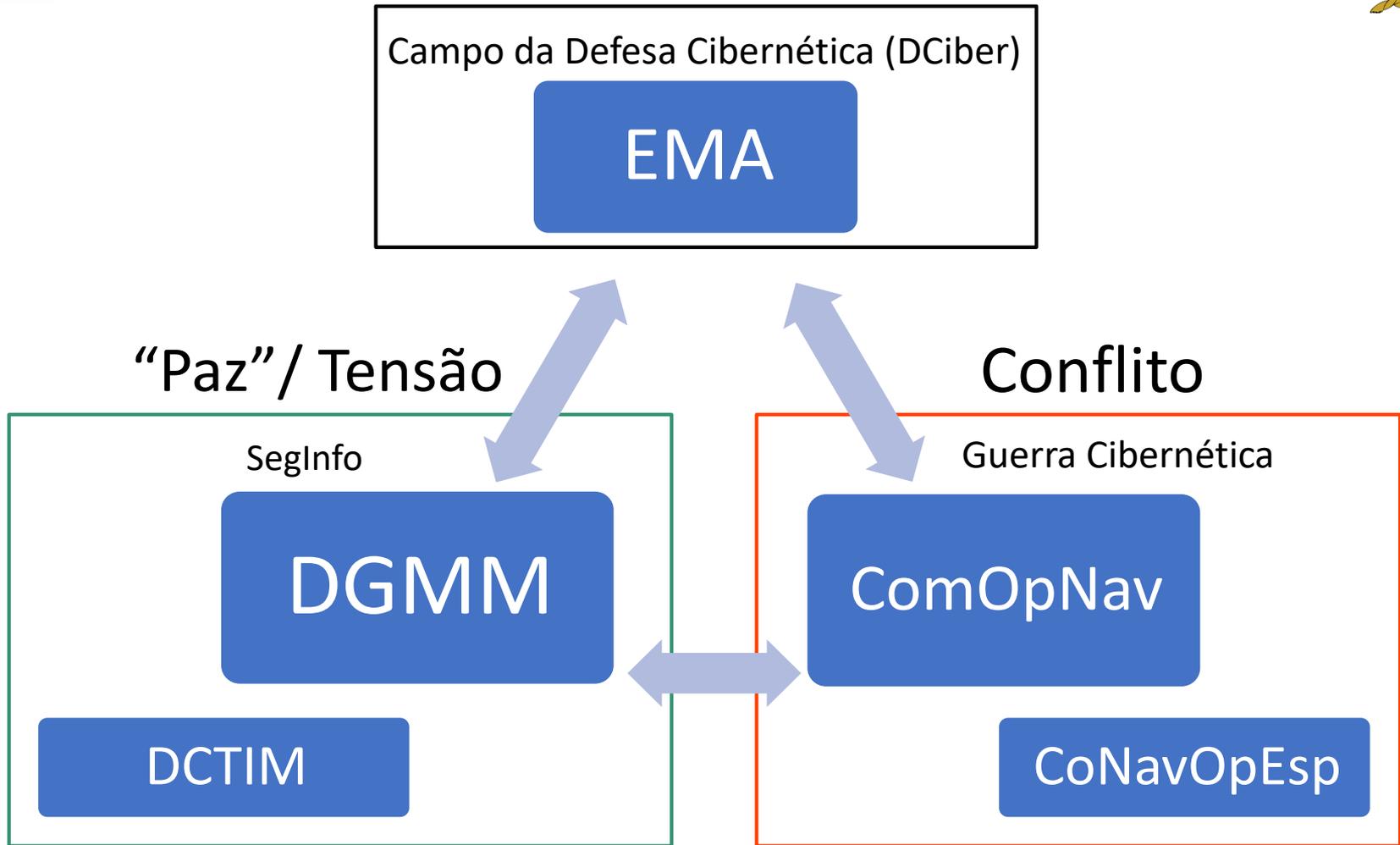
- DefCiber (Estratégico)
- Seg Info
- GCiber (Operacional e Tático)

Contextos

- “Paz”/ Tensão
- Conflito



Estrutura Cibernética na MB





Setor do Material



Natureza

- Administrativa
- Contínua

Atuação

- Cadeia logística (*hardware e software*)
 - Normas e especificações
 - Configuração, operação e manutenção
- com concurso do CMatFN

Segurança da Informação e Proteção Administrativa



Setor Operativo



Natureza

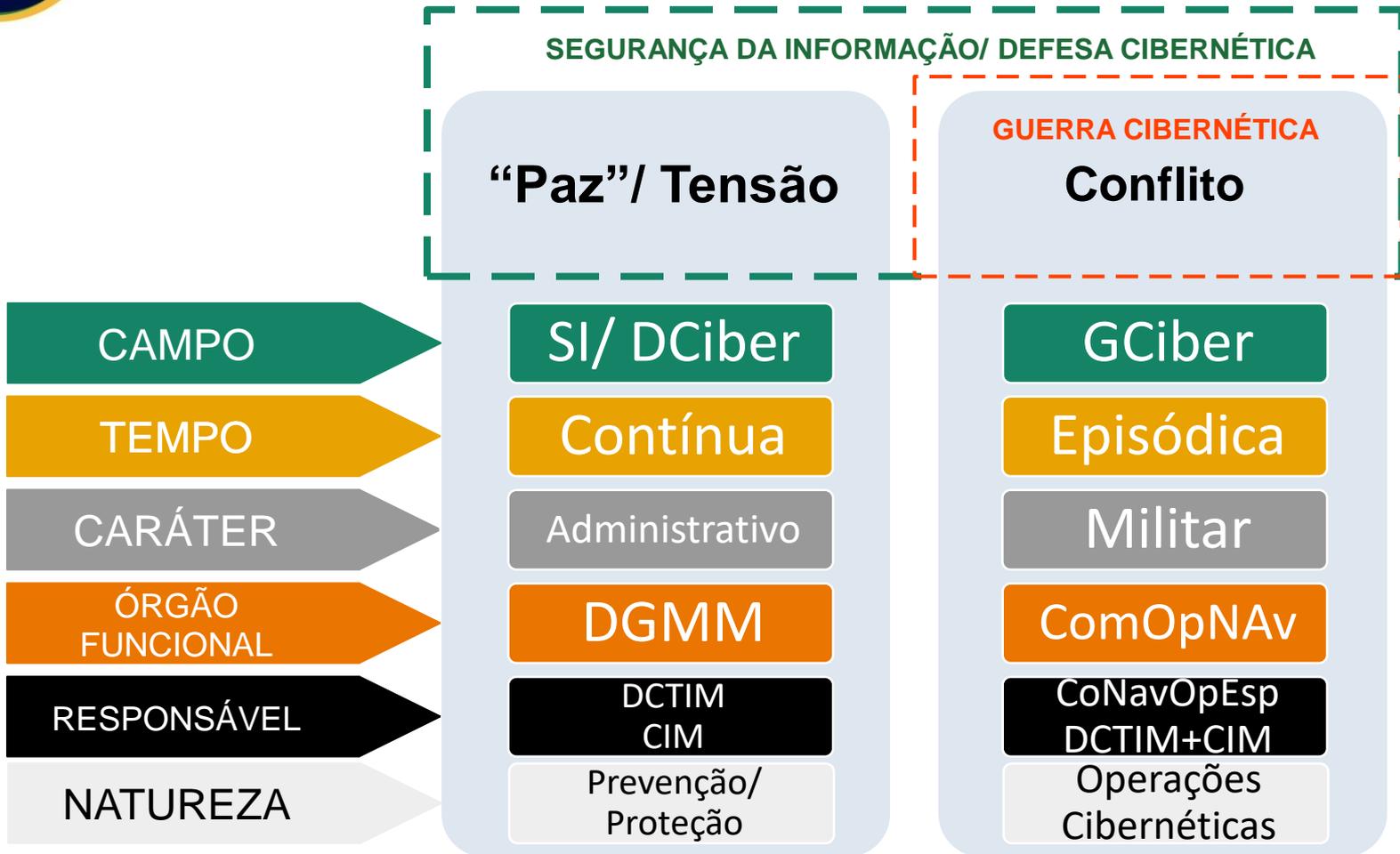
- Operativa
- Episódica

Atuação

- Planejamento militar
- Operações e exercícios militares
- Táticas e procedimentos operativos voltados para OpInfo



Estrutura Cibernética na MB





Estrutura Cibernética na MB



ComOpNav

- Diretivas e Regras de Engajamento
- GptOpGCiber

DCTIM

- Prevenção e Proteção da RECIM

CIM

- Inteligência e Contra-inteligência Cibernética



Roteiro



- Introdução
- Espaço Cibernético e suas Ameaças
- Estrutura Cibernética na MB
- **Sistema Dreadnought**
- Operações Cibernéticas na MB
- Projetos e Desafios
- Considerações Finais



Dreadnought



Sistema Militar de Proteção Cibernética (SMPC) - Projeto autóctone para:

- prover proteção cibernética customizada às unidades operacionais;
- otimizar a utilização do link das unidades operacionais (X, Ku e SISCOMIS);
- oferecer consciência situacional; e
- instalado em mais de 20 OM.





Sistema Dreadnought



Hardware padrão servidor escalável

Software livre configuração modular

Monitoramento e segurança aplicada



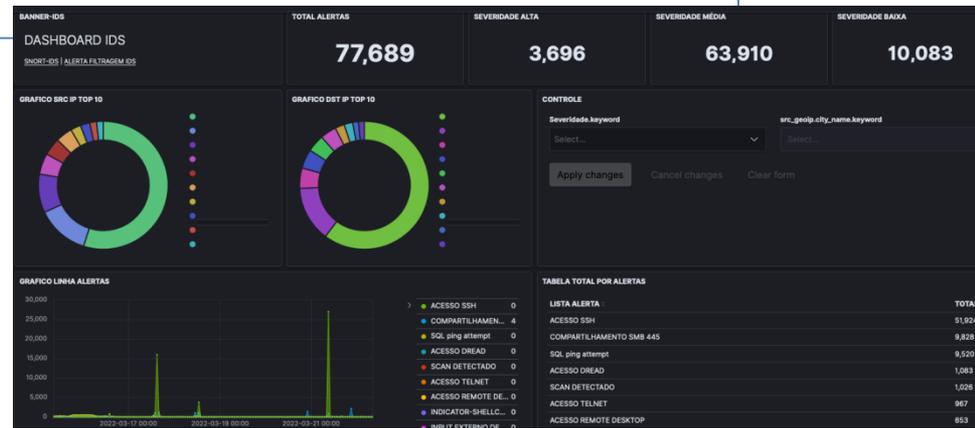
Possibilidades Dreadnought



Identificação das ameaças na rede

Proteção cibernética customizada

Consciência situacional cibernética





Limitações Dreadnought



Tratamento de incidentes cibernéticos

Levantamento das vulnerabilidades existentes

Análise automatizada do espaço cibernético



Roteiro



- Introdução
- Espaço Cibernético e suas Ameaças
- Estrutura Cibernética na MB
- Sistema Dreadnought
- Operações Cibernéticas na MB
- Projetos e Desafios
- Considerações Finais



Octopus / Alligator



Atividades

Adestrar Operadores Cibernéticos no emprego do Dreadnought

Adestrar EqExplAtq na realização das AGCiber do tipo Exploração





Ciber Securitas



Atividades

Adestrar EqDsv na construção do Ambiente Virtual

Adestrar CLTI e EqExplAtq na realização das AGCiber

Desenvolver procedimentos integrados
(CLTI e DivGCiber)





Baluarte



Objetivos

Adestrar a realização das AGCiber

Testar e aperfeiçoar procedimentos operativos

Adestrar a estrutura de prevenção e salvaguarda da
RECIM

Identificar oportunidades de melhorias dos sistemas e
das ferramentas de segurança



Op Baluarte



Ataque de Força Bruta

Engenharia Social
(Phishing)





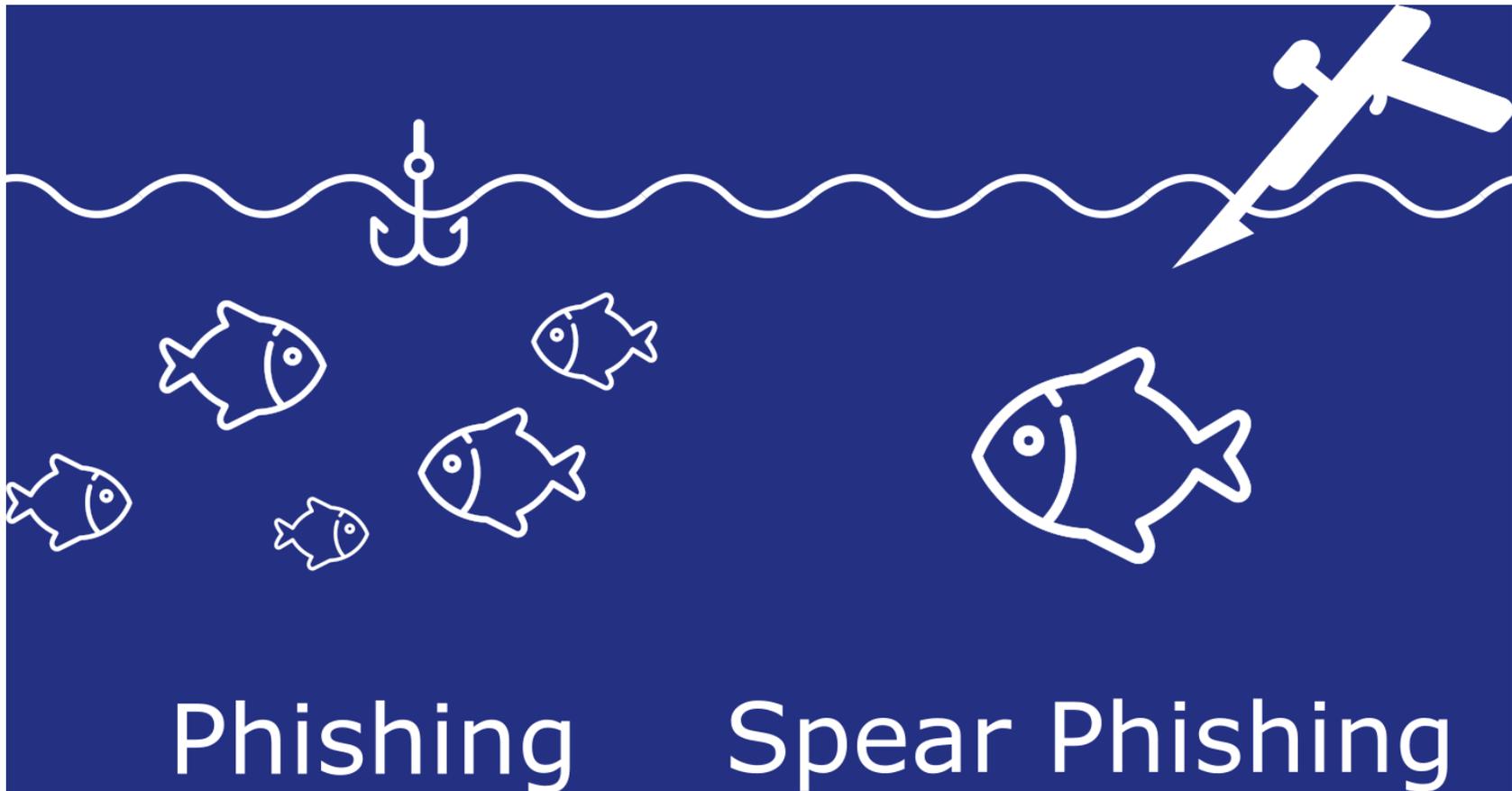
Phishing



- O Phishing como ferramenta de Engenharia social atua diretamente na fraqueza da mentalidade em defesa cibernética do usuário; e
- Todos os usuários devem ter consciência cibernética, sabendo que são os donos da proteção dos próprios dados, evitando abrir e-mails maliciosos e clicar em links de anúncios desconhecidos.



DEFINIÇÃO



Spear Phishing - Utilização de ferramentas de forma direcionada, atreladas a anúncios personalizados, para captar informações sigilosas da vítima.



Phishing



esquentafinalde2017.com.br/categoria/PRODUTO76655ap

Lista de Casamento - Crie sua lista ou encontre o presente ideal para os noivos. Pague em até 12x sem juros com o Cartão Pontofrio. **Peça Já!**

Pontofrio.com.br - Telefones e Celulares - Smartphones - **Android**

Smartphone Samsung Galaxy J7 Prime Duos Dourado com 32GB, Tela 5.5", Dual Chip, 4G, Câmera 13MP, Leitor Biométrico, Android 6.0 e Processador OctaCore

Múltiplas 550 Pontos

Imagens Vídeos

compre no site Entrega Super Expressa

354 avaliações Leia [faça uma avaliação](#)

Confira outras lojas que vendem o mesmo produto: De R\$ 999,00 até R\$ 1.499,00

Vendido e entregue por **Pontofrio.com**

Aproveite e contraste

Microsoft Office 365 Pacote Office + 170 armazenamento nuvem Em até 12x de R\$ 4,00 Total à vista: R\$ 48,99

De: R\$ 1.299,00 Por: **R\$ 501,50**

Comprar Reciba em casa

Negocie Negocie o preço

Seguro | https://www.pontofrio.com.br/TelefonesCelular

Lista de Casamento - Crie sua lista ou encontre o presente ideal para os noivos. Pague em até 12x sem juros com o Cartão Pontofrio. **Peça Já!**

Pontofrio.com.br - Telefones e Celulares - Smartphones - **Android**

Smartphone Samsung Galaxy J7 Prime Duos Dourado com 32GB, Tela 5.5", Dual Chip, 4G, Câmera 13MP, Leitor Biométrico, Android 6.0 e Processador OctaCore

Múltiplas 550 Pontos

Imagens Vídeos

compre no site Confira as opções

356 Avaliações Leia [faça uma avaliação](#)

Confira outras lojas que vendem o mesmo produto: De R\$ 999,00 até R\$ 1.619,00

Vendido e entregue por **Pontofrio.com**

Aproveite e contraste

Microsoft Office 365 Pacote Office + 170 armazenamento nuvem Em até 12x de R\$ 4,00 Total à vista: R\$ 48,99

De: R\$ 1.299,00 Por: **R\$ 1.099,00** ou até 12x de R\$ 91,58 sem juros

Comprar Reciba em casa

Retirar na loja Retire o Grátis

ReclameAQUI
(0xx11) 4002-3050



ROTEIRO



- Introdução
- Espaço Cibernético e suas Ameaças
- Estrutura Cibernética na MB
- Sistema Dreadnought
- Operações Cibernéticas na MB
- **Projetos e Desafios**
- Considerações Finais



Projetos e Desafios



Projeto Submarino Nuclear



Projeto Classe Tamandaré



Sistema de Comando e Controle do CFN

ECiber



Fusão de Dados



Fluxo de Informações



Tomada de Decisão



Projetos e Desafios



Ampliar a capacidade cibernética dissuasória

Separar o contexto operacional e tático

Capacitar o combatente cibernético



Criação do EsqdGCiber



Ampliará a capacidade dissuasória

Assumirá as tarefas no nível tático

Permitirá uma postura de combatente



Roteiro



- Introdução
- Espaço Cibernético e suas Ameaças
- Estrutura Cibernética na MB
- Sistema Dreadnought
- Operações Cibernéticas na MB
- Projetos e Desafios
- Considerações Finais



Considerações Finais



Transversabilidade

- ECiber é transversal aos domínios clássicos: mar, terra, ar e espaço

Integração

- ACiber são vetores de integração das expressões de poder: política, militar, econômica, psicossocial e científico tecnológica (informacional)

Mentalidade de SegCiber

- Escolas de Formação
- Centros de Instrução
- Escolas de Alto Estudos



Desafios



Revisão dos marcos legais

Cooperação

Gerenciamento da crise em **alto nível**

Aumento da **conscientização** nos níveis político, estratégico, operacional e tático

Desenvolvimento da capacidade cibernética



Elementos da Solução

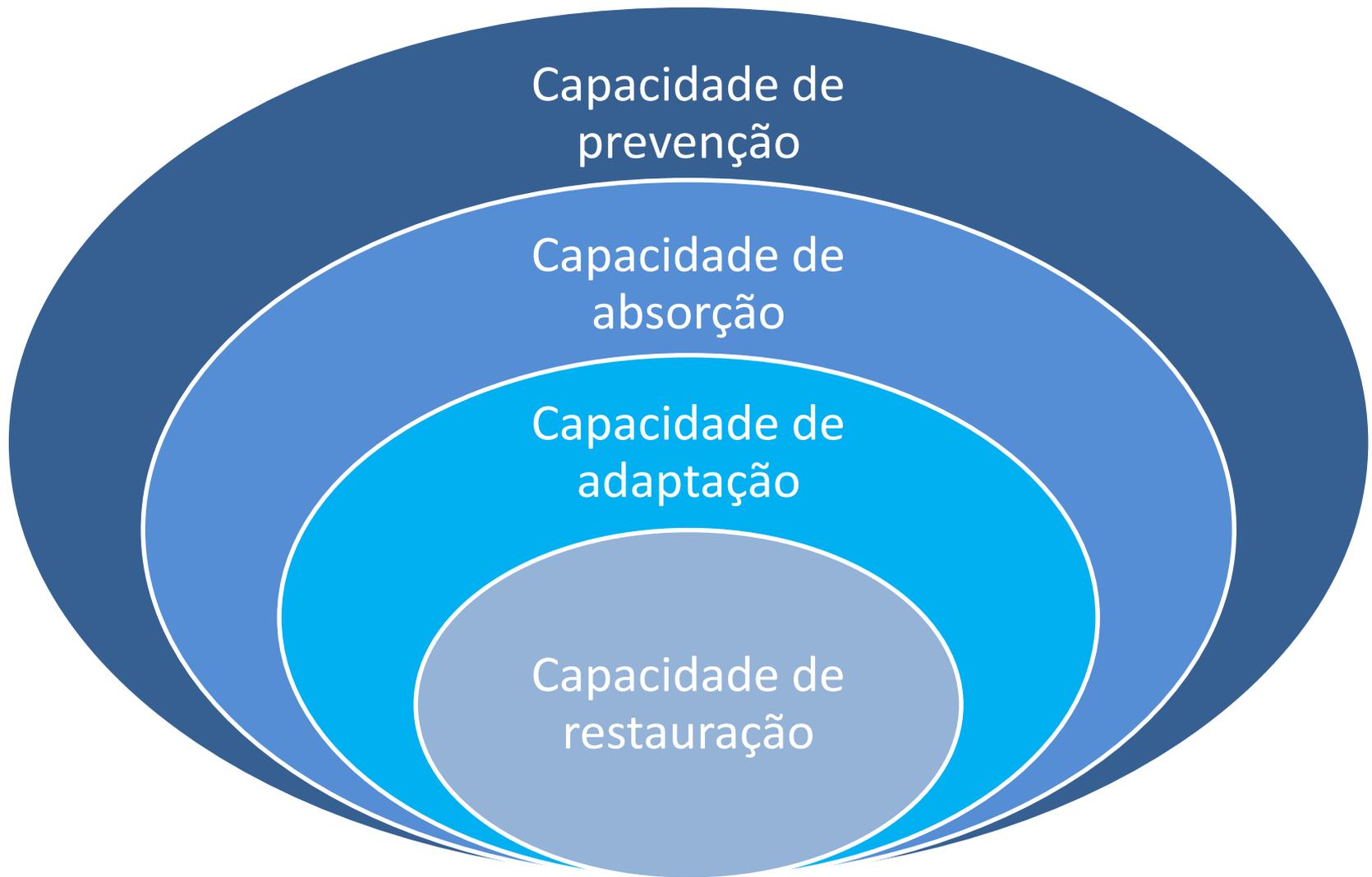


Eficiência





Resiliência





Cooperação



Governo

Participação de ministérios e outras entidades

Ações conjuntas e interagências

Respostas com credibilidade e adequadas

Sociedade civil

Conscientização da importância do tema

Academia

Setor privado

Internacional

Colaboração entre Estados e Organizações Internacionais

Compartilhamento de Informações

Ações multilaterais





Proatividade



Proatividade é **agir antecipadamente**, evitando ou resolvendo problemas futuros.



Proatividade



Estratégia proativa é essencial para reduzir riscos cibernéticos

Identificar, mitigar, preparar e decidir são alguns dos verbos a ter em conta no processo:

1. Identificar os riscos e ameaças cibernéticas;
2. Mitigá-los de acordo com as melhores práticas de segurança cibernética;
3. Preparar-se e estar pronto para novos incidentes;
4. Decidir com base na informação.

Comando Naval de Operações Especiais



CA (FN) Claudio EDUARDO Silva Dias

eduardo@marinha.mil.br



Previsão de Atividades 2022

Operações Combinadas

- Estudo para Exercício com Peru

Operações Conjuntas

- Operação Guardião Cibernético

Operações Singulares

- Operação Octopus_(n) com ComemCh
- Operação Alligator com o ComFFE
- Operação BALUARTE
- Operação Ciber Securitas

